업무참고 2025-클라우드대응-②-64

금융분야
상용 클라우드컴퓨팅서비스 보안 관리 참고서

카카오엔터프라이즈

금융보안원
FINANCIAL SECURITY INSTITUTE

kakaoenterprise

CONTENTS

1. 가상자원 관리

1.1. 가상자원 생성 시 최초 계정에 대한 비밀번호 규칙 수립
1.2. 이용자 가상자원 접근시 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 가상자원 별 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 등 보안통제 방안을 수립하여야 한다.

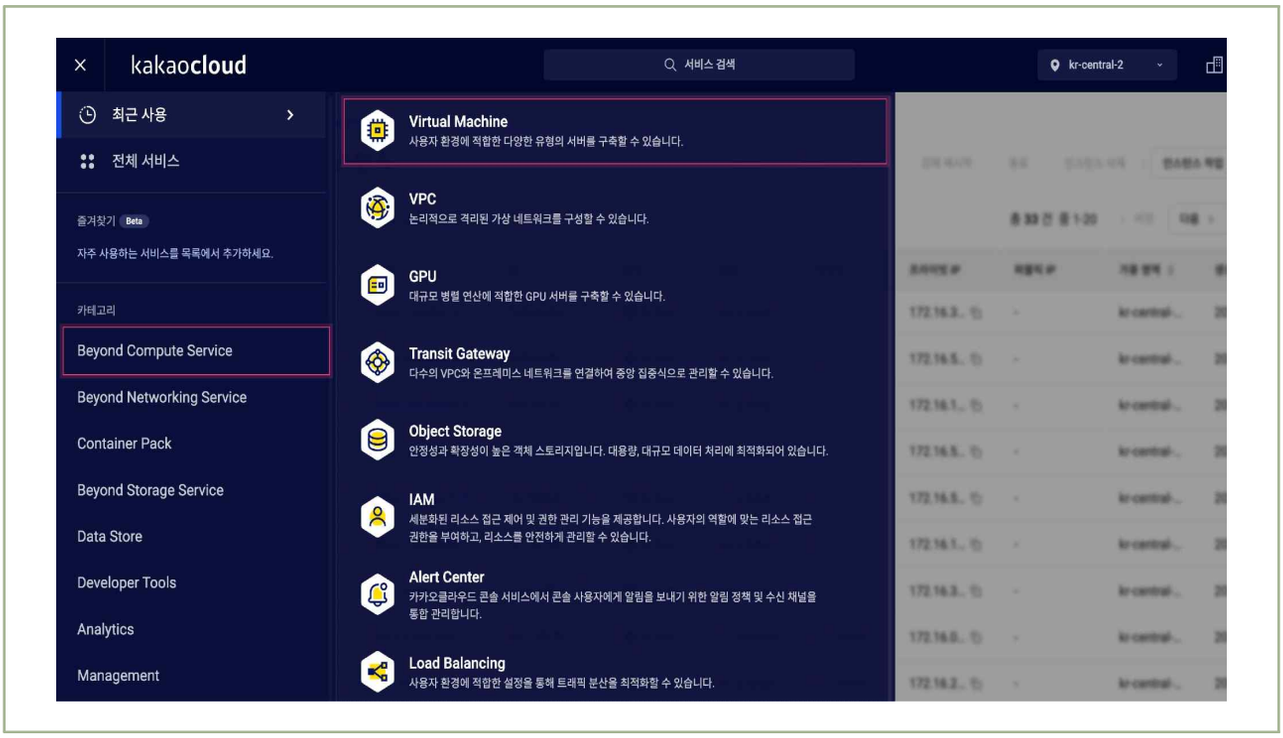
  - 예시

    1) 가상머신, 베어메탈 생성 시 PEM키(private key)를 생성한 이용자가 다운로드 받도록 하고, 이후 클라우드 상에서는 공유하는 기능을 제공하지 않는다.
    2) 가상머신 또는 베어메탈 생성 이후 OS 내에서 사용자 생성 및 암호 부여는 이용자의 권한이며, 클라우드 공급자는 별도로 이용자가 생성한 암호를 관리하지 않는다.
    3) 가상자원의 OS 내에 생성된 계정은 가급적 PEM키 사용을 권장하며, 패스워드 사용이 필요한 경우 패스워드 복잡도 및 만료일 설정을 통해 관리할 수 있도록 권장한다.

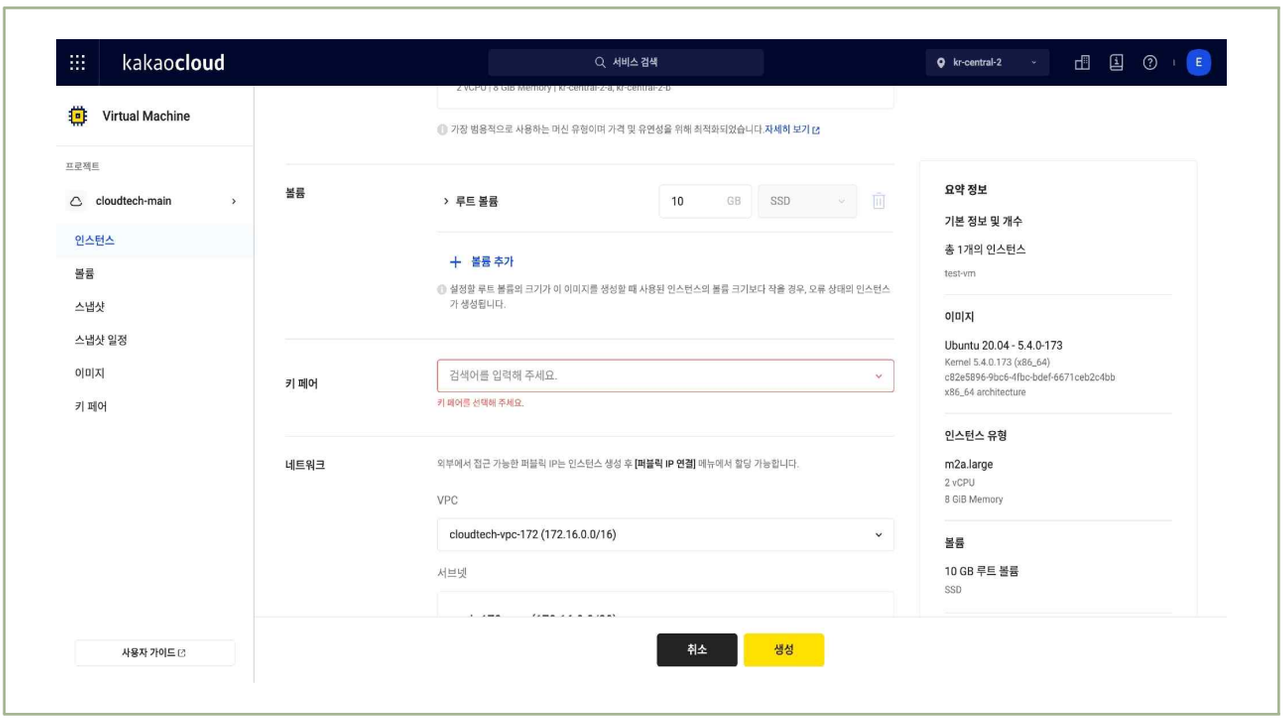
3 우수 사례

- 이용자가 가상자원 생성 시 비밀번호를 설정할 수 없으며, PEM키를 선택해야 생성이 가능합니다.

  - **(Console)** ‘Dashboard’ → ‘Beyond Compute Service’ → ‘Virtual Machine’ → ‘인스턴스 생성’ 시 비밀번호를 입력하는 기능은 없으며, PEM키를 선택하지 않으면 설치가 진행되지 않습니다.



| 그림 1-1-1 | 카카오클라우드 콘솔 〉 Virtual Machine 서비스 이동



| 그림 1-1-2 | 인스턴스 생성 시, 키페어 선택 필수

- (API(CLI)) ‘API/CLI 환경을 통한 가상자원 생성 시에도 server.key_name 값이 필수값이어서 PEM키가 없이는 가상자원 생성이 불가합니다.

Request Header

종류	파라미터	형식	설명
Header	X-Auth-Token*	String	{tokenId} : API 인증 토큰

Request Body

종류	파라미터	형식	설명
Body	server*	Object	생성할 인스턴스 객체
	server.name*	String	인스턴스 이름
	server.imageRef*	String	사용할 이미지 ID
	server.flavorRef*	String	사용할 인스턴스 유형 ID
	server.availability_zone*	String	인스턴스의 가용영역
	server.security_groups*	Array	인스턴스와 연결되는 보안 그룹
	server.key_name*	String	인스턴스 적용할 기존 키 페어

| 그림 1-1-3 | 가상자원 생성 시, 요구되는 Header, Request 파라미터

4 참고 사항

- 카카오클라우드 마켓플레이스 소개
- 카카오클라우드 인스턴스 생성 및 연결 가이드
- 카카오클라우드 키 페어 생성 및 관리 가이드

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.

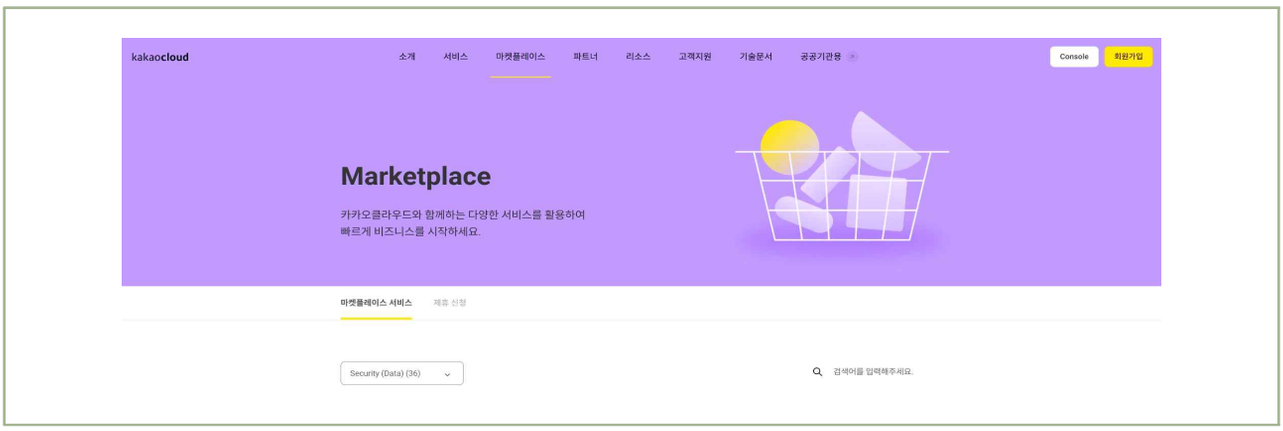
  - 예시

    1) 로그인 오류에 따른 보안통제 방안 수립 등

3 우수 사례

- 보안 솔루션을 이용한 로그인 규칙 적용

  - **(3rd-party 제품)** MarketPlace 중 security(Data) 상품 군 내 서버접근제어 솔루션을 이용하여 로그인 규칙(실패 허용 횟수, 차단 시간 등)을 설정할 수 있습니다.



| 그림 1-2-1 | 카카오클라우드 마켓플레이스 상품 소개 페이지

4 참고 사항

- 카카오클라우드 마켓플레이스 소개

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.(단, 기능이 제공되지 않는 경우 안전한 로그인 수단을 확보하여야 한다.)

  - 예시

    1) 이메일 인증
    2) SMS 인증
    3) 별도 인증도구 활용
    4) SSH PEM Key 등을 통한 안전한 로그인 수단 확보 등

3 우수 사례

- 이용자는 1.1. 항목을 참고하여 SSH PEM Key를 통한 로그인 정책 적용이 필요합니다.

4 참고 사항

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 내부 IP 또는 IP 대역에서만 접근할 수있도록 설정하여야 한다.

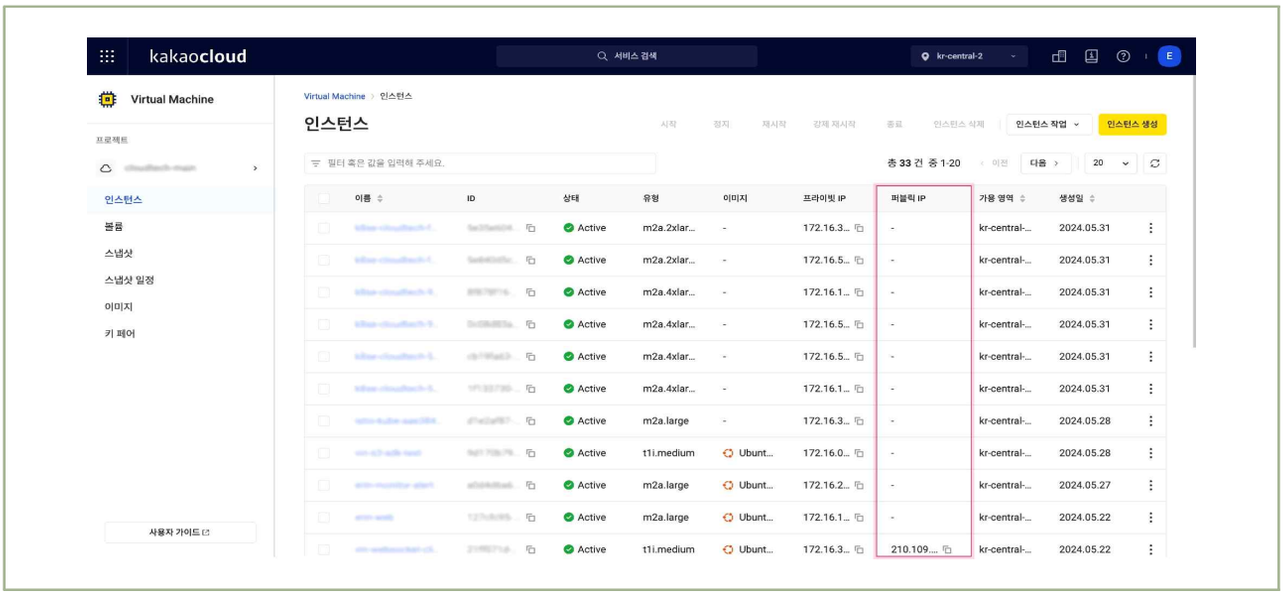
  - 예시

    1) 가상자원에 연결된 퍼블릭 IP(외부) 점검 및 제거
    2) IP/Port 기반 접근 통제 설정
    3) VPC 및 라우팅 테이블을 통한 내부 네트워크 대역 접근 설정

3 우수 사례

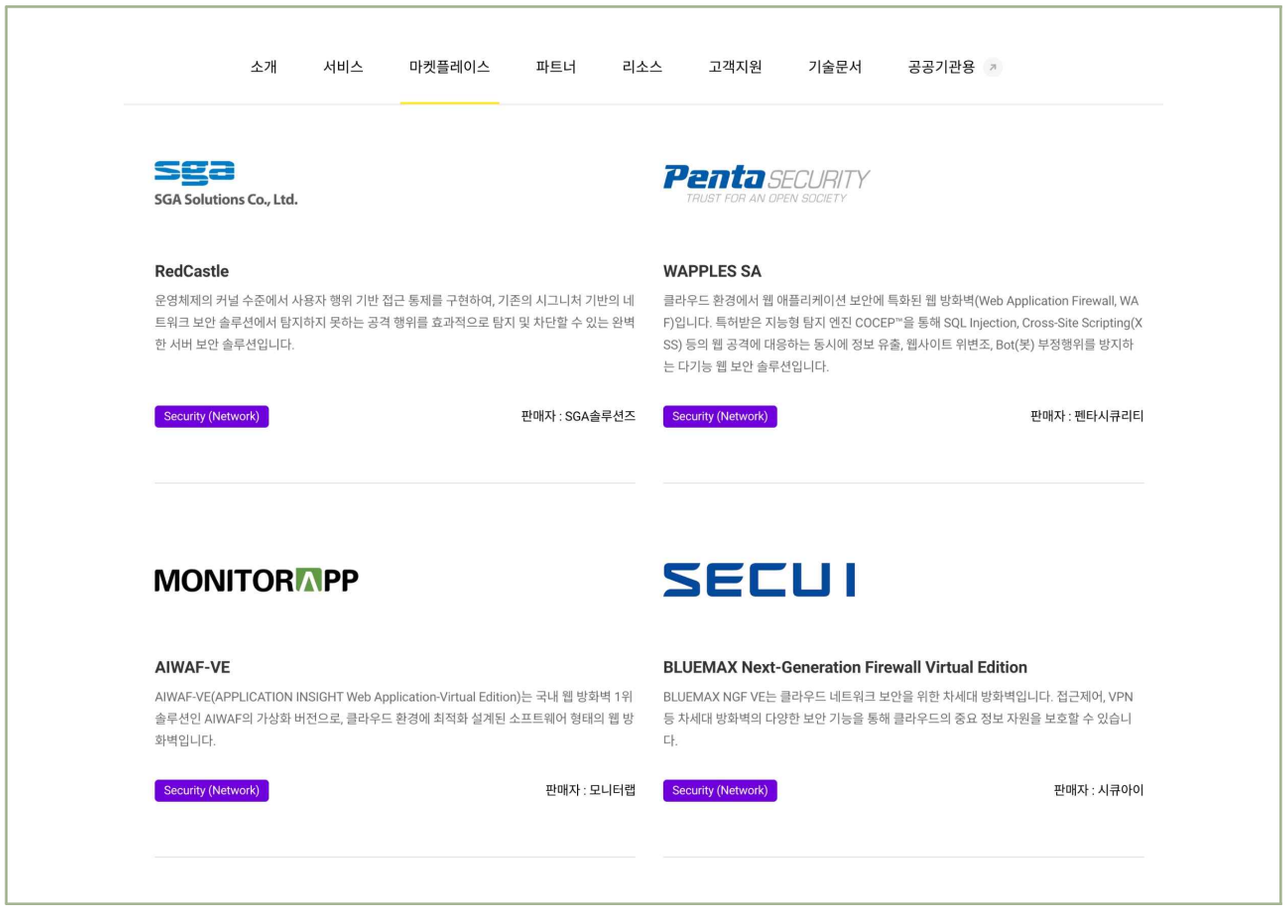
- 가상자원에 연결된 퍼블릭 IP가 있는지 점검

  - **(Console)** ‘Dashboard’ → ‘Beyond Compute Service’ → ‘Virtual Machine’ → ‘인스턴스’ 화면에서 노출되는 가상자원 목록에 “퍼블릭 IP” 가 연결되어 있는지 확인합니다.



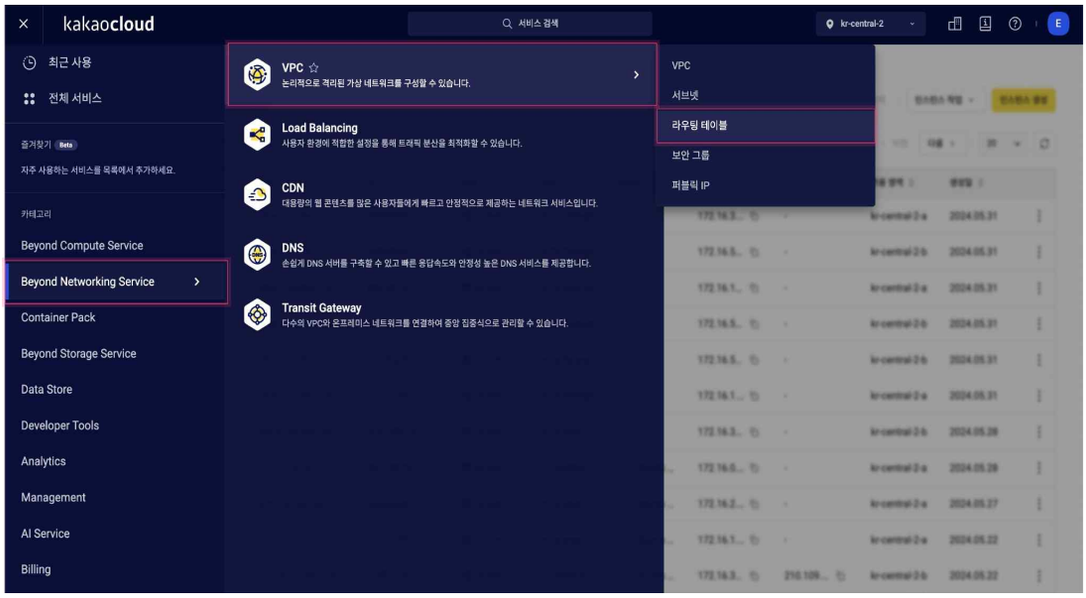
| 그림 1-4-1 | VM 인스턴스 목록 조회 시, 퍼블릭 IP 연결 여부 확인

- 접근 가능한 IP 또는 IP 대역대 설정
  - **(3rd-party 제품)** MarketPlace 상품 중 Security(Network) 상품군에 해당하는 제품을 활용하여 접근 제어 설정을 할 수 있습니다.

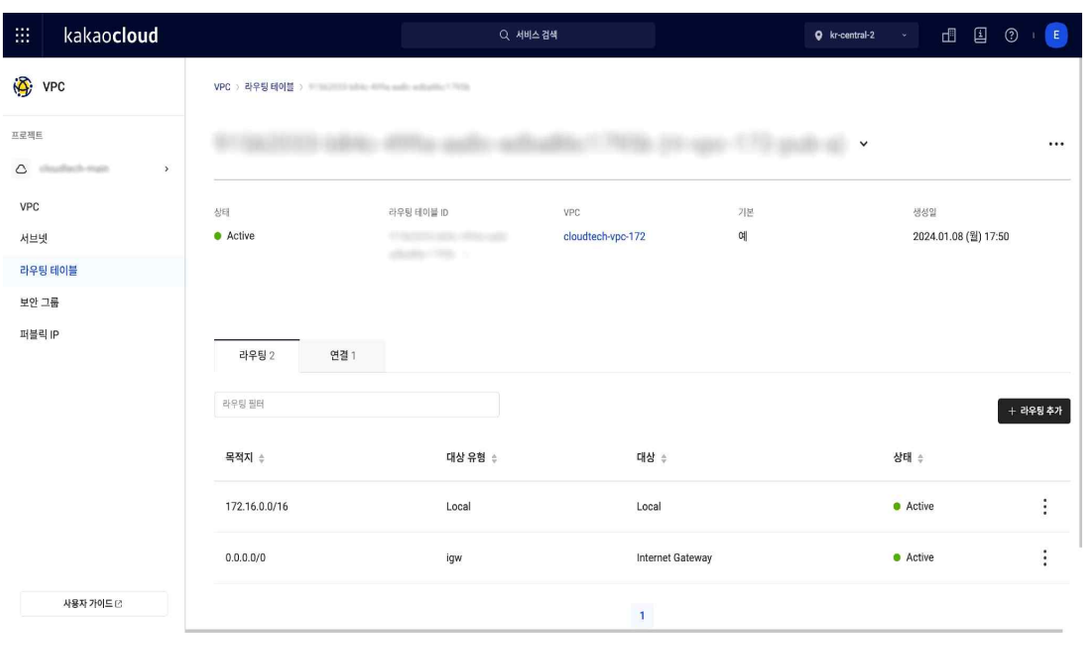


| 그림 1-4-2 | 카카오클라우드 마켓플레이스의 접근 제어 가능 상품 중 일부

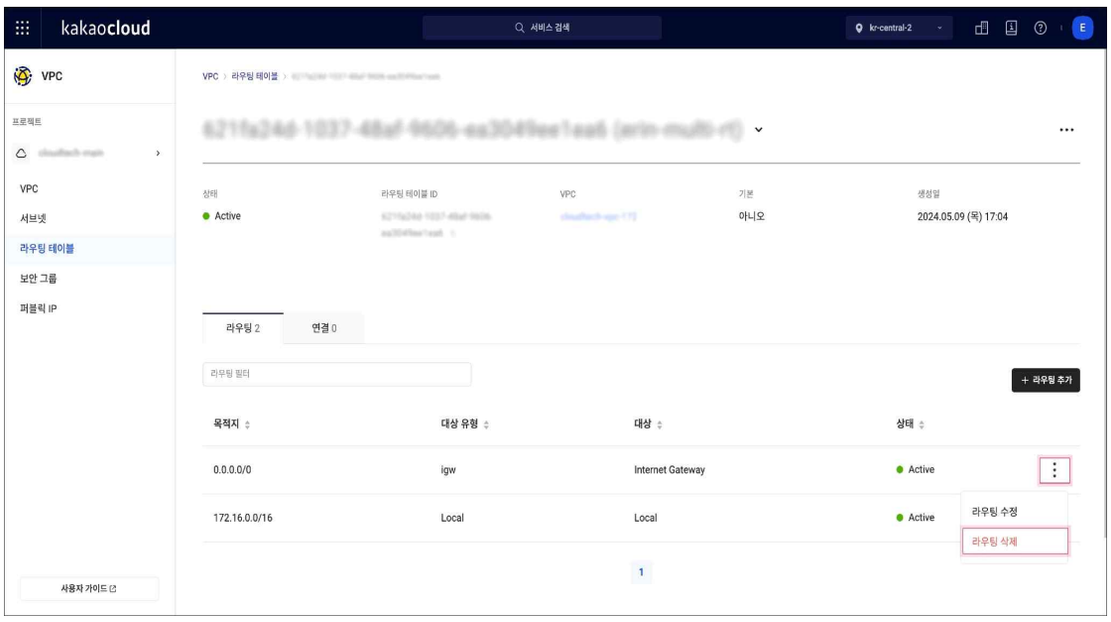
- VPC 및 보안 그룹을 통한 내부 네트워크 대역 접근 설정
  - **(Console)** 'Dashboard' → 'Beyond Networking Service' → 'VPC' → '라우팅 테이블' 화면에서 확인할 라우팅테이블 선택합니다. → 라우팅 테이블 상세 페이지에서 라우팅 정보를 확인하여 불필요하게 외부에서 통신이 가능하도록 설정되어 있는 부분이 없는지 점검합니다. (모든 대역을 목적지로 Internet Gateway로 가도록 되어있는 설정 등)



| 그림 1-4-3 | 카카오클라우드 콘솔 〉 라우팅테이블 서비스 이동

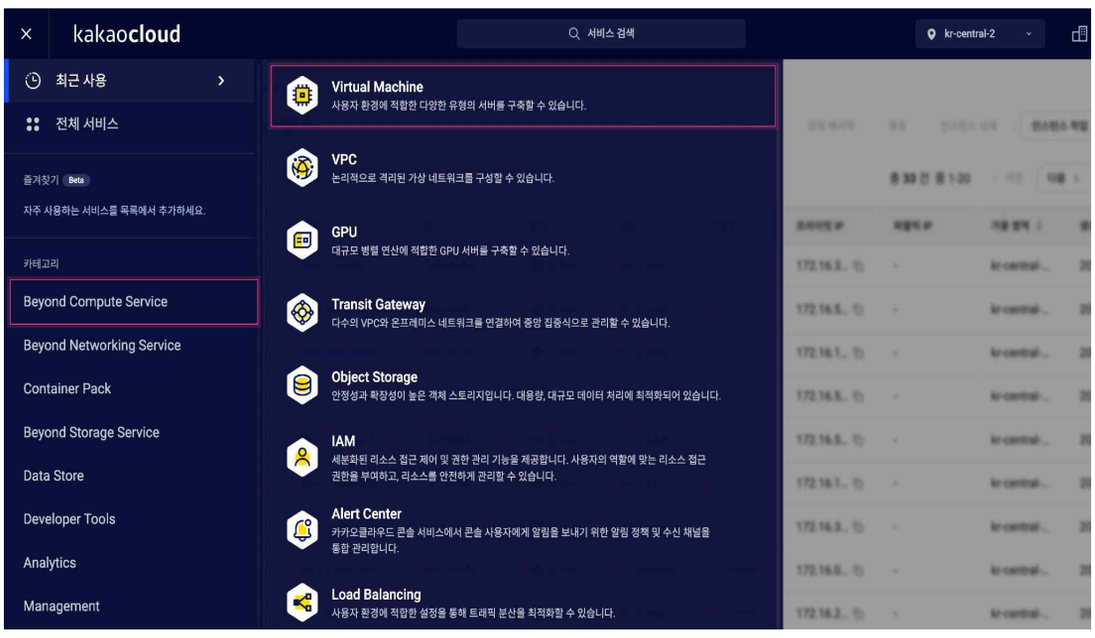


| 그림 1-4-4 | 라우팅 테이블 상세 페이지에서 라우팅 정보를 확인

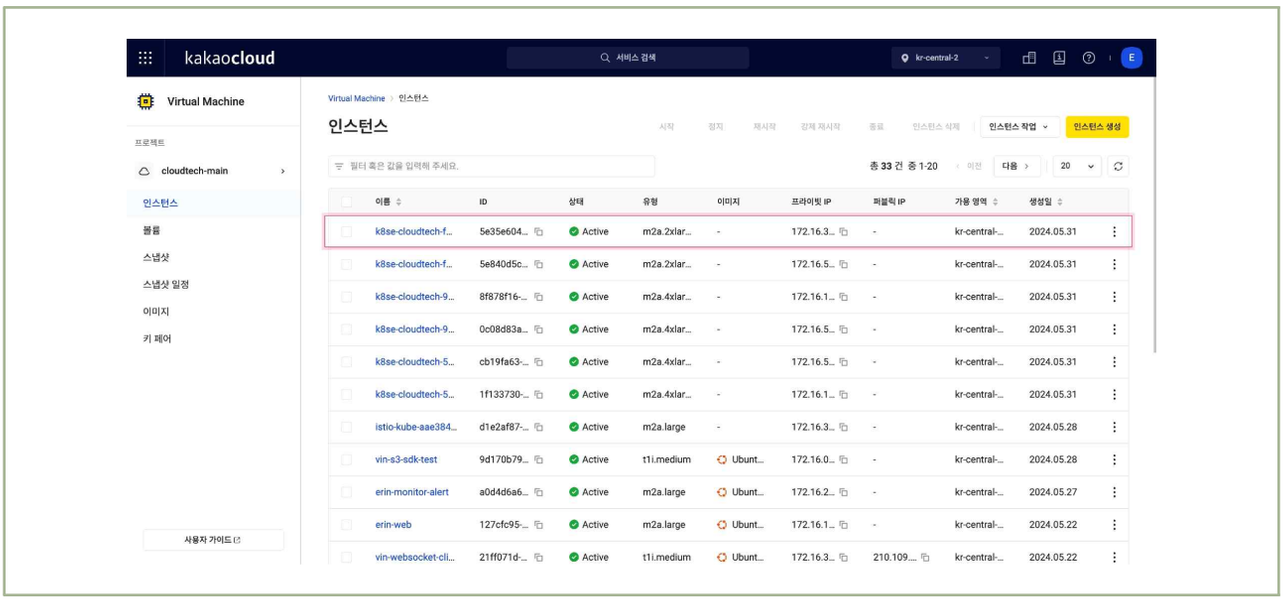


| 그림 1-4-5 | 외부 접점 차단을 위해 Internet Gateway 제거

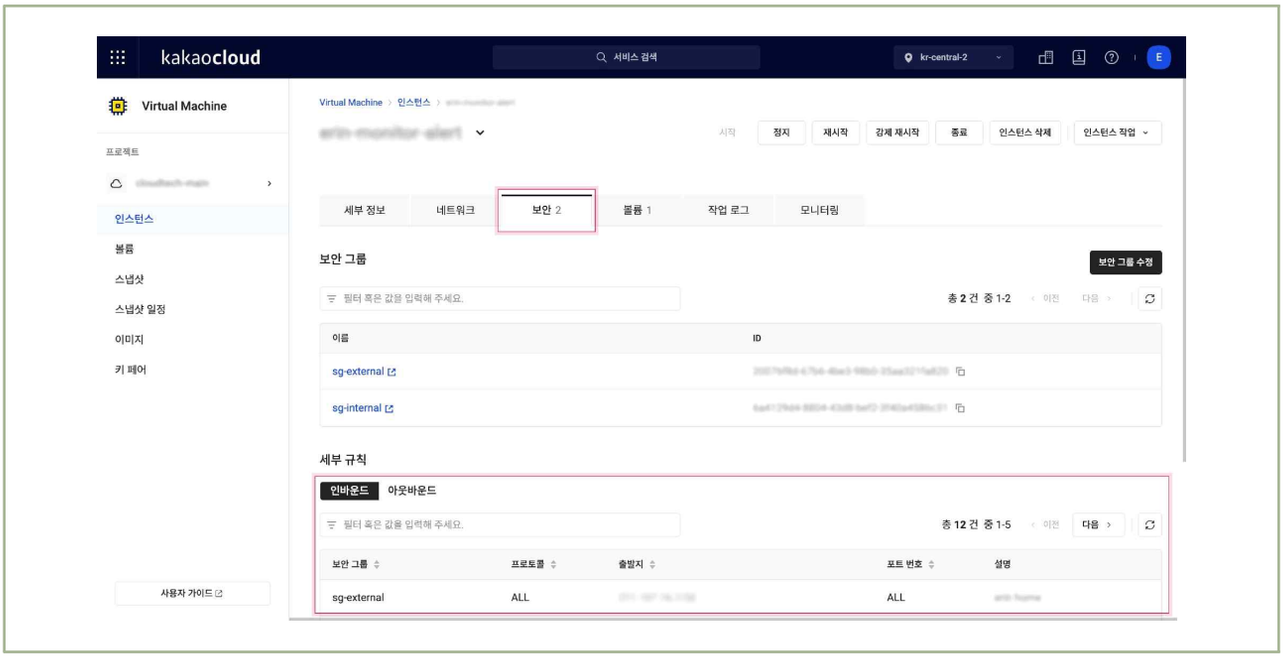
- (Console) 'Dashboard' → 'Beyond Compute Service' → 'Virtual Machine' → '인스턴스' 화면에서 확인할 인스턴스 선택 → '인스턴스 상세 페이지' 에서 '보안' 탭 → 인바운드에 대한 세부 규칙 확인하여 의도하지 않은 인바운드 규칙이나 모든 대역에 대해 허용되어 있는 규칙이 있는지 점검합니다.



| 그림 1-4-6 | 카카오클라우드 콘솔 〉 Virtual Machine 이동



| 그림 1-4-7 | 인스턴스 상세 페이지로 이동



| 그림 1-4-8 | 인스턴스 상세 페이지 〉 보안 탭 〉 인바운드 규칙 확인

| 그림 1-4-9 | 보안그룹명칭을 출발지로 설정하여 해당 보안그룹을 가진 가상자원들만이 접근할 수 있는 규칙 생성

4 참고 사항

- 카카오클라우드 인스턴스 목록 보기 가이드
- 카카오클라우드 VPC 〉 라우팅 테이블 관리 가이드
- 카카오클라우드 인스턴스 보안 그룹 수정 가이드

1 기준

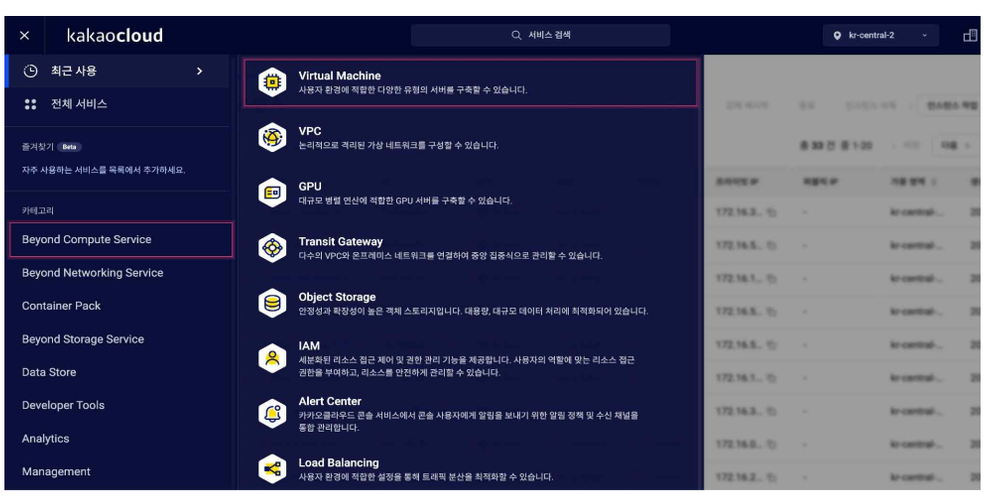
식별번호	기준	내용
1.5.	**가상자원 접속 시 보안 방안 수립**	**이용자 가상자원 접속 시 안전한 인증절차를 통해 접속하여야 한다.**

2 설명

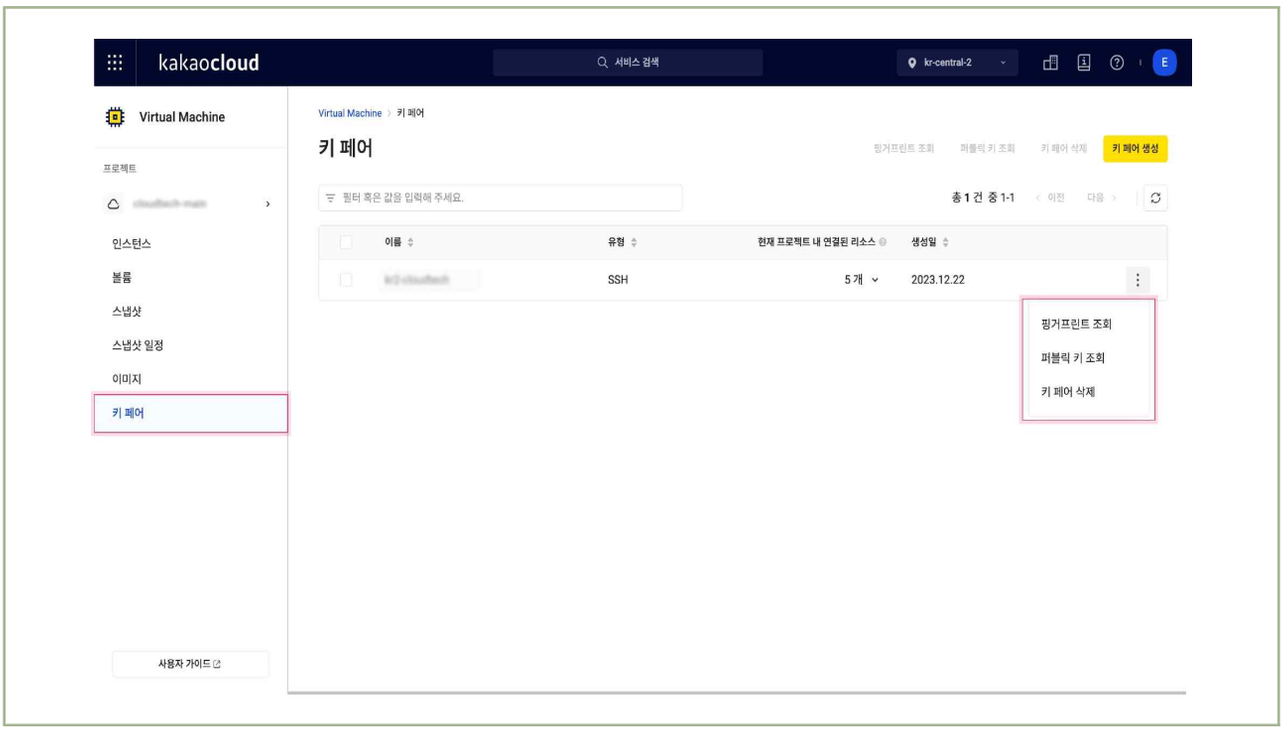
- 이용자 가상자원(인스턴스) 접속 시 안전한 방식을 통해 접근하여야 한다.
  - 예시
    1) 가상머신, 베어메탈 생성 시 PEM키(private key)를 생성한 이용자가 다운로드 받도록 하고, 이후 클라우드 상에서는 공유하는 기능을 제공하지 않는다.
    2) PEM키를 이용하여 원격 터미널 접근 방식 외에 콘솔에서 직접 접근하는 방식은 제공하지 않는다.

3 우수 사례

- 키 페어는 최초 생성시에만 다운로드 받을 수 있으며, 이후에는 public key 조회만 가능하며, 추가 다운로드는 불가합니다.
  - **(Console)** 'Dashboard' → 'Beyond Compute Service' → 'Virtual Machine' → '키 페어'에서 생성되어 있는 키 페어 확인

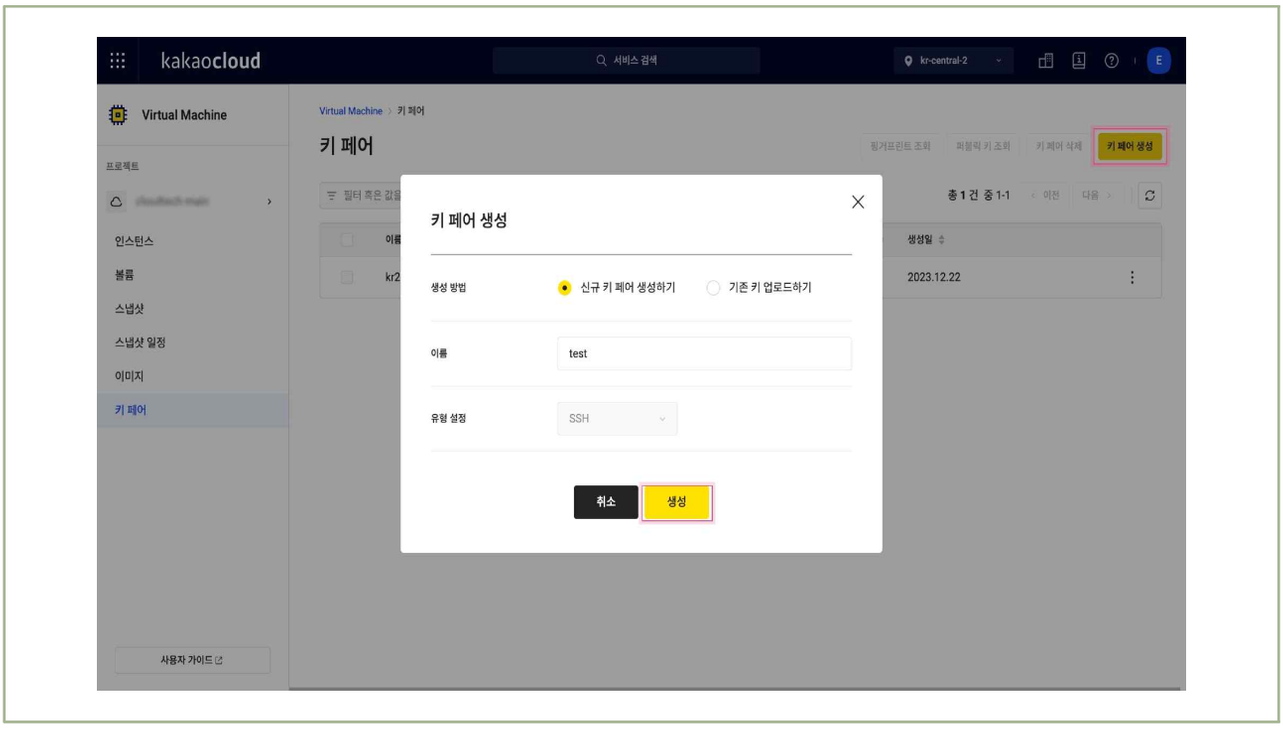


| 그림 1-5-1 | 카카오클라우드 콘솔 〉 Virtual Machine 서비스 이동



| 그림 1-5-2 | 키 페어 관리 화면 (별도의 다운로드 기능은 제공하지 않음)

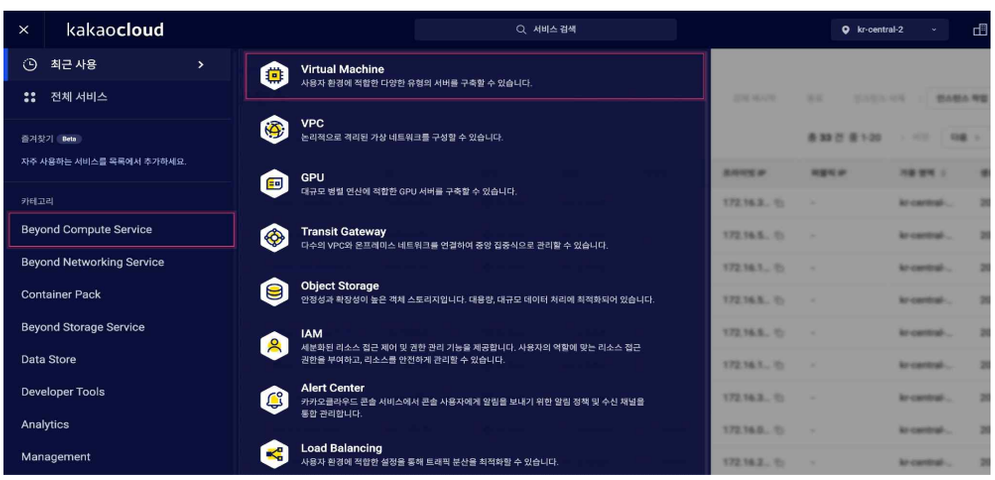
- 최초 키페어 생성 시에만 PEM키가 자동으로 다운로드 됩니다.
  - PEM키에 대한 관리는 이용자 영역이며, 추가 다운로드는 불가하므로 관리 시 주의가 필요합니다.



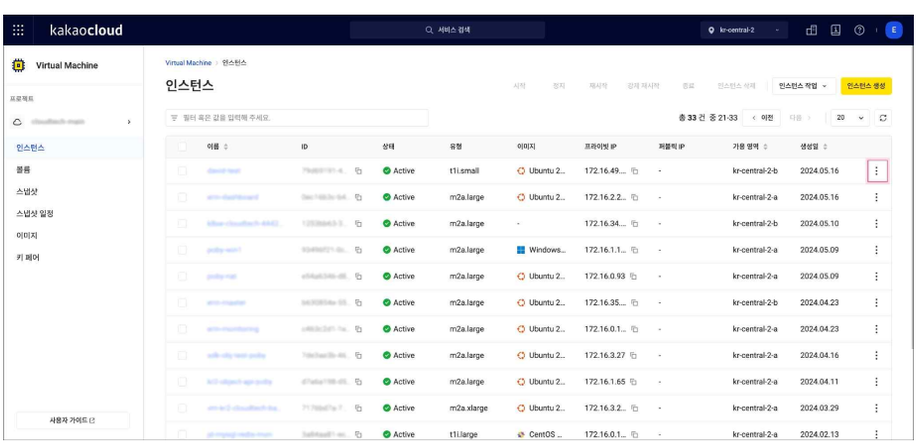
| 그림 1-5-3 | 최초 키 페어 생성

| 그림 1-5-4 | 최초 키 페어 생성 시 PEM Key 자동 다운로드

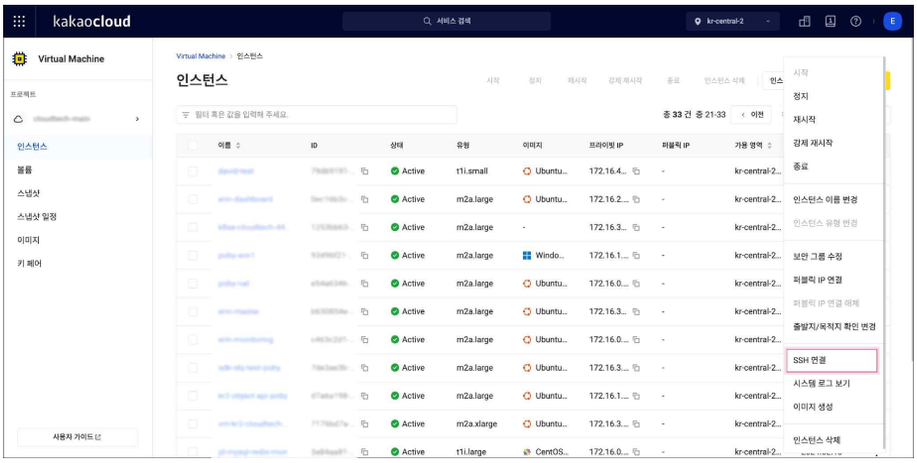
- 카카오클라우드에선 콘솔을 통해 이용자의 인스턴스에 직접 접속하는 방법은 제공하지 않습니다.
  - **(Console)** 'Dashboard' → 'Beyond Compute Service' → 'Virtual Machine' → '인스턴스"에서 해당되는 인스턴스의 확장 메뉴에서 SSH 연결 메뉴가 있으나, 해당 메뉴는 연결에 대한 가이드만 제공되고 직접 터미널 연결은 제공되지 않습니다.



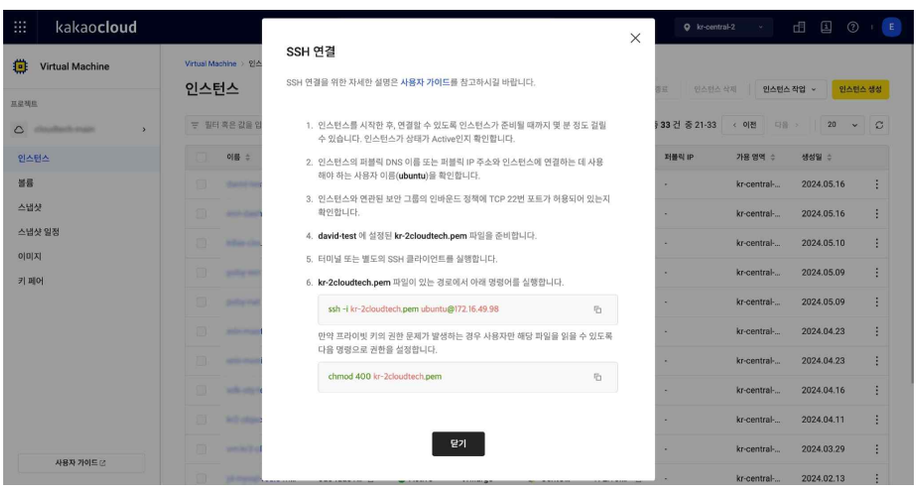
| 그림 1-5-5 | 카카오클라우드 콘솔 〉 Virtual Machine 서비스 이동



| 그림 1-5-6 | 인스턴스 더보기 아이콘 클릭



| 그림 1-5-7 | SSH 연결 클릭



| 그림 1-5-8 | SSH 연결 가이드 확인

4 참고 사항

- 카카오클라우드 인스턴스 생성 및 연결 가이드
- 카카오클라우드 키 페어 생성 및 관리 가이드

1 기준

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

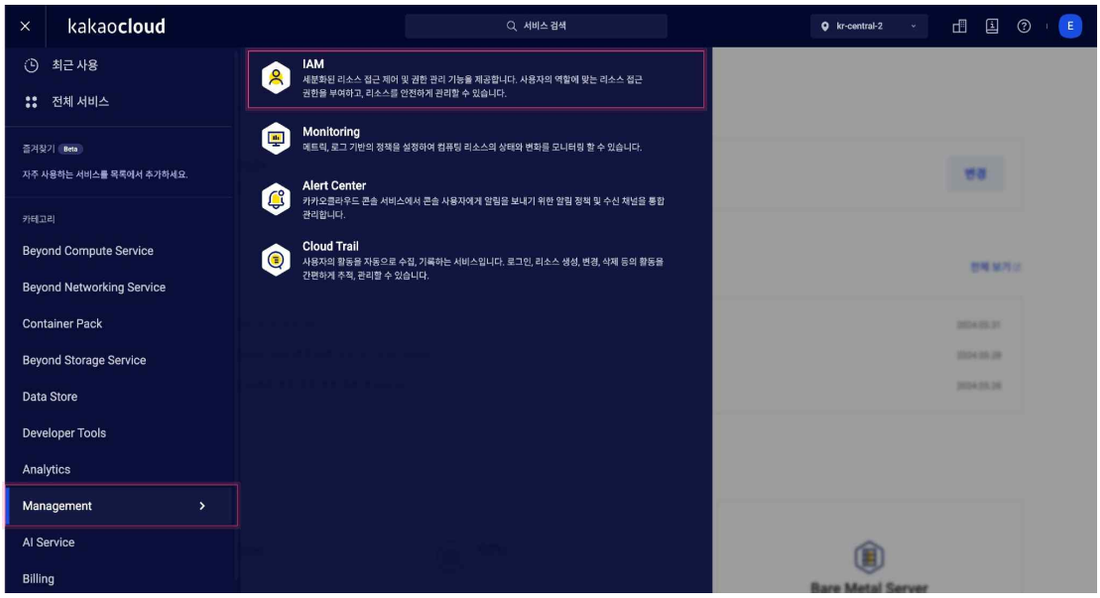
2 설명

- 이용자 직무 및 권한에 따른 가상자원 별 접근통제 방안(권한 설정 등)을 수립하여야 한다.
  - 예시
    1) 가상자원 종류별 접근통제 방안 수립 (ex. IAM을 통한 접근권한 관리)
       * 모든 가상자원에 접근 가능한 Role에 대해서는 최소 인원에 대해서만 부여

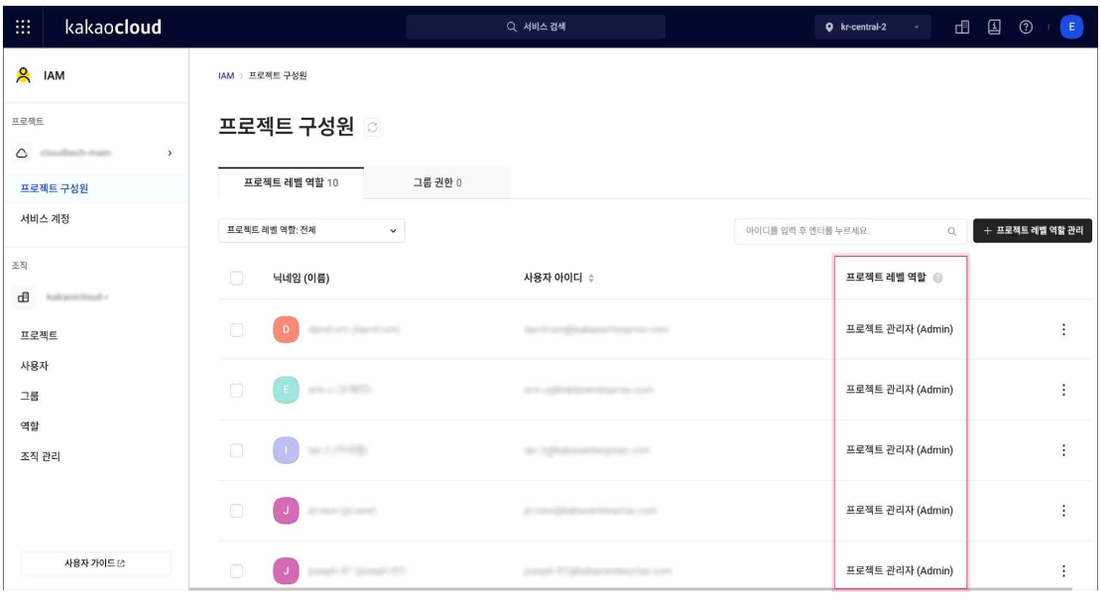
3 우수 사례

- 카카오클라우드는 조직, 프로젝트 단위로 논리적으로 공간을 분리하고 각 공간에 접근 가능한 계정을 분리하여 권한 설정을 할 수 있도록 기능을 제공합니다
- 상위 개념의 공간인 조직에는 조직소유자(owner), 조직관리자(admin), 조직리더(view) 등의 권한으로 구분. 조직소유자는 조직마다 1명만 존재하며, 권한 이양이 가능합니다.
- 프로젝트는 조직 하위에서 실질적인 자원을 생성하고 관리하는 공간으로, 관리자(Admin), 멤버(Member), 리더(Viewer) 권한을 설정할 수 있으며, 서비스별로 Object Storage 매니저(Manager)·뷰어(Viewer), Kubeflow 관리자(Admin), Alert Center 프로젝트 매니저(Manager)·뷰어(Viewer) 등의 역할도 추가할 수 있습니다.
- 가상자원 접근(SSH, RDP 등)에 대한 제어는 마켓플레이스 상품을 통해 이용할 수 있으며, 다양한 접근제어솔루션을 활용하여 유저 및 그룹별 접근통제 기능을 제공합니다.

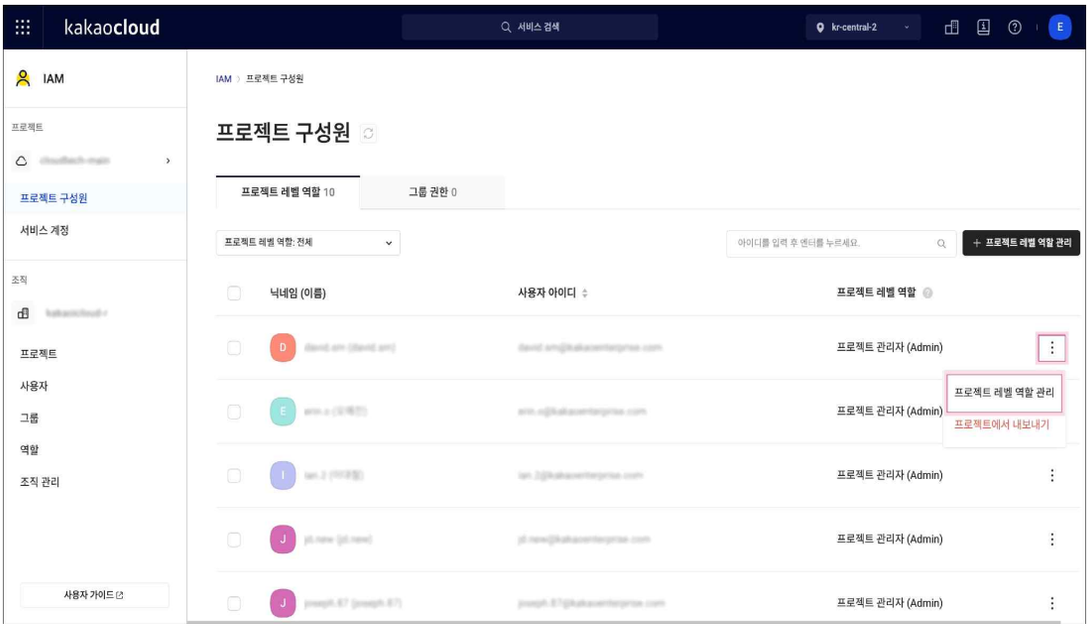
- 프로젝트 레벨에서의 가상자원 종류별 접근통제 방안 수립 (ex. IAM을 통한 접근권한 관리)
  - **(Console)** 'Dashboard' → 'Management' → 'IAM' → '프로젝트 구성원' 페이지에서 프로젝트 레벨 역할을 확인. 부적절하게 권한이 부여된 경우 역할 변경



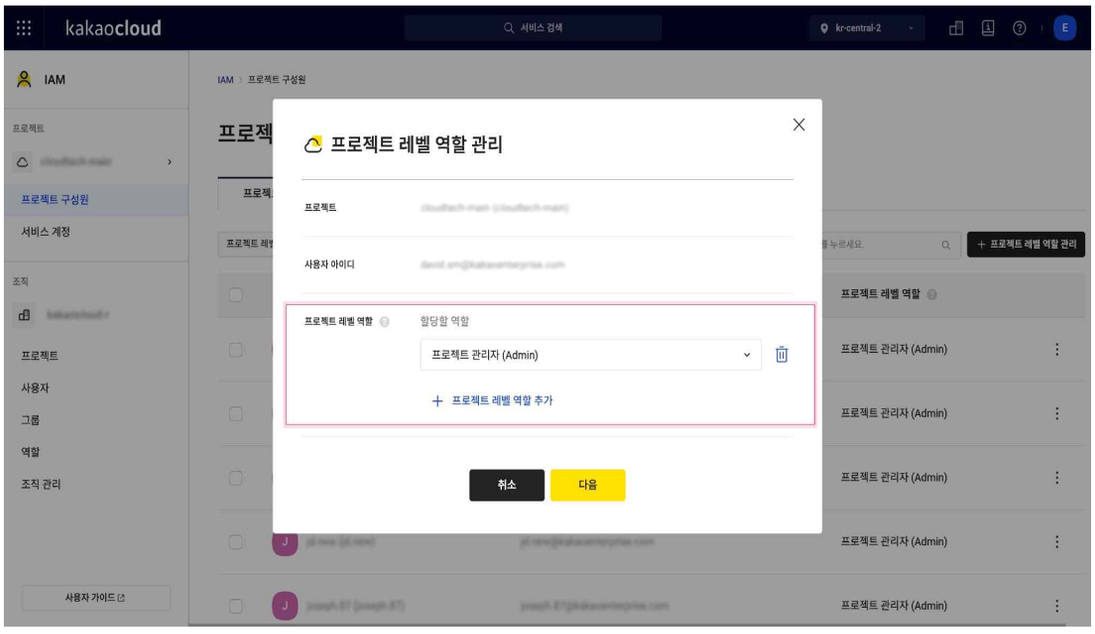
| 그림 1-6-1 | 카카오클라우드 콘솔 〉 IAM 서비스 이동



| 그림 1-6-2 | 프로젝트 구성원 중, 프로젝트 레벨 역할 확인

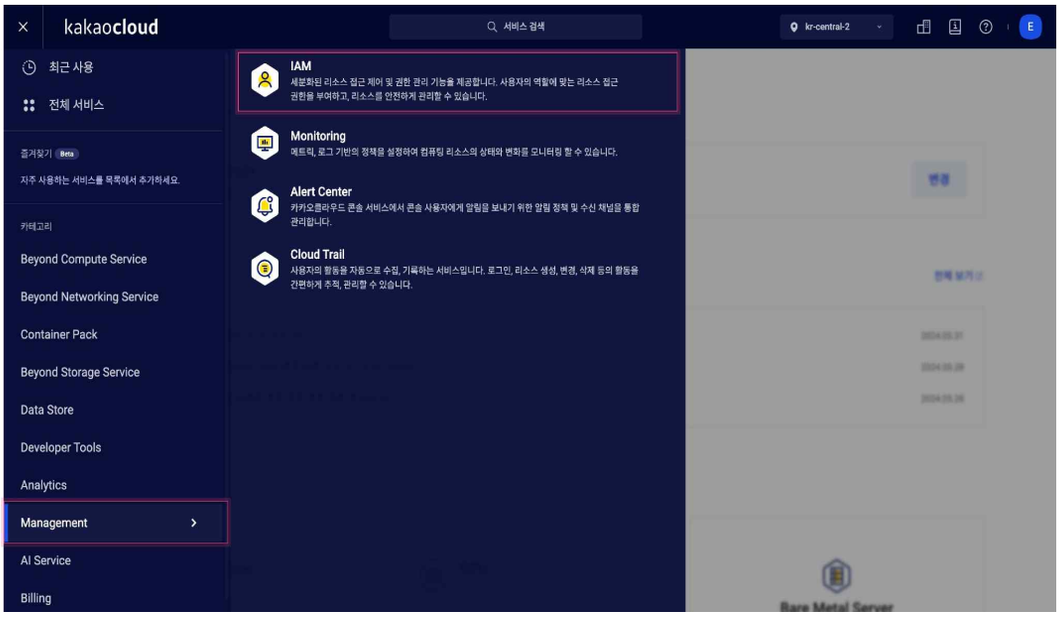


| 그림 1-6-3 | 부적절하게 권한이 부여된 경우 역할 변경

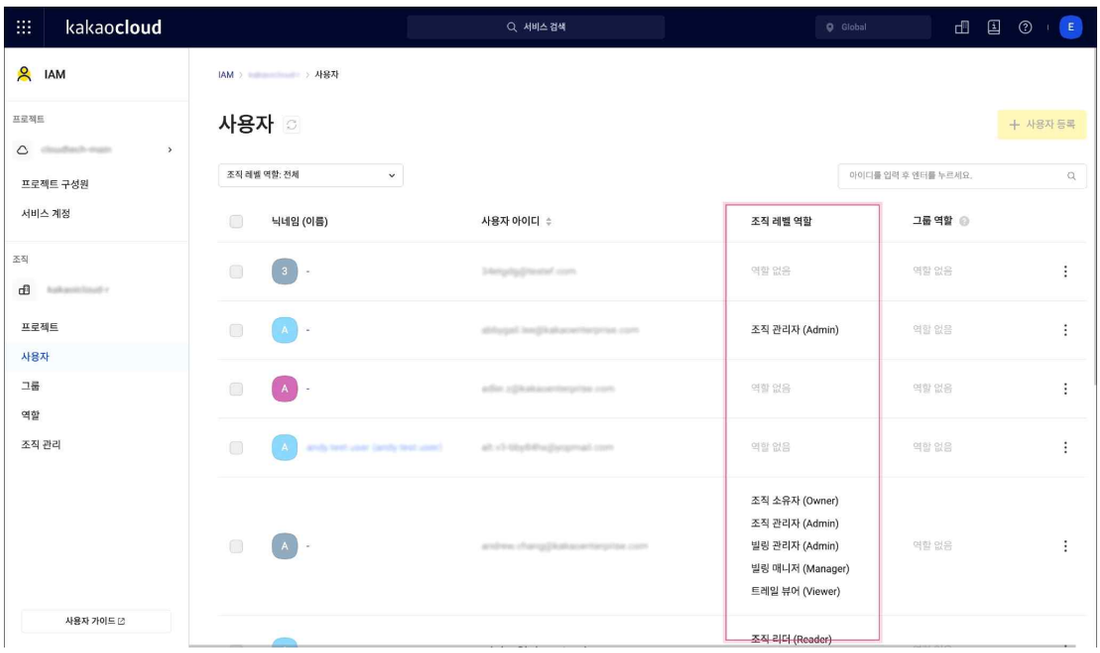


| 그림 1-6-4 | 프로젝트 레벨 역할 변경 모달

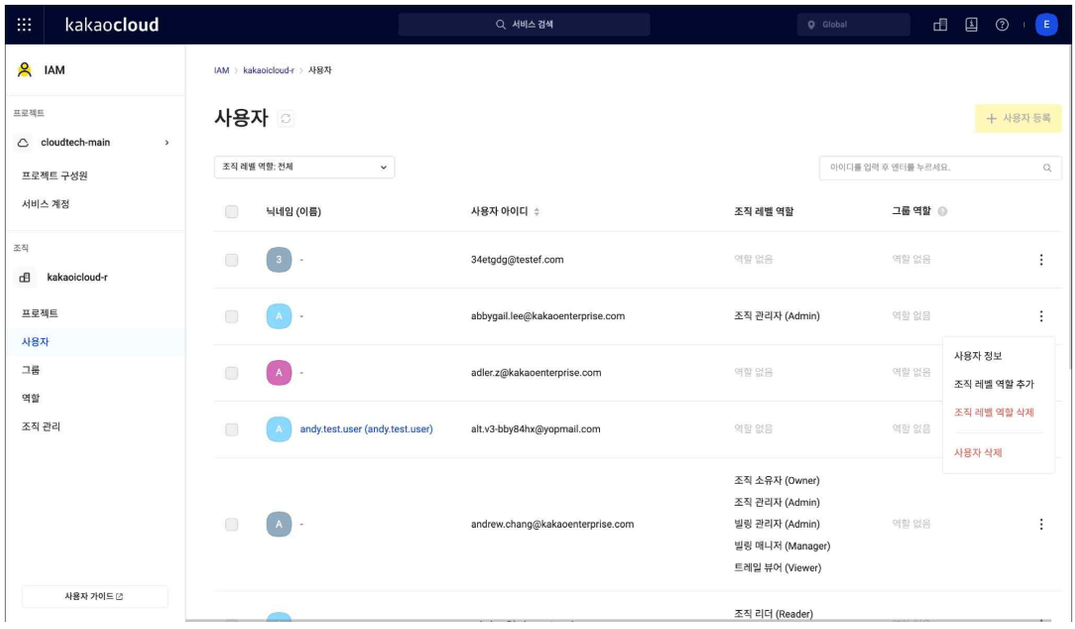
- 조직 레벨에서의 가상자원 종류별 접근통제 방안 수립 (ex. IAM을 통한 접근권한 관리)
  - **(Console)** 'Dashboard' → 'Management' → 'IAM' → '사용자' 페이지에서 조직 레벨 역할을 확인. 부적절하게 권한이 부여된 경우 역할



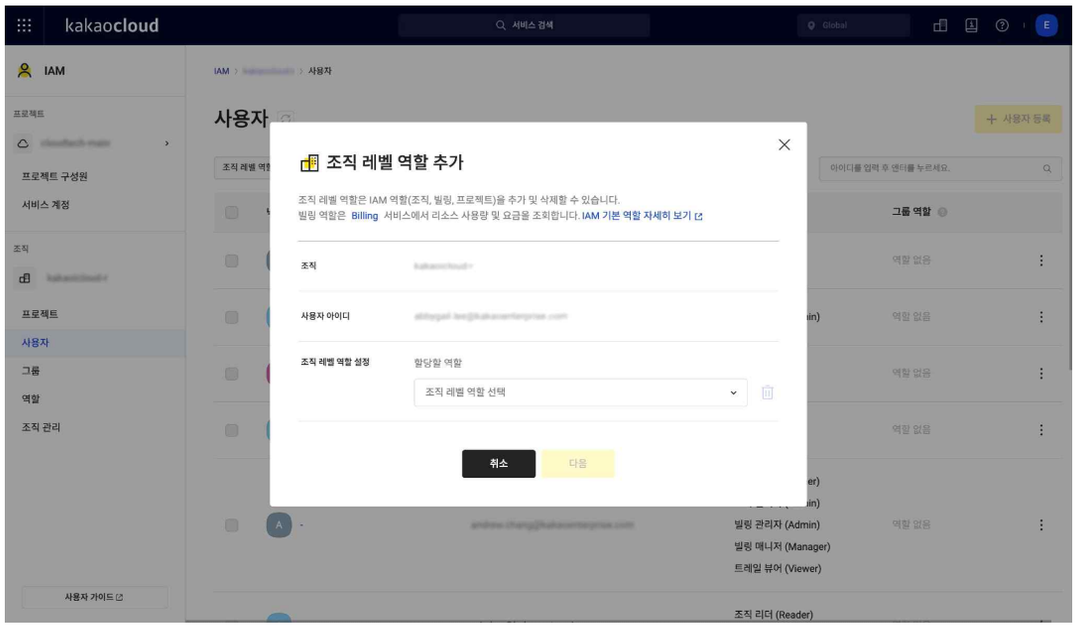
| 그림 1-6-5 | 카카오클라우드 콘솔 〉 IAM 서비스 이동



| 그림 1-6-6 | 조직 구성원 중, 조직 레벨 역할 확인



| 그림 1-6-7 | 부적절하게 권한이 부여된 경우 역할 변경



| 그림 1-6-8 | 조직 레벨 역할 변경 모달

4 참고 사항

- 카카오클라우드 IAM 역할 가이드
- 카카오클라우드 IAM 〉 프로젝트 레벨 역할 관리 가이드

1 기준

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

2 설명

- 이용자 가상자원 내 악성코드 통제방안을 수립하여야 한다.

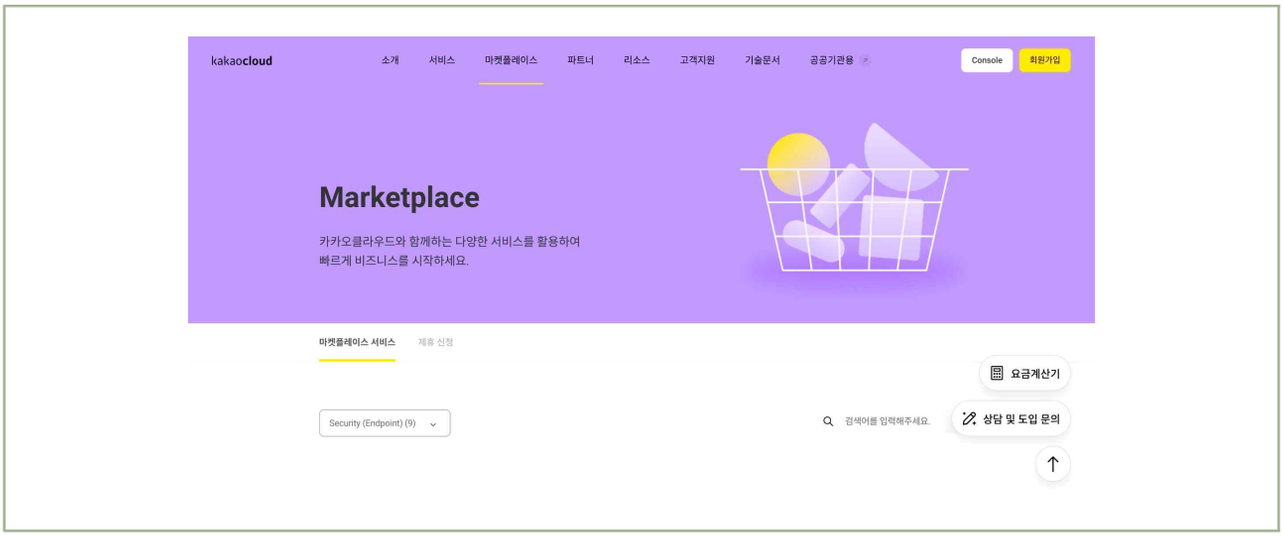
  - 예시

    1) 이용자가 보유하고 있는 악성코드 통제방안 수립(백신 등)
    2) 클라우드 사업자가 악성코드 통제방안 제공(백신 등)
    3) 백신 등 설치가 불가능한 환경인 경우 그 수준에 준하는 악성코드 통제방안 수립

3 우수 사례

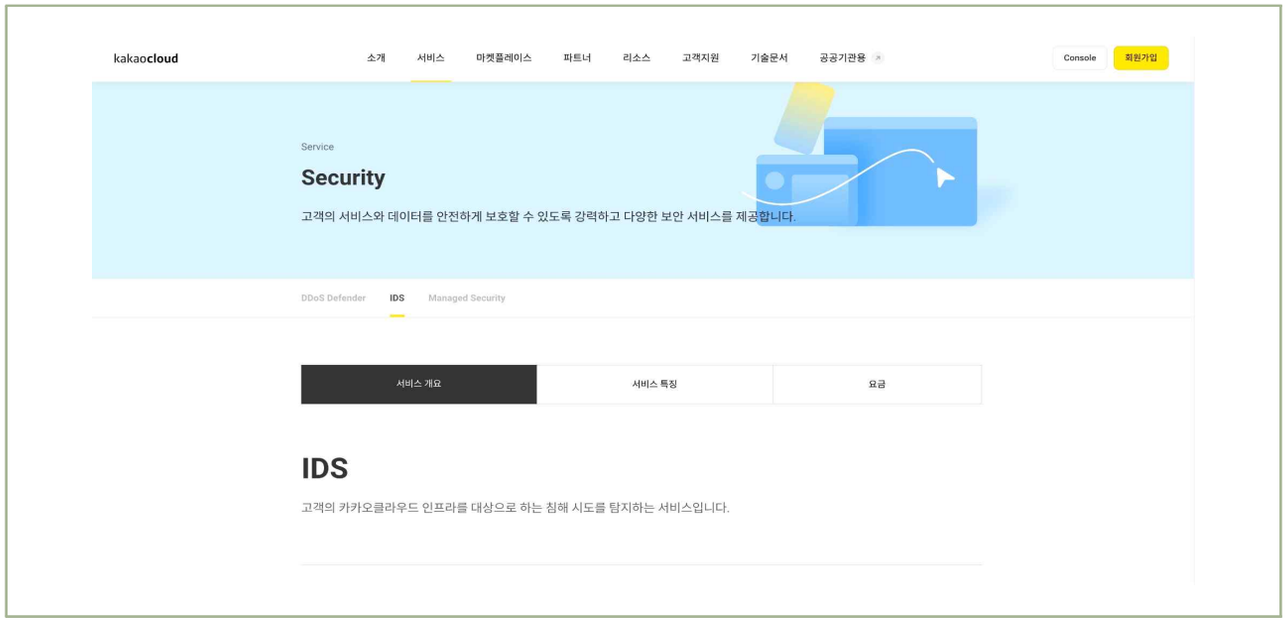
- 이용자가 보유하고 있는 악성코드 통제방안 수립

  - **(3rd-party 제품)** MarketPlace 상품 중 security(endpoint) 상품군에 해당하는 제품을 활용하여 악성코드 통제가 가능합니다.



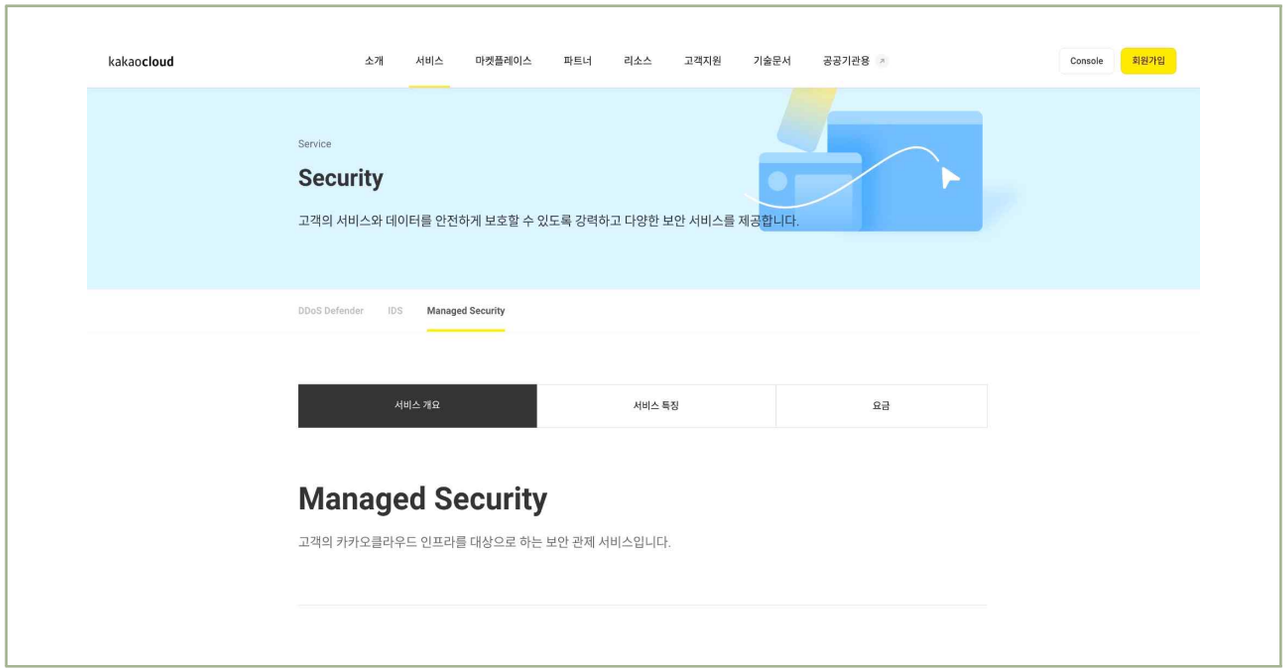
| 그림 1-7-1 | 카카오클라우드 마켓플레이스 상품 소개 페이지

- 클라우드 사업자가 악성코드 통제방안 제공
  - 카카오클라우드에서는 이용자의 안전한 인프라 관리를 위해 아래와 같은 보안서비스를 무료(Tier 1) / 유료(Tier 2)로 제공합니다.
    - 카카오클라우드 〉 Security 〉 IDS(침입탐지시스템)



| 그림 1-7-2 | 카카오클라우드 IDS 상품 소개 페이지

- 카카오클라우드 〉 Security 〉 Managed Security (보안관제)



| 그림 1-7-3 | 카카오클라우드 Managed Security 상품 소개 페이지

- 카카오클라우드에서는 정기적으로 공격시도 및 악성코드 탐지 패턴을 업데이트하며, 치명적인 위협에 대비한 비정기 업데이트를 수시로 진행하여 최신 공격 및 악성코드 탐지 서비스를 제공하며, 카카오클라우드 서비스를 이용하는 이용자에게 기본적인 보안 관제 서비스를 제공합니다. (서비스 등급별 통지 방식 및 전파 이벤트 대상 범위 상이함)

안녕하세요. 카카오엔터프라이즈 보안관제팀 입니다.

다음과 같이 [redacted]에서 외부로 암호화폐 채굴하기 위한 통신이 확인되고 있습니다.
해당 내용에 대한 분석보고서 보내드리오니 참고 하시기 바랍니다.

KC 보안관제 이벤트			
고 객 사	[redacted]		
탐 지 명	[redacted]		
탐 지 룰	[redacted]_Malware_Alert		
탐지 일시	[redacted]	위험 등급	MEDIUM
티켓 번호	[redacted]		
출발지 IP	[redacted]	출발지 PORT	[redacted]
목적지 IP	[redacted]	목적지 PORT	[redacted]
탐지 장비	IDS		
이벤트 정보	[redacted]-hacktool_Monero_Miner_[redacted] [redacted]-hacktool_Cryptocurrency_miner_Connection.1[redacted] 탐지근거 : hacktool Monero Miner -[redacted] [취약점 설명] - "[redacted]-hacktool_Monero_Miner"는 Monero 암호화폐를 채굴하기 위해 시스템 리소스를 사용하는 악성코드입니다. 이 악성코드는 주로 이메일 첨부 파일이나 피싱 링크를 통해 유포됩니다. 한번 시스템에 침입하면, File-hacktool_Monero_Miner는 시스템의 CPU, GPU, 메모리 등을 사용하여 Monero를 채굴합니다. 이로 인해 시스템 성능이 저하될 수 있습니다. [영향도 분석 결과] - [redacted]. 악성코드채굴 소프트웨어를 통한 채굴 활동 확인되며, 추가 공격 예방을 위해서 [redacted]차단하였습니다.		
공격 구문	Packet: [redacted]		
조치 및 권고	[조치 사항] - 추가 공격에 대비하여 공격자 IP 차단 진행 [권고 사항] - 보안 소프트웨어 업데이트 - 의심스러운 프로세스 종료, 시스템 백업 - 비인가 불특정다수 외부로의 접근을 제한하기 위해 Security Group 강화 권고 - 임시 폴더 내 악성 의심 파일 제거 - 작업 스케줄러 내 미사용 또는 악성 의심 작업 제거 - 백신 정밀 검사 권고		
kakao cloud			

| 그림 1-7-4 | Tier 2 대상 - 카카오클라우드 IDS/Managed Service 이용자 통지 메일 샘플

4 참고 사항

- 카카오클라우드 마켓플레이스 상품 안내
- 카카오클라우드 Security(IDS) 상품 안내
- 카카오클라우드 Security(Managed Security) 상품 안내

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 프라이빗 IP 주소 할당 및 관리
2.6. 네트워크(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*에 따른 네트워크를 구성하여야 한다.** *** 개발, 운영, 업무 등**

2 설명

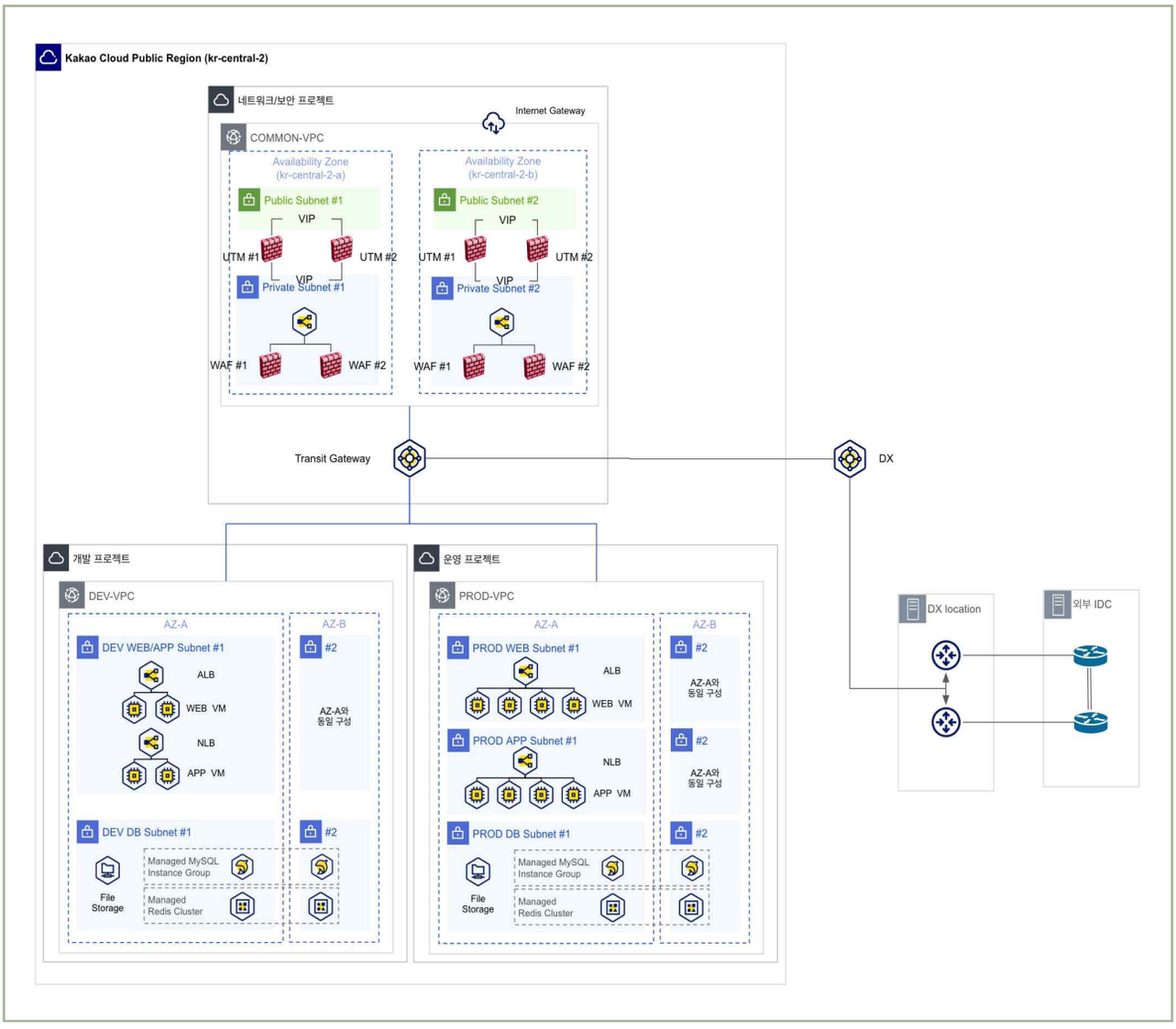
- 클라우드 환경 내 업무 목적(개발, 운영, 업무 등)에 따른 네트워크 구성 및 네트워크 간 접근 통제 방안을 수립하여야 한다.

  - 예시

    1) VPC 등 네트워크 관련 기능을 통한 네트워크 구성 및 통제
    2) 보안그룹(Security group)의 기능을 통한 네트워크 구성 및 통제(인/아웃바운드 통제 등)

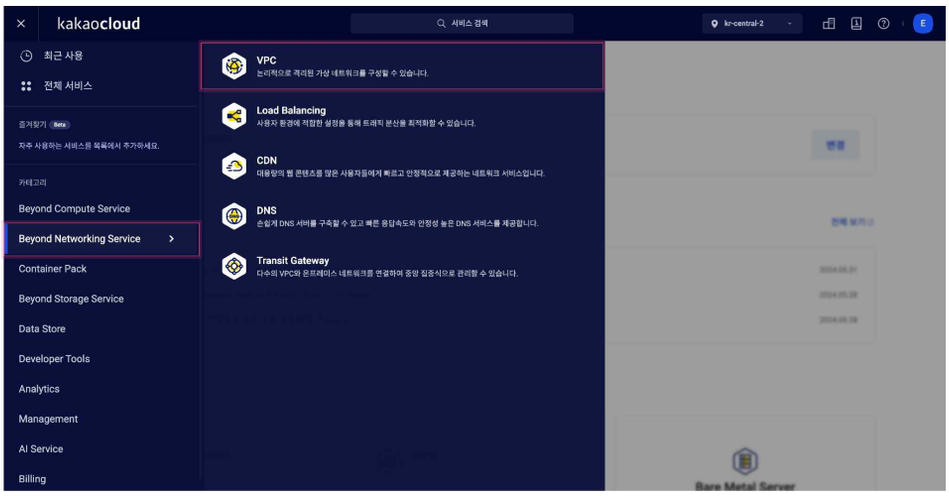
3 우수 사례

- 업무 목적에 따른 네트워크 구성 예시

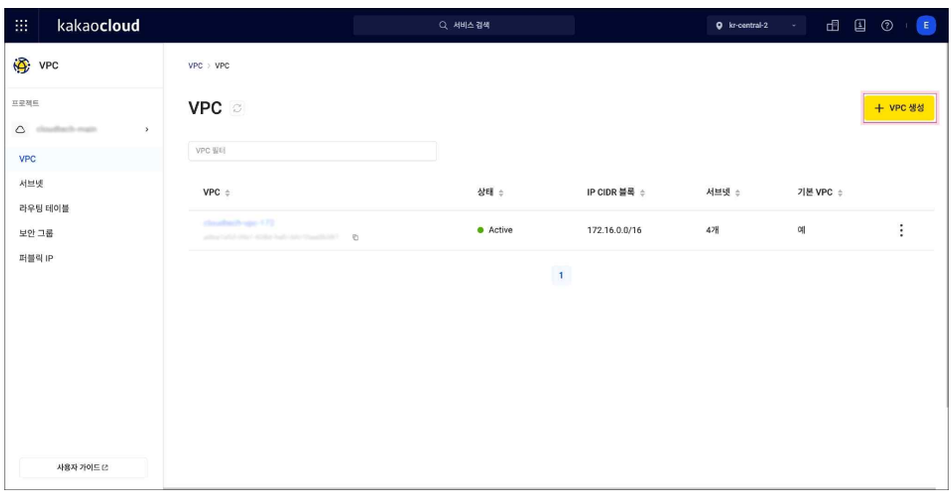


| 그림 2-1-1 | 카카오클라우드를 활용한 네트워크 구성도

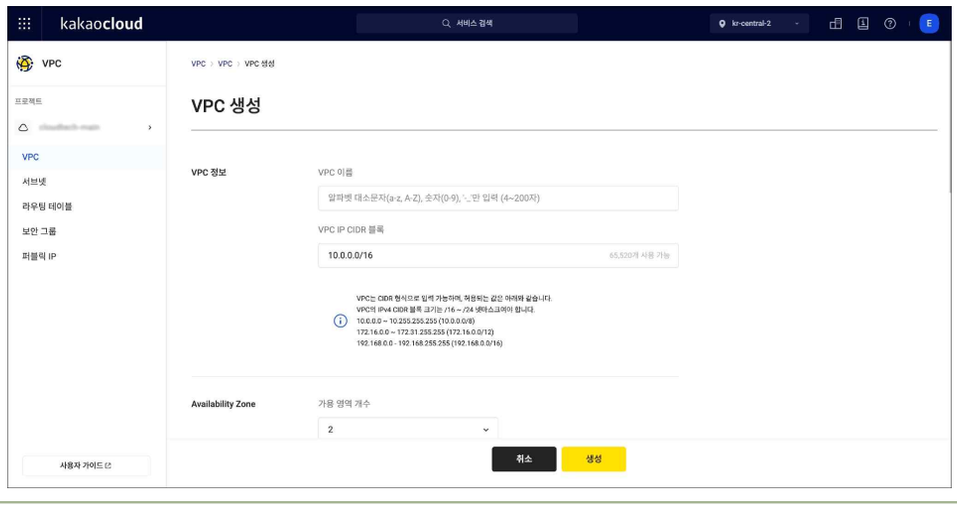
- VPC 등 네트워크 관련 기능을 통한 네트워크 구성 및 통제
  - 업무 목적에 따라 하나의 프로젝트에 여러 개의 VPC를 구성합니다. 예를 들어 네트워크/보안을 위한 VPC, 개발 환경용 VPC, 운영 환경용 VPC를 각각 생성하여 목적에 맞게 네트워크를 분리 구성합니다.
  - (Console) 'Dashboard' → 'VPC' → 'VPC 생성' 기능을 통해 업무 목적에 따라 여러 VPC를 생성합니다.



| 그림 2-1-2 | 카카오클라우드 콘솔 〉 VPC 서비스 이동

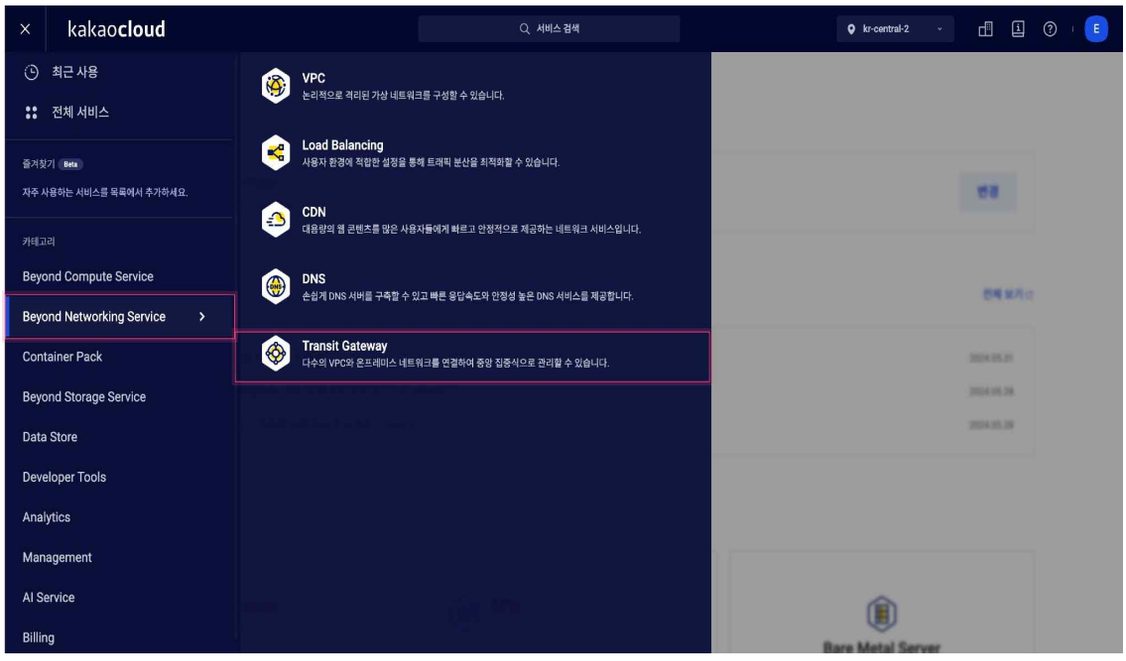


| 그림 2-1-3 | VPC 생성 버튼 클릭

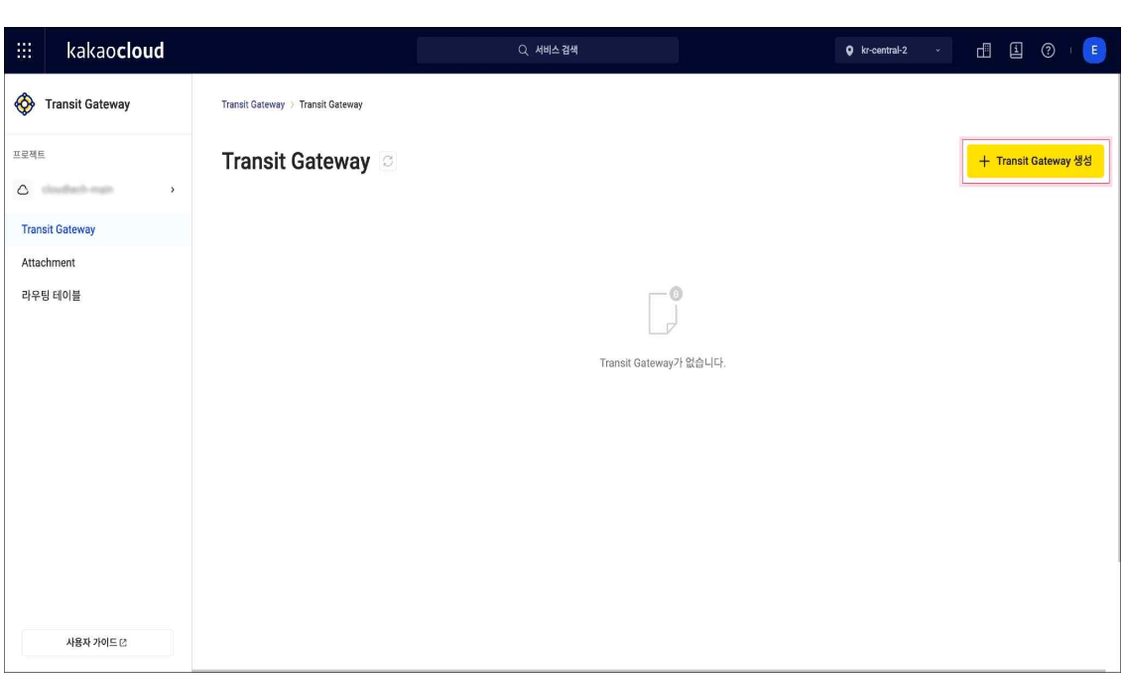


| 그림 2-1-4 | VPC 생성 페이지

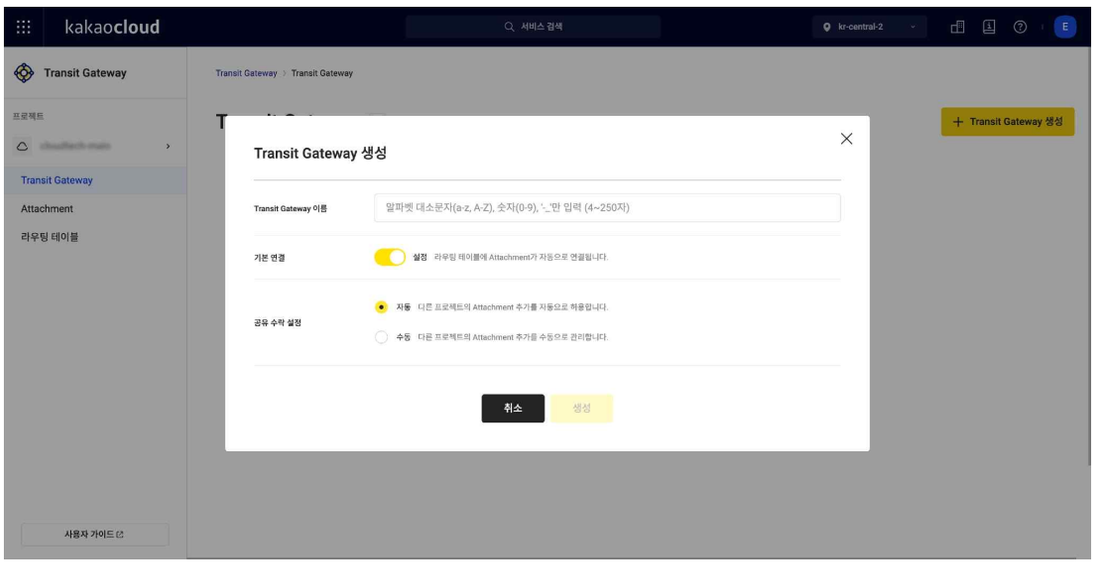
- **(Console)** 'Dashboard' → 'Transit Gateway' → 'Transit Gateway 생성' 기능을 통해 Transit Gateway를 생성하여 서로 간에 통신이 필요한 VPC를 연결합니다.



| 그림 2-1-5 | 카카오클라우드 콘솔 〉 Transit Gateway 서비스 이동

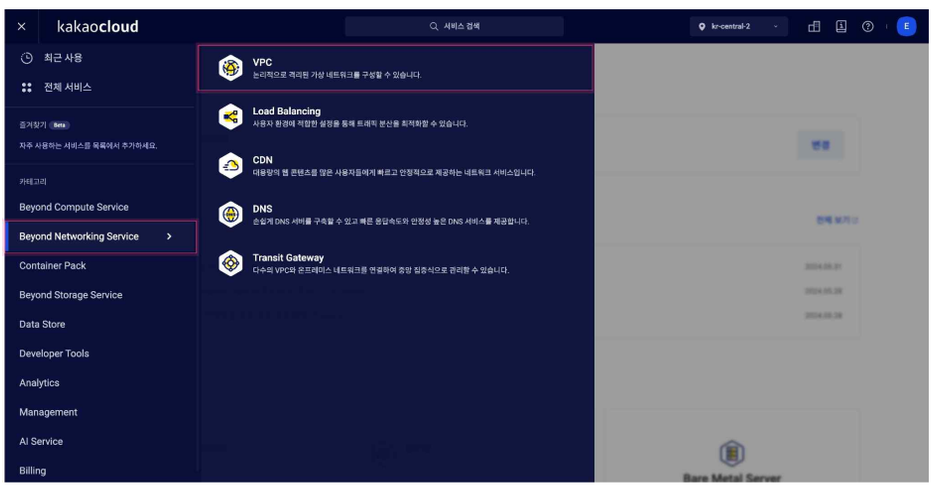


| 그림 2-1-6 | Transit Gateway 생성 버튼 클릭

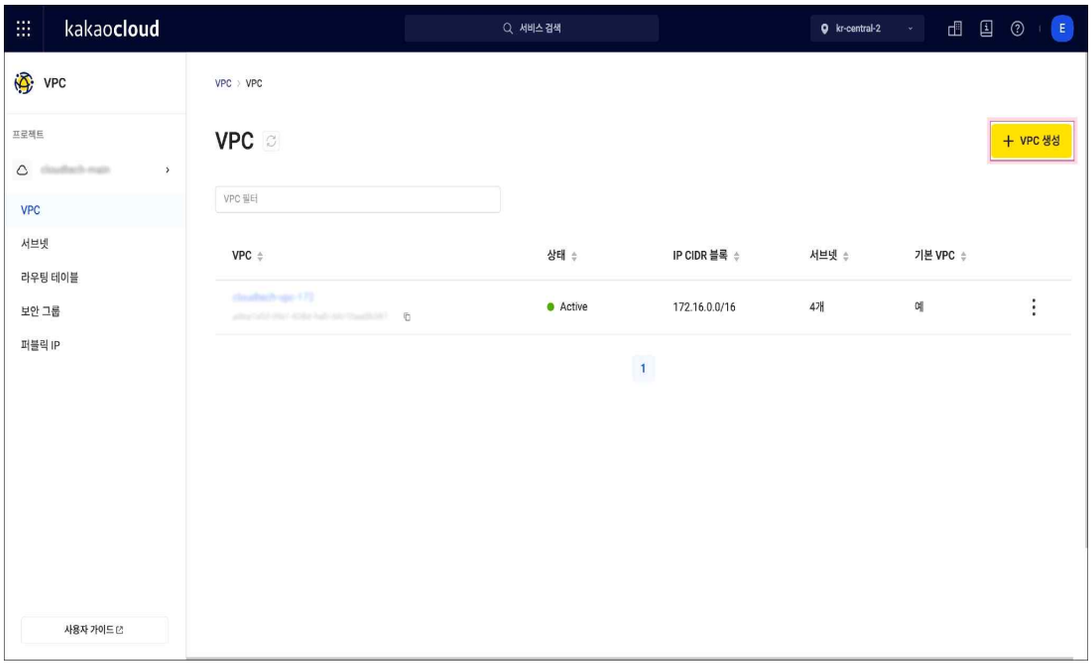


| 그림 2-1-7 | Transit Gateway 생성 페이지

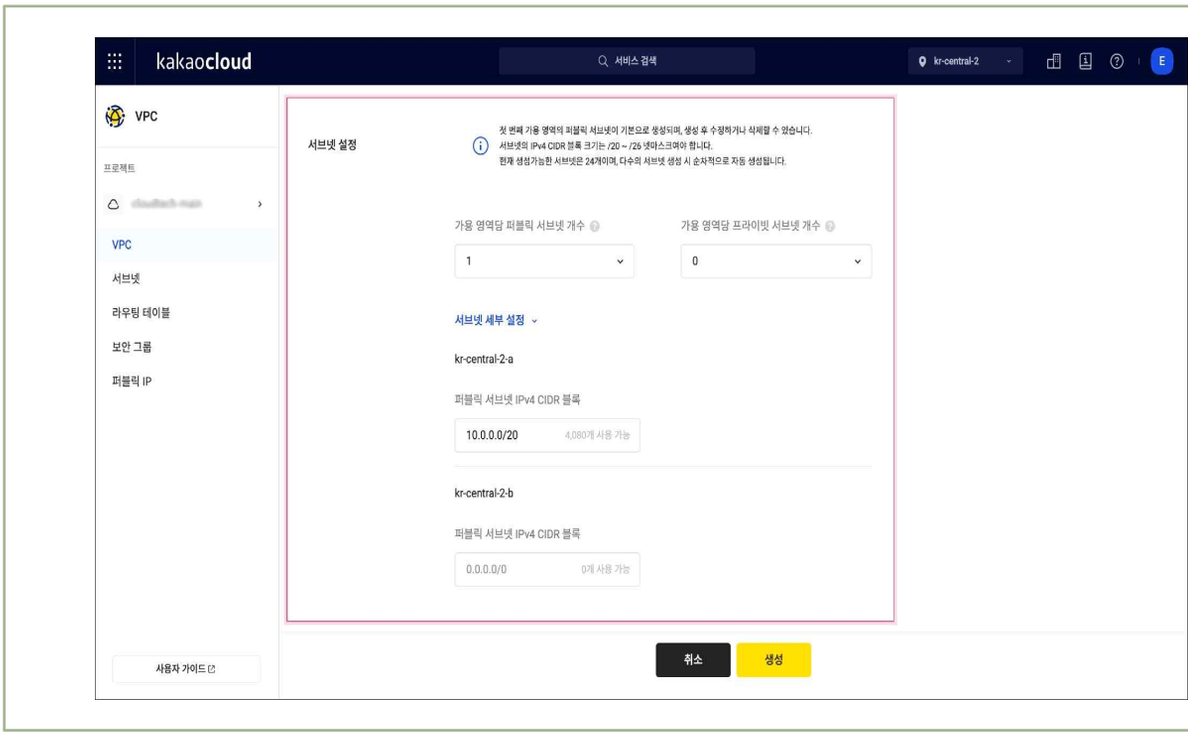
- 보안그룹(Security group)의 기능을 통한 네트워크 구성 및 통제(인/아웃바운드 통제 등)
  - 하나의 VPC에서도 업무 목적에 따라 Subnet을 구분하여 구성할 수 있습니다.
  - (Console) 'Dashboard' → 'VPC' → 'VPC 생성' 페이지에서 가용 영역당 퍼블릭 서브넷 개수와 가용 영역당 프라이빗 서브넷 개수를 설정하여 업무 목적에 따라 외부와 통신해야 할 경우 퍼블릭 서브넷을 사용하고, 그렇지 않을 경우 프라이빗 서브넷을 사용합니다.



| 그림 2-1-8 | 카카오클라우드 콘솔 〉 VPC 서비스 이동

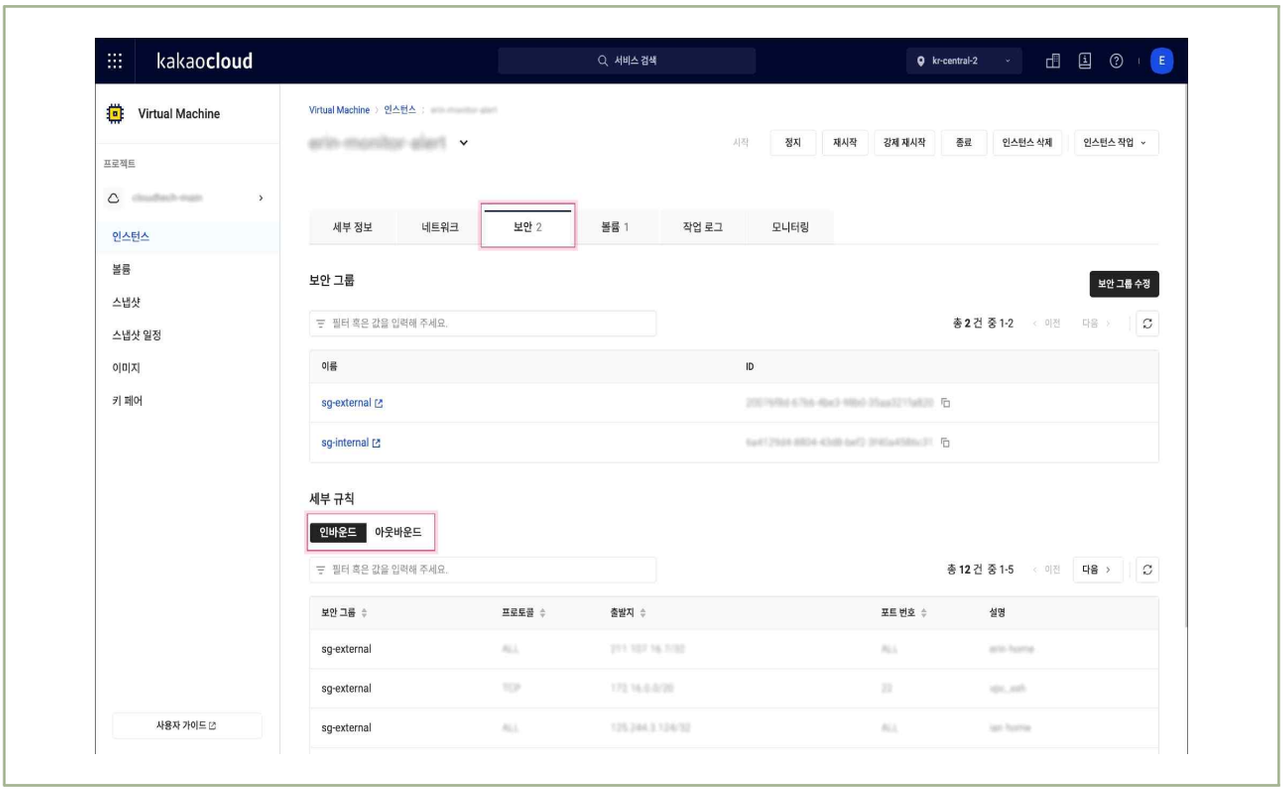


| 그림 2-1-9 | VPC 생성 버튼 클릭

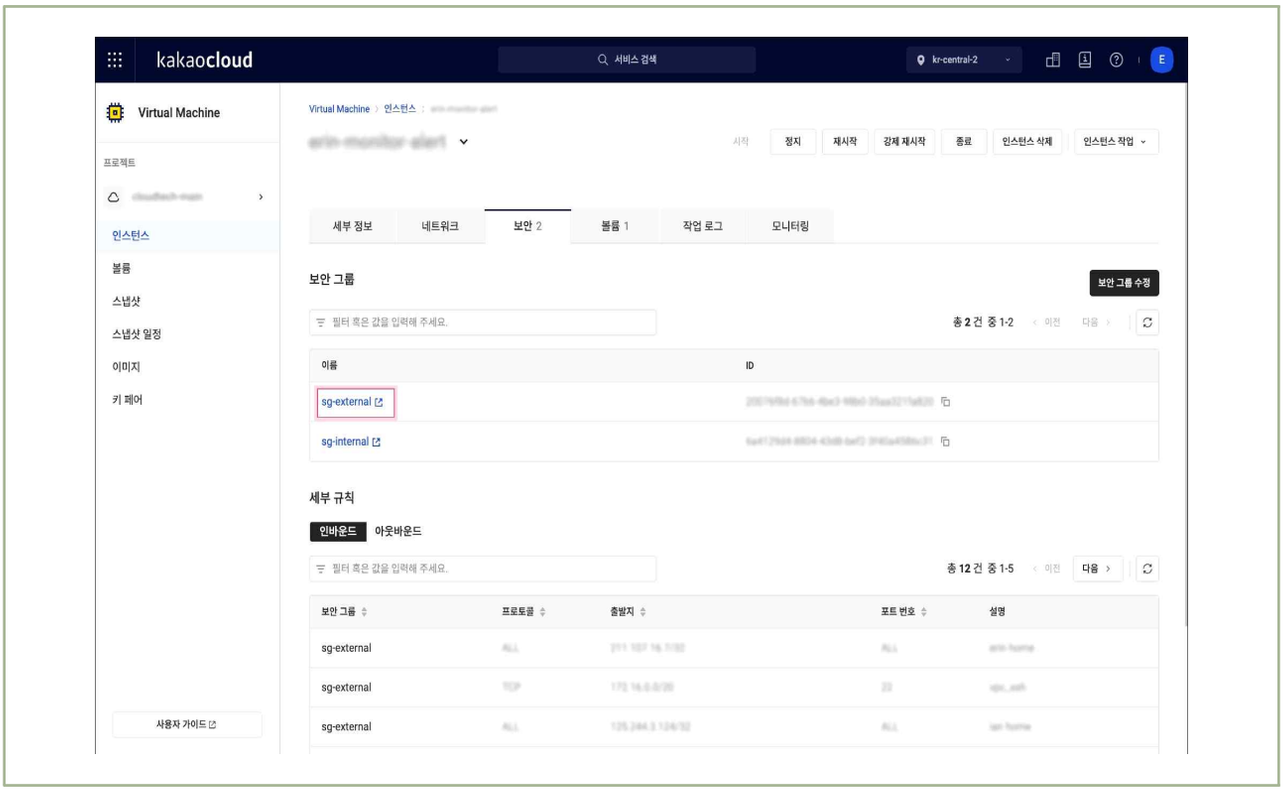


| 그림 2-1-10 | VPC 생성 시, 가용영역 당 퍼블릭과 프라이빗 서브넷 설정 가능

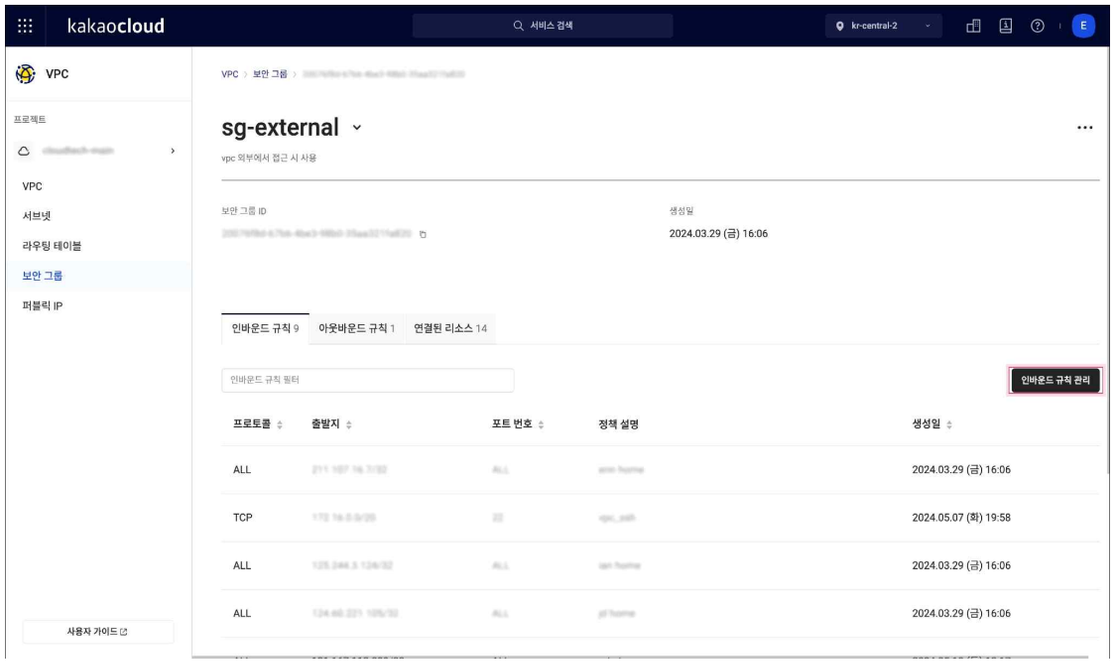
- 서브넷 간 접근 통제는 인스턴스에 연결된 보안 그룹(Security Group)의 인바운드 규칙을 설정합니다.



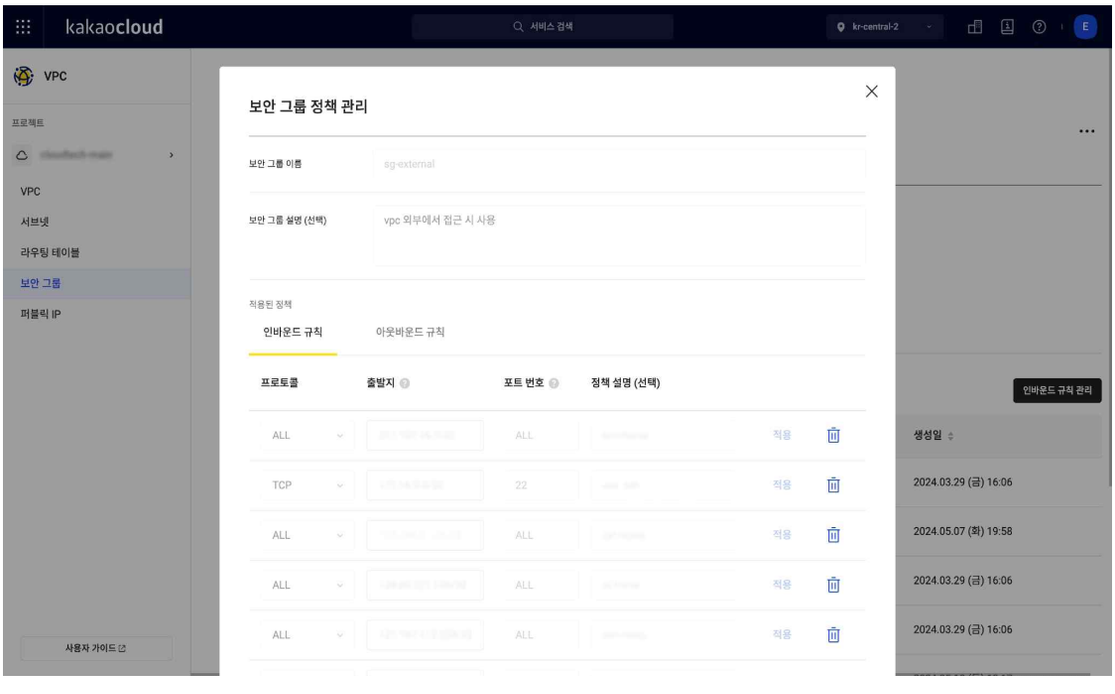
| 그림 2-1-11 | 인스턴스 상세페이지에서 인바운드 규칙 확인



| 그림 2-1-12 | 인바운드 규칙 수정이 필요할 경우, 해당 보안 그룹 클릭



| 그림 2-1-13 | 보안 그룹 상세 페이지에서 인바운드 규칙 관리 클릭



| 그림 2-1-14 | 인바운드 규칙 삭제 및 추가

4 참고 사항

- 카카오클라우드 VPC 생성 및 관리 가이드
- 카카오클라우드 Transit Gateway 생성 및 관리 가이드
- 카카오클라우드 서브넷 생성 및 관리 가이드
- 보안 그룹 생성 및 관리 가이드

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 합니다.

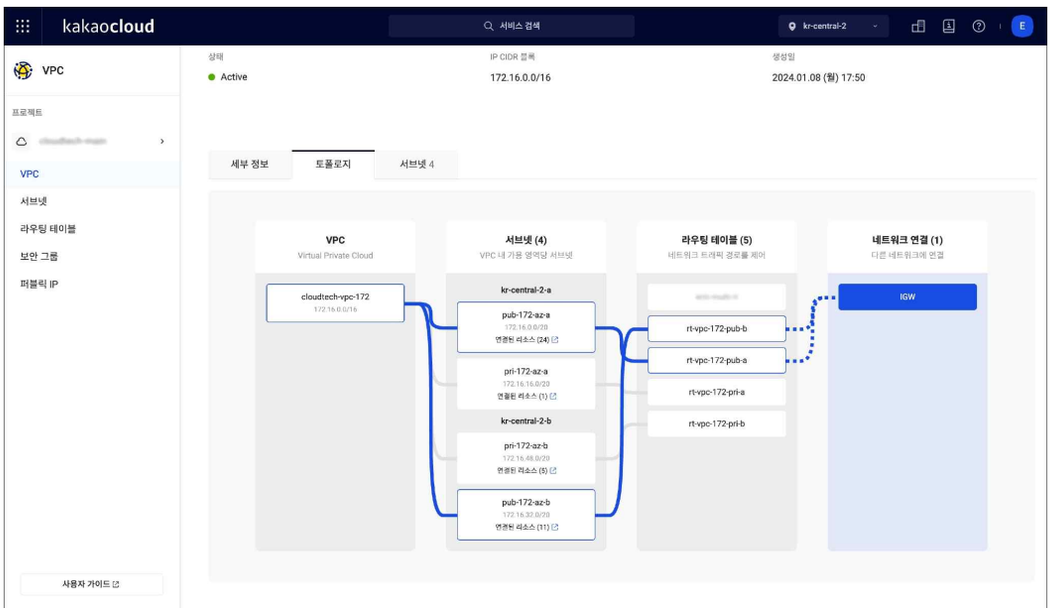
  - 예시

    1) VPC 등 네트워크 관련 기능을 통한 네트워크 접근 통제(인터넷망 등)
    2) 보안그룹(Security group)의 기능을 통한 네트워크 구성(인/아웃바운드 통제 등)
    3) 내부망으로 구현한 가상자원(서버, 데이터베이스 등)에 퍼블릭 IP 미 할당
    4) 방화벽 서비스를 통한 IP 통제 등

3 우수 사례

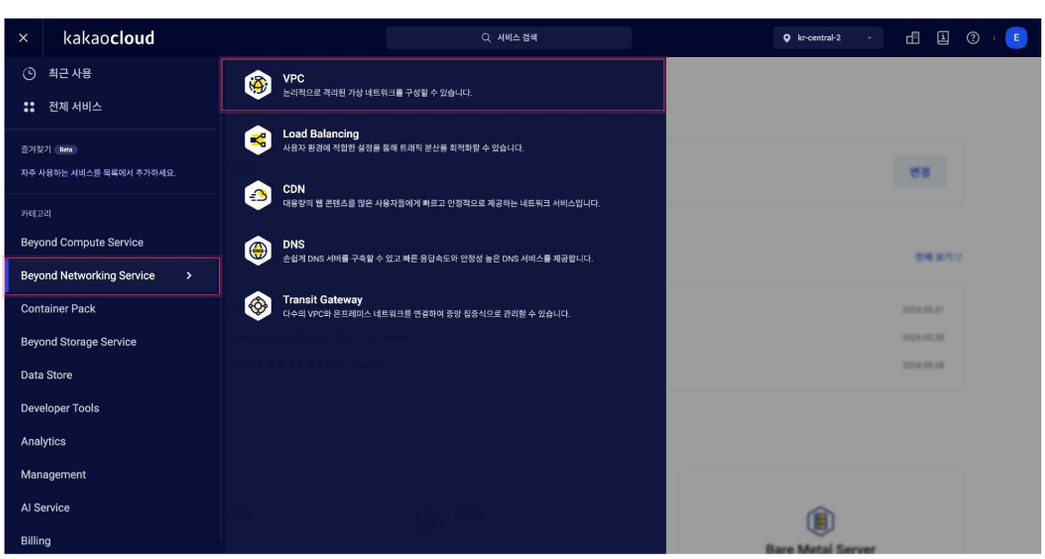
- VPC 등 네트워크 관련 기능을 통한 네트워크 접근 통제 (인터넷망 등)

  - 카카오클라우드에서는 하나의 VPC 내에 Internet Gateway 가 존재합니다.
  - 라우팅 테이블에 Internet Gateway를 대상(target)으로 하는 라우팅을 설정하고, 해당 라우팅 테이블에 서브넷을 연결하면 연결된 서브넷은 퍼블릭 서브넷이 됩니다.

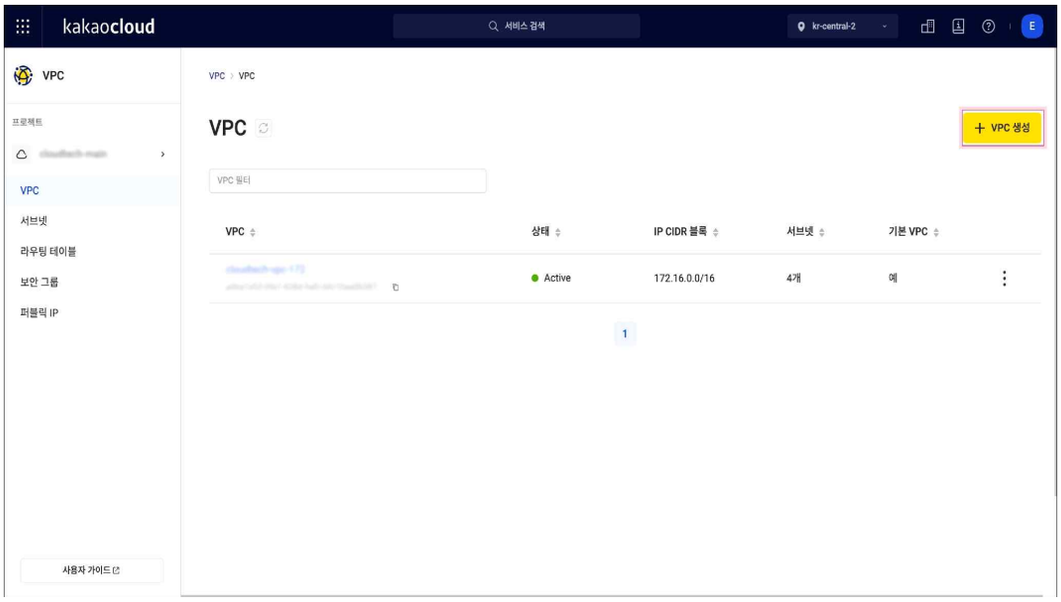


| 그림 2-2-1 | Internet Gateway 연결된 퍼블릭 서브넷

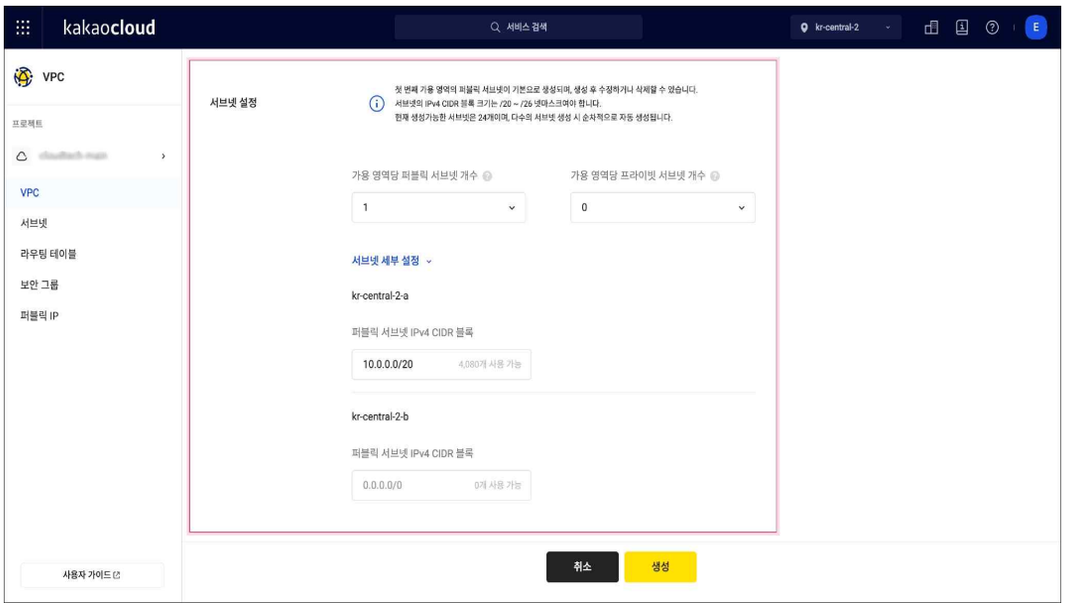
- 하나의 서브넷은 하나의 라우팅 테이블을 가질 수 있고, 하나의 라우팅 테이블은 여러 서브넷에 연결될 수 있습니다. (서브넷 : 라우팅 테이블 = N : 1 관계)
- **(Console)** 'Dashboard' → 'Beyond Networking Service' → 'VPC' → 'VPC 생성' 페이지에서 가용 영역당 퍼블릭 서브넷 개수와 가용 영역당 프라이빗 서브넷 개수를 설정하여 업무 목적에 따라 외부와 통신해야 할 경우 퍼블릭 서브넷을 사용하고, 그렇지 않을 경우 프라이빗 서브넷을 사용합니다.



| 그림 2-2-2 | 카카오클라우드 콘솔 〉 VPC 서비스 이동



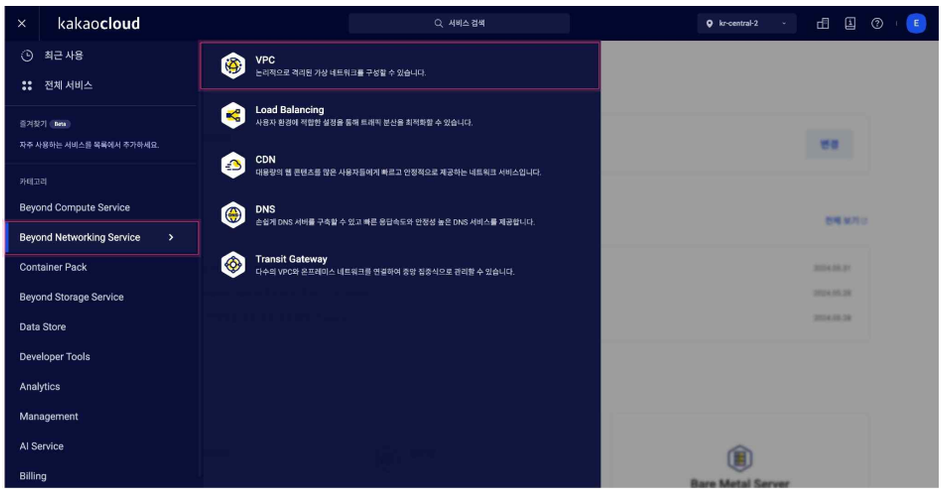
| 그림 2-2-3 | VPC 생성 버튼 클릭



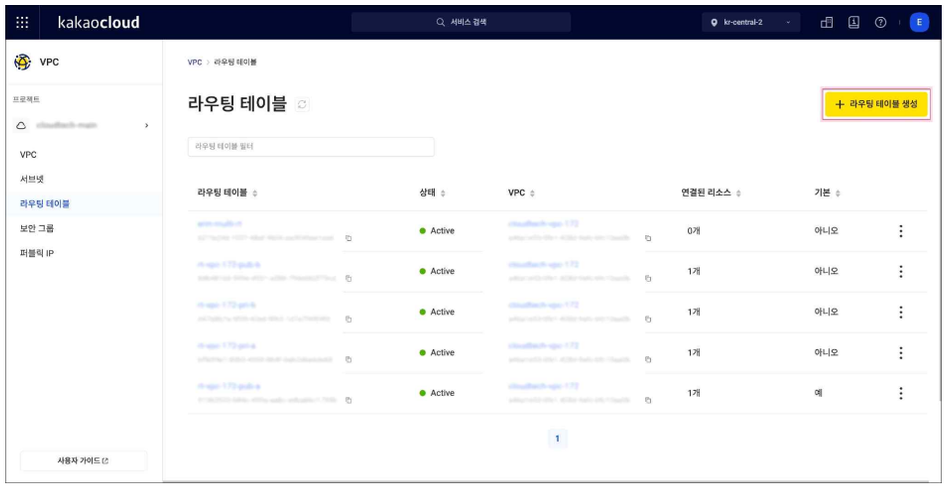
| 그림 2-2-4 | VPC 생성 시, 가용영역 당 퍼블릭과 프라이빗 서브넷 설정 가능

* 단, 서브넷 간 접근 통제는 보안 그룹(Security Group) 설정을 통해 접근 통제가 가능합니다.

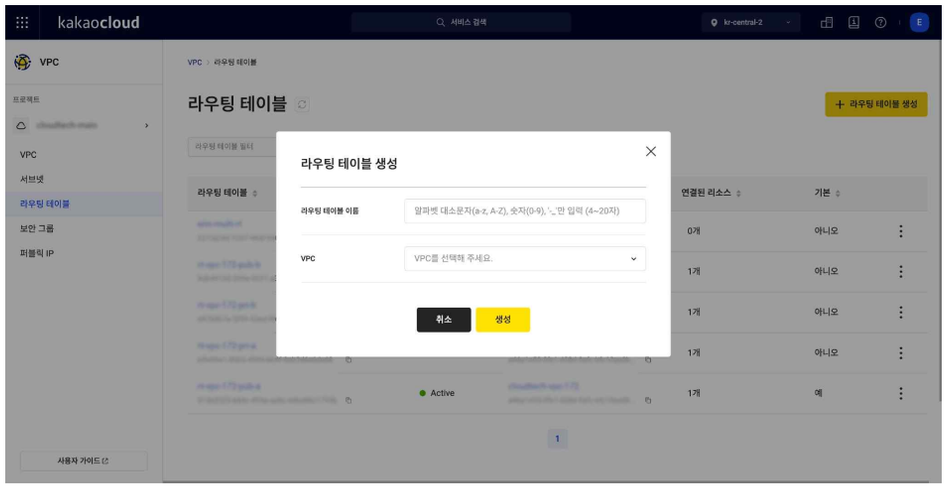
또는, **(Console)** 'Dashboard' → 'Beyond Networking Service' → 'VPC' → '라우팅 테이블' → '라우팅 테이블 생성' 기능을 통해 새로 라우팅 테이블을 생성하고, 생성된 라우팅 테이블을 프라이빗 서브넷 목적으로 사용할 서브넷에 연결하면 해당 서브넷은 인터넷과 통신이 안 되는 프라이빗 서브넷이 됩니다.



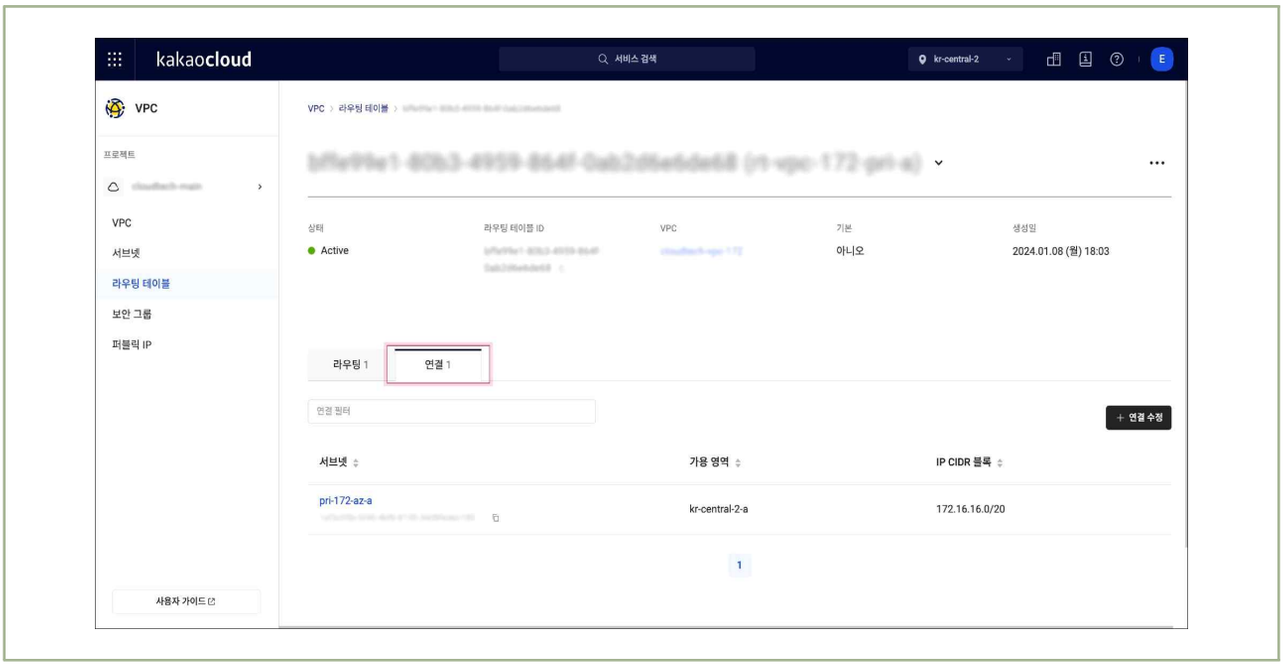
| 그림 2-2-5 | 카카오클라우드 콘솔 〉 Beyond Networking Service 〉 VPC 서비스 이동



| 그림 2-2-6 | 라우팅 테이블 〉 라우팅 테이블 생성 버튼 클릭

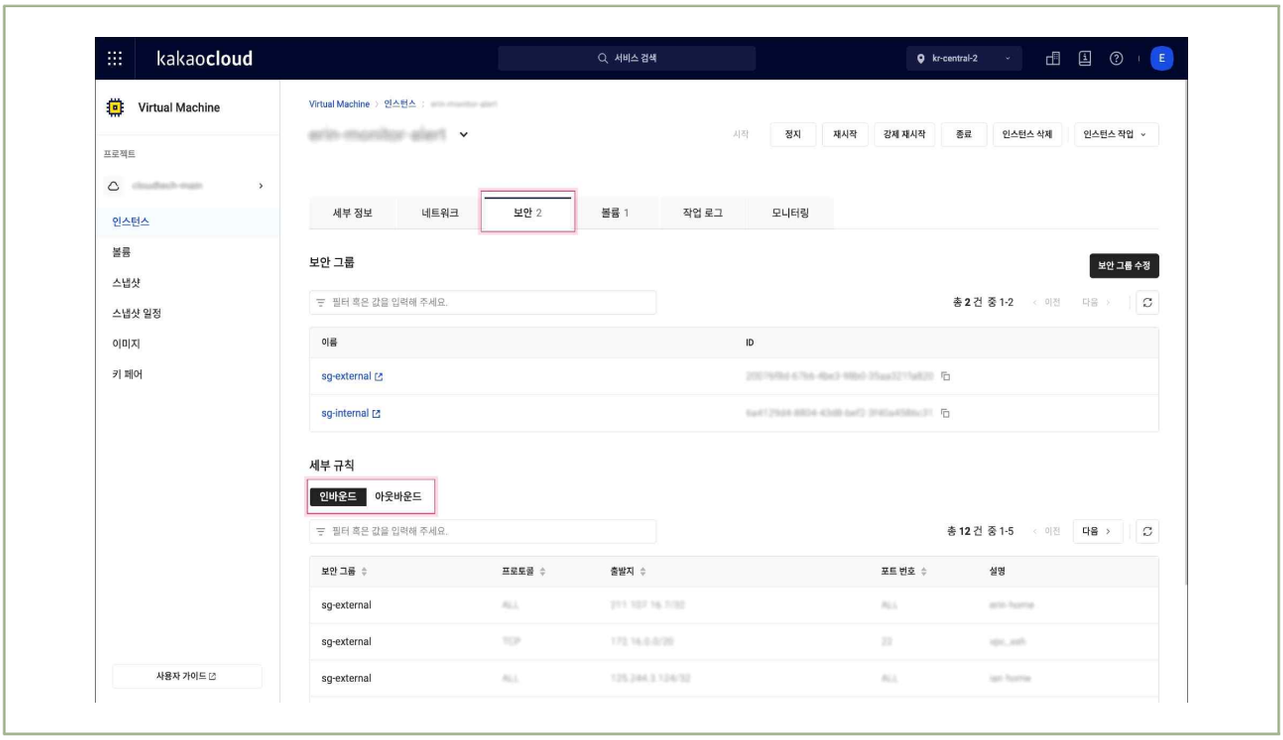


| 그림 2-2-7 | 라우팅 테이블 생성 모달

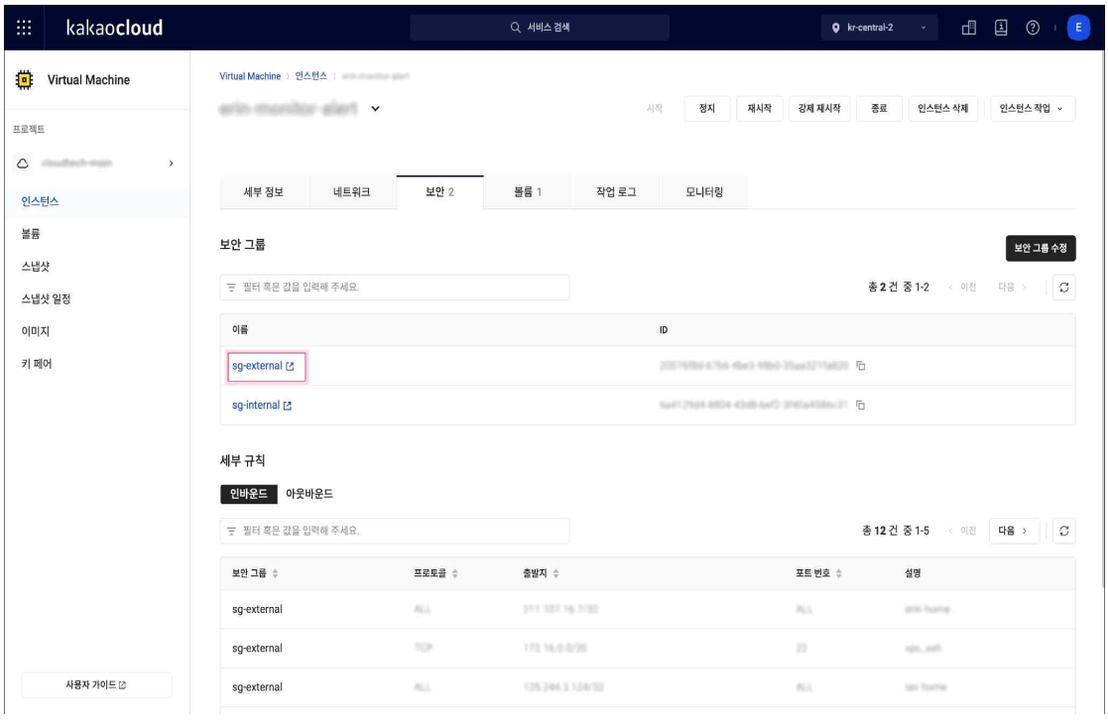


| 그림 2-2-8 | 생성된 라우팅 테이블 상세 페이지에서 연결된 프라이빗 서브넷 확인

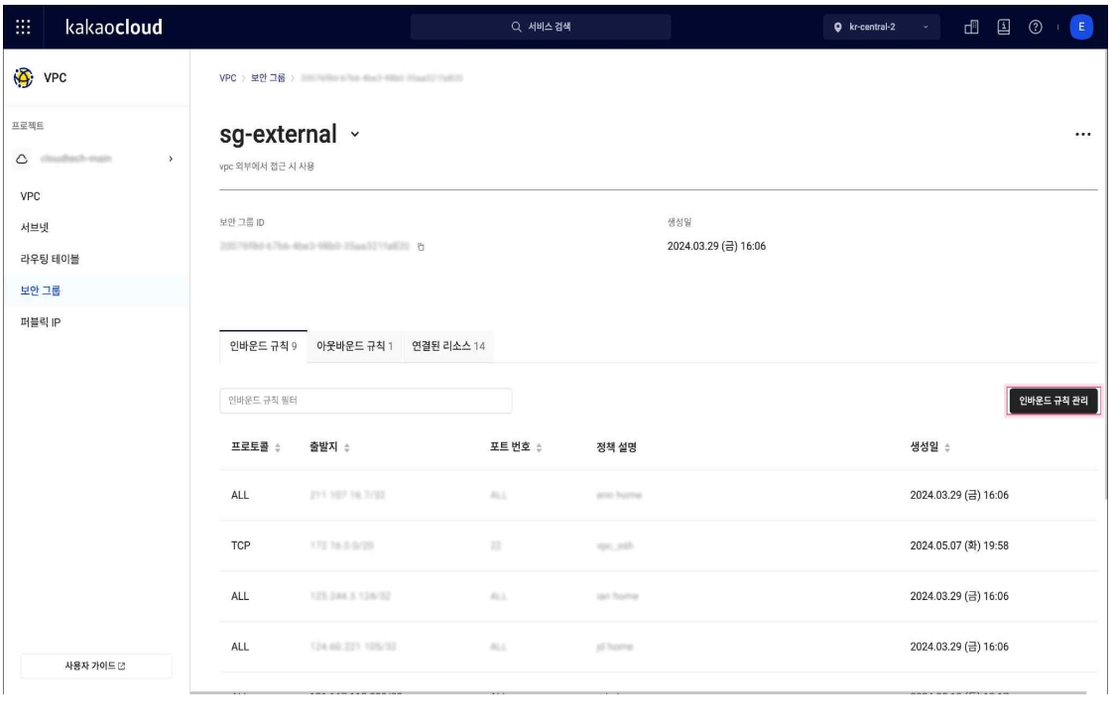
- 보안 그룹(Security Group) 기능을 통한 네트워크 구성(인/아웃바운드 통제 등)
  - 서브넷 간 접근 통제는 인스턴스에 연결된 보안 그룹(Security Group)의 인바운드 규칙을 설정합니다.



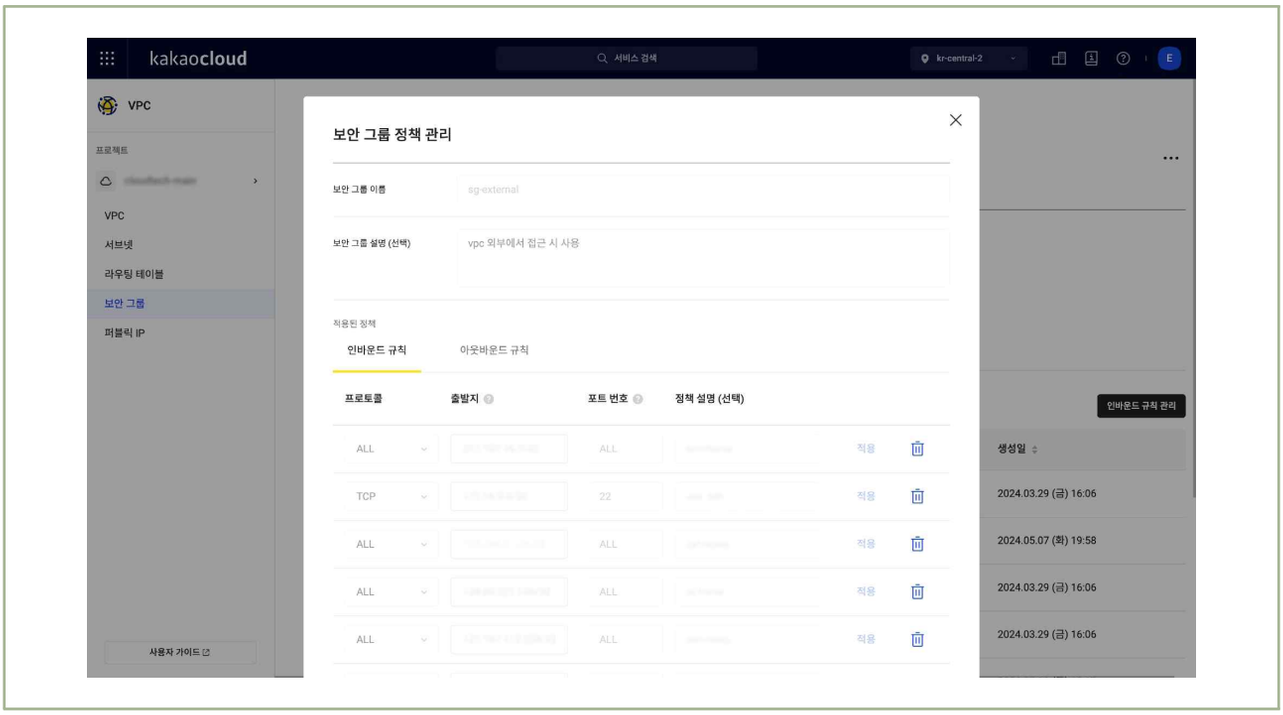
| 그림 2-2-9 | 인스턴스 상세페이지에서 인바운드 규칙 확인



| 그림 2-2-10 | 인바운드 규칙 수정이 필요할 경우, 해당 보안 그룹 클릭

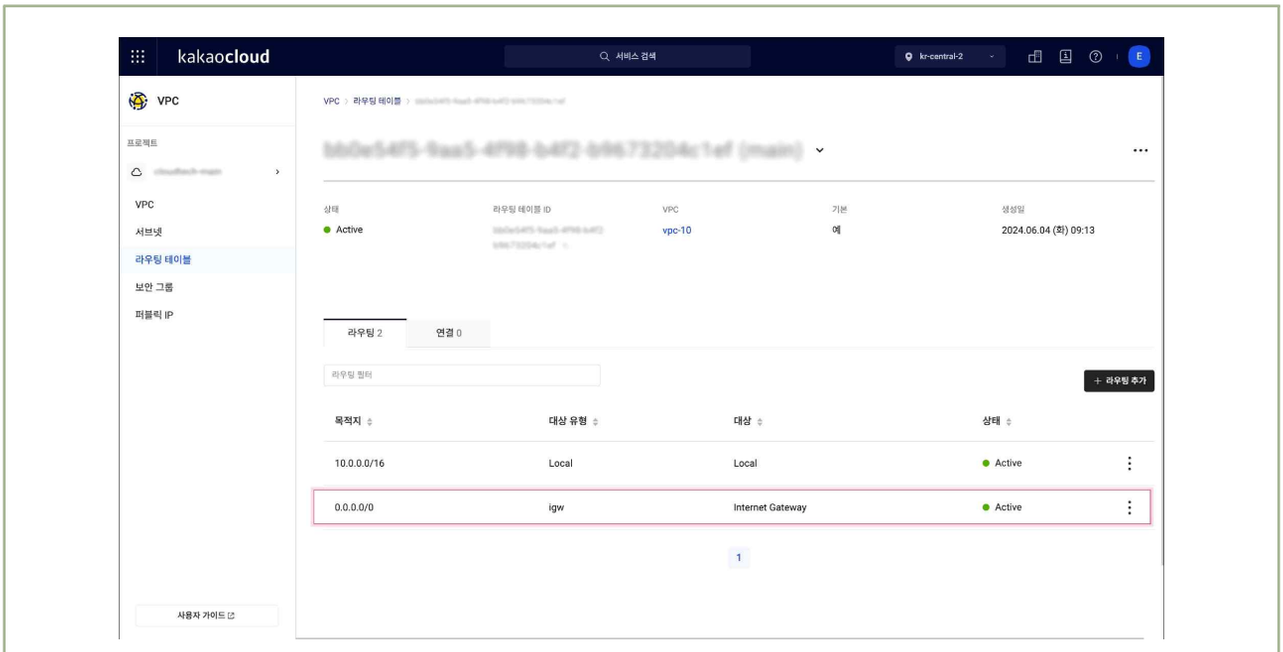


| 그림 2-2-11 | 보안 그룹 상세 페이지에서 인바운드 규칙 관리 클릭

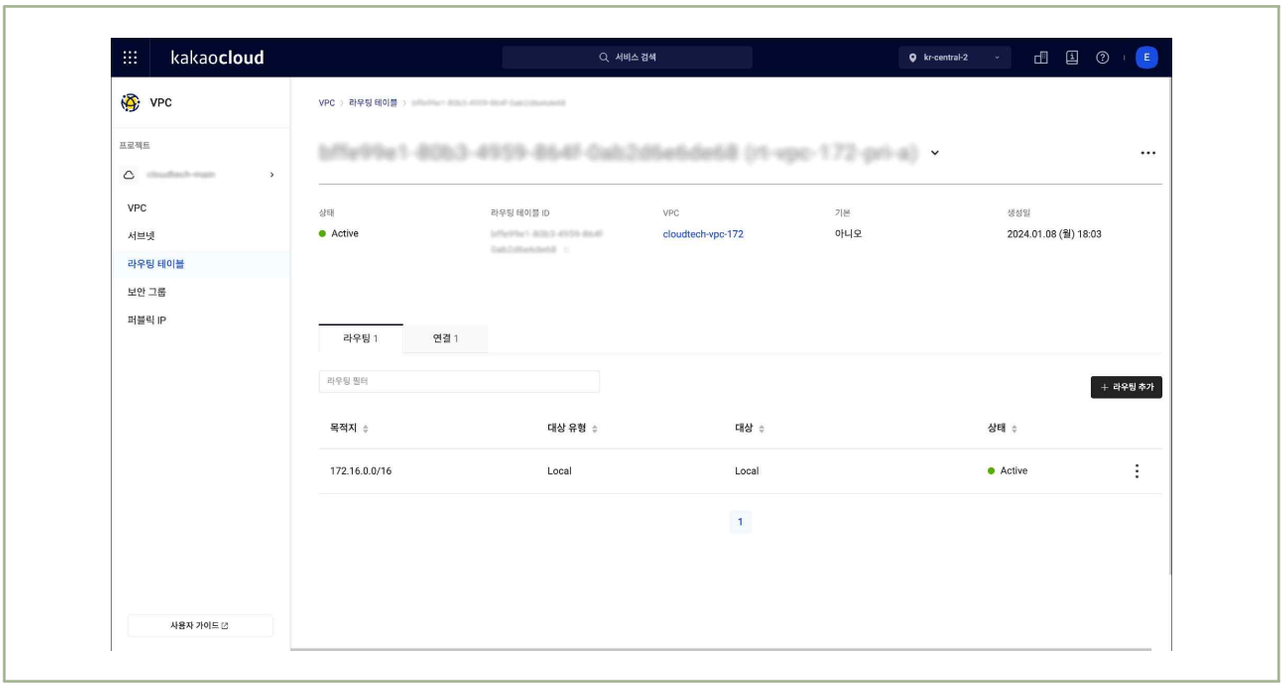


| 그림 2-2-12 | 인바운드 규칙 삭제 및 추가

- 내부망으로 구현한 가상자원(서버, 데이터베이스 등)에 퍼블릭 IP 미 할당
  - 내부망을 서브넷으로 구분하여 설정한 경우, 해당 서브넷에 연결된 라우팅 테이블에 Internet Gateway를 대상으로 하는 라우팅을 설정하지 않습니다. 설정되어 있는 경우에는 해당 라우팅 설정을 삭제합니다.

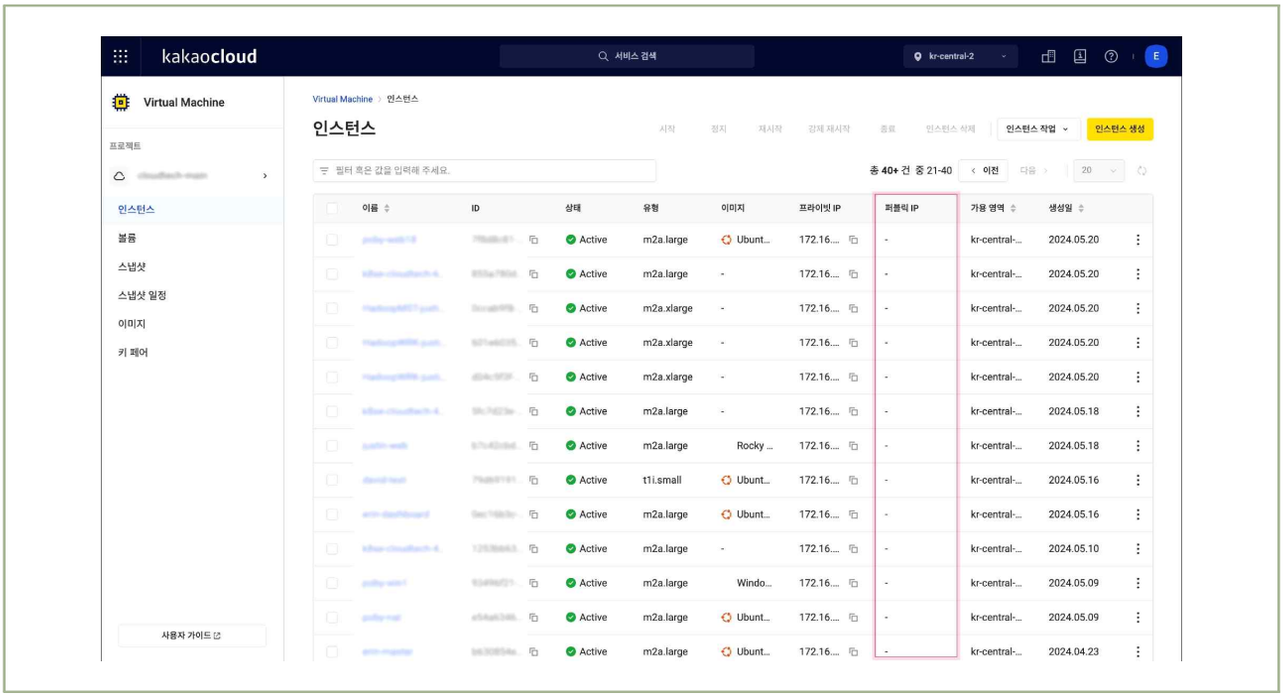


| 그림 2-2-13 | Internet Gateway를 대상으로 하는 라우팅이 있는 라우팅 테이블



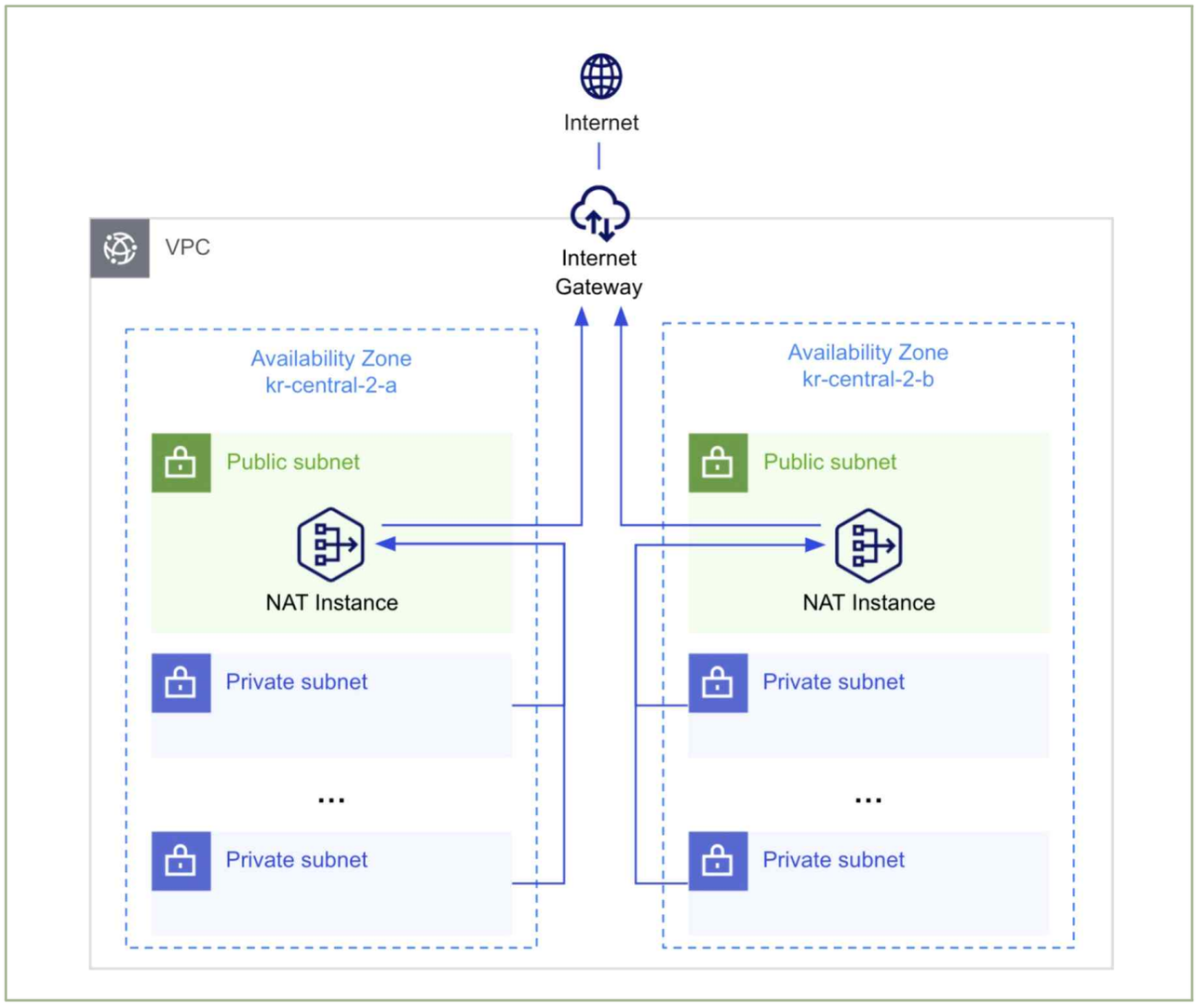
| 그림 2-2-14 | Internet Gateway를 대상으로 하는 라우팅이 없는 라우팅 테이블

- 또는, 서브넷에 연결된 라우팅 테이블에 Internet Gateway를 대상으로 하는 라우팅이 있다고 하더라도 해당 서브넷에 생성한 자원에 퍼블릭 IP를 연결하지 않습니다.

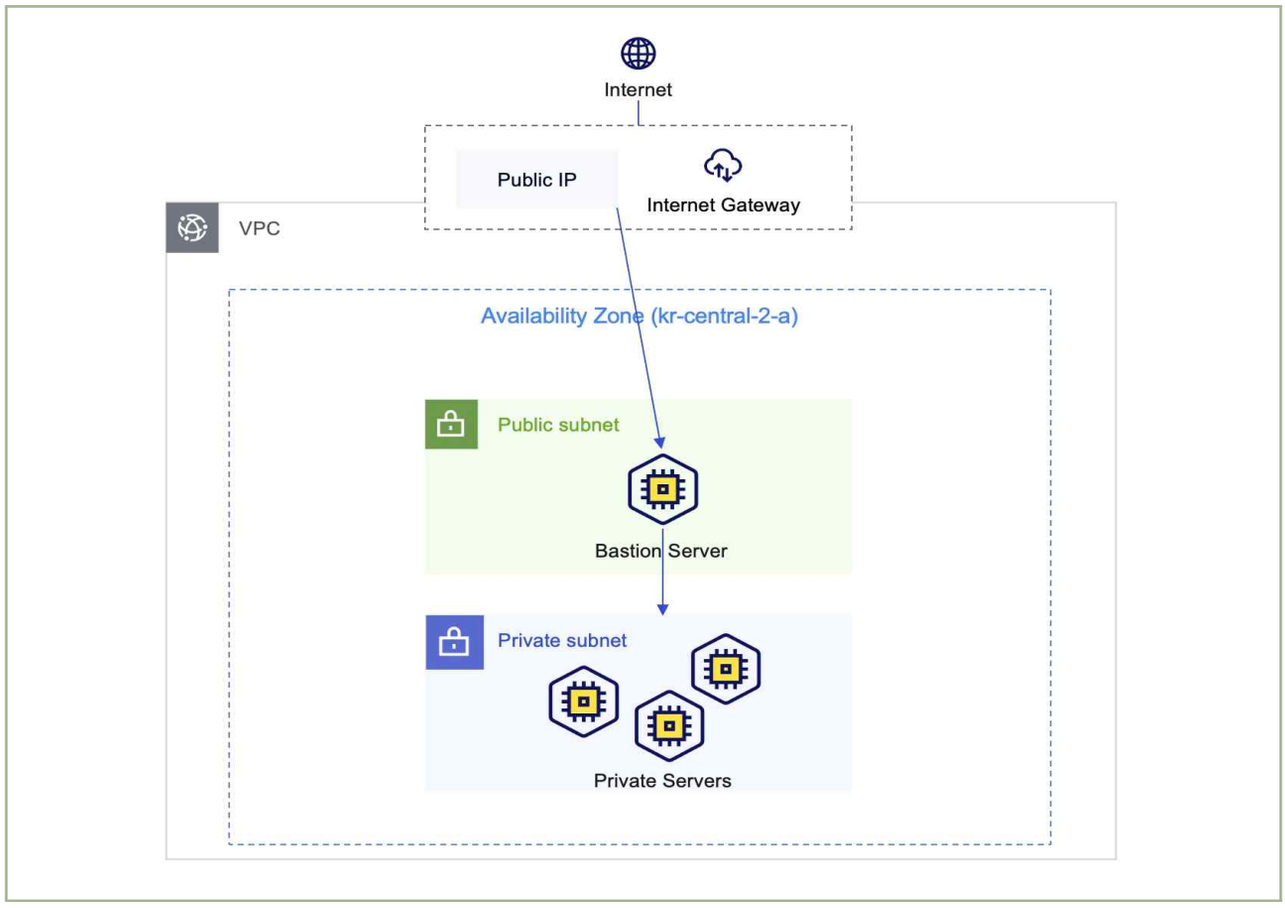


| 그림 2-2-15 | Virtual Machine 인스턴스의 퍼블릭 IP연결 여부 확인

- 외부 접근이 필요한 경우 NAT Instance, Bastion 서버 등을 활용하여 접근합니다. 이 때, NAT 인스턴스, Bastion 서버는 퍼블릭 서브넷에 위치합니다.

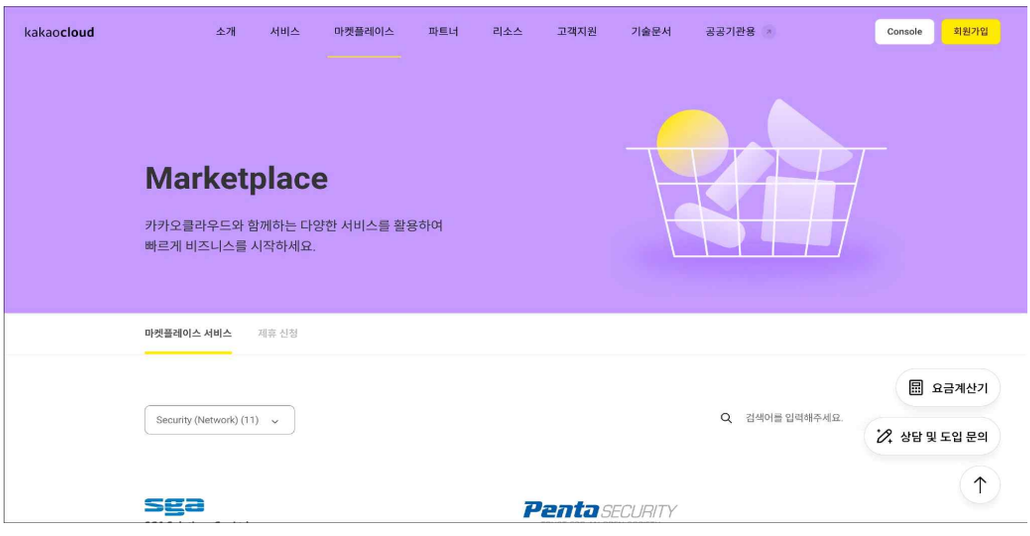


| 그림 2-2-16 | NAT 인스턴스 구성 예시 아키텍처



| 그림 2-2-17 | Bastion 서버 구성 예시 아키텍처

- 방화벽 서비스를 통한 IP 통제 등
  - 마켓플레이스 방화벽 상품을 활용하여 내부로 접속하는 IP들을 제한할 수 있습니다. (그림 3.1.1 네트워크/보안 프로젝트 내 UTM, WAF 구성 참고)



| 그림 2-2-18 | 카카오클라우드 마켓플레이스 상품 소개 페이지

4 참고 사항

- 카카오클라우드 VPC 생성 및 관리 가이드
- 카카오클라우드 서브넷 생성 및 관리 가이드
- 카카오클라우드 라우팅 테이블 생성 및 관리 가이드
- 카카오클라우드 마켓플레이스 상품 안내

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 가상자원을 보호하기 위해 네트워크 보안 관제를 수행하여야 한다.

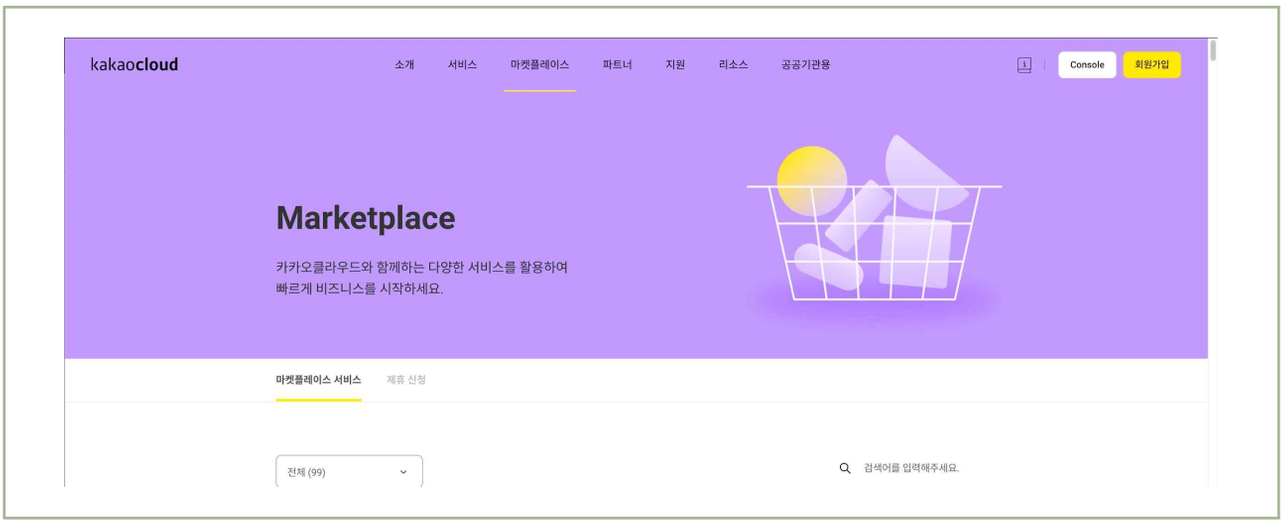
  - 예시

    1) 금융회사 보안 관제 서비스와 연동하여 관제 수행(클라우드 내 발생하는 네트워크 트래픽 연동 등을 활용)

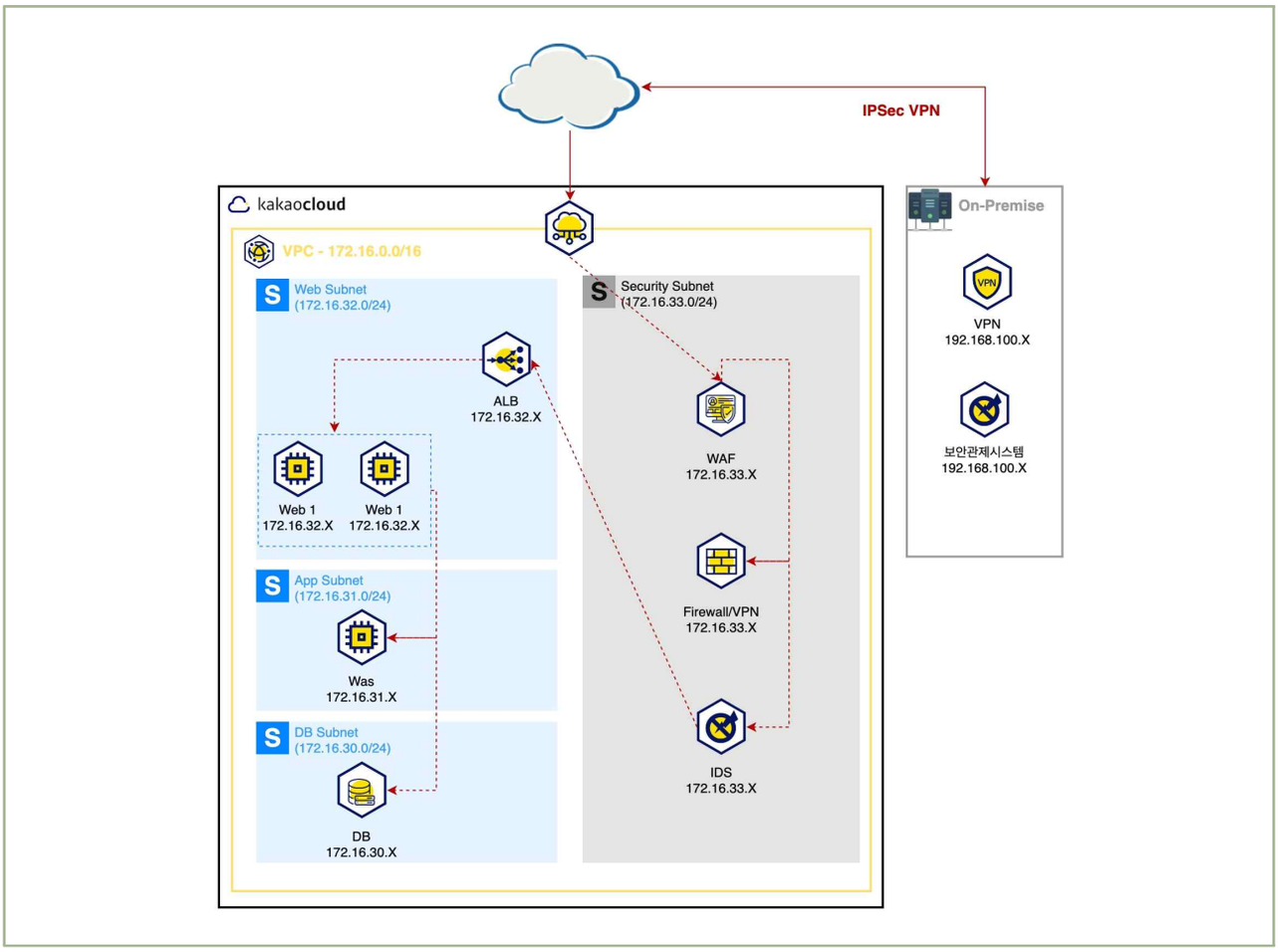
    2) 클라우드 서비스 제공자가 제공하는 가상자원 보호를 위한 네트워크 보안관제 및 유사 기능(DDoS, WAF 등) 활용

3 우수 사례

- 보안 관제를 위한 IDS 상품을(마켓플레이스) VPC 내 구성하고, 금융회사의 보안관제 시스템과 IPSec VPN 또는 전용선을 통해 연동하여 관제를 수행합니다.



| 그림 2-3-1 | 카카오클라우드 마켓플레이스 상품 소개 페이지



| 그림 2-3-2 | 네트워크 보안 관제 예시 아키텍처

- 카카오클라우드 보안 서비스를 통한 네트워크 보안관제를 제공받습니다.
  - 24x365 모니터링을 통해 카카오클라우드를 이용하는 이용자 자원에 대한 다양한 위협 대응
  - Managed Security, DDoS Defender, IDS 서비스

4 참고 사항

- 카카오클라우드 보안 서비스 안내

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.

  - 예시

    1) VPC 등 네트워크 분리 기능을 통한 DMZ 망 구축 후 공개용 웹서버 구현

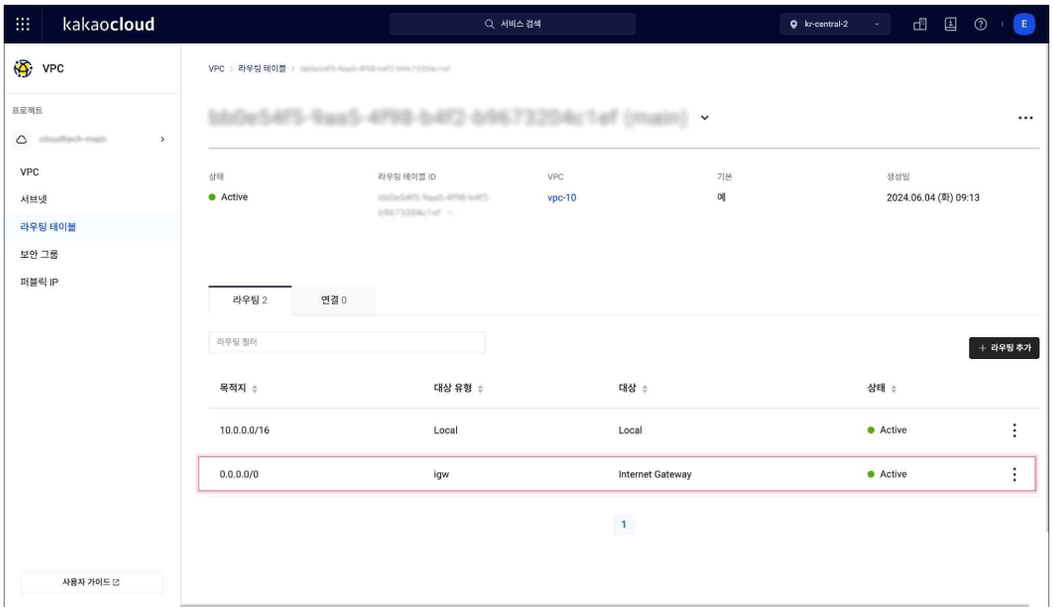
    2) 공개용 웹서버 직접 접근 시 통제(ACL 등)에 의한 중요단말기 등에서 접근하도록 관리

3 우수 사례

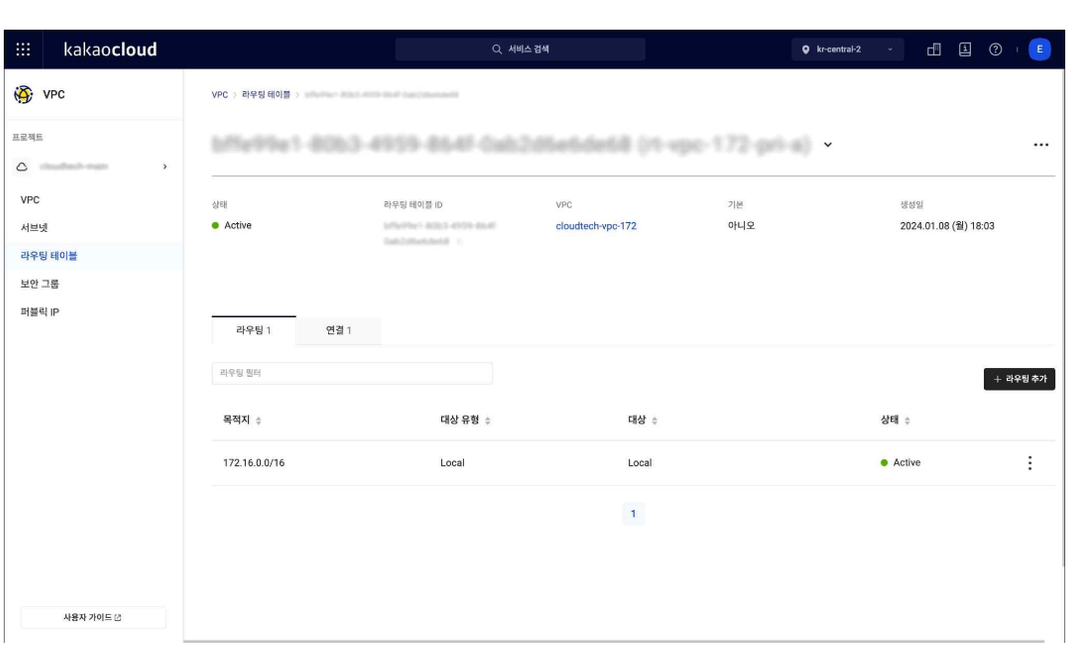
- VPC 등 네트워크 분리 기능을 통한 DMZ 망 구축 후 공개용 웹서버 구현 (그림 2.1.1 참고)

  - 하나의 프로젝트에 외부망, DMZ 망, 내부망으로 구분되는 여러 VPC를 생성합니다. VPC 간 통신을 연결하기 위해 Transit Gateway를 생성한 후, TGW 라우팅 테이블에 VPC 간 통신이 필요한 구간에 대해서만 라우팅 설정을 추가합니다.

  - 또는, 하나의 VPC 내에 여러 서브넷을 구성하여 인터넷 통신이 필요한 서브넷에는 Internet Gateway를 대상으로 하는 라우팅이 설정된 라우팅 테이블을 연결하고, 그렇지 않은 서브넷에는 Internet Gateway를 대상으로 하는 라우팅이 없는 라우팅 테이블을 연결합니다.



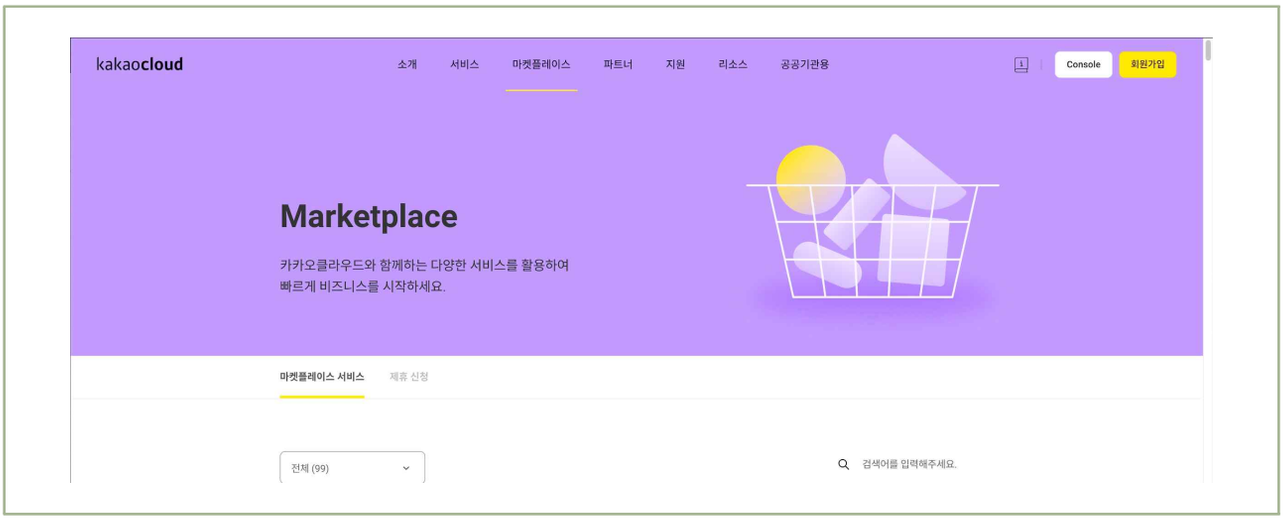
| 그림 2-4-1 | Internet Gateway를 대상으로 하는 라우팅이 있는 라우팅 테이블



| 그림 2-4-2 | Internet Gateway를 대상으로 하는 라우팅이 없는 라우팅 테이블

- 공개용 웹서버 직접 접근 시 통제(ACL 등)에 의한 중요단말기 등에서 접근하도록 관리
  - 하나의 프로젝트에 외부망, DMZ 망, 내부망으로 구분되는 여러 VPC를 생성합니다. VPC 간 통신을 연결하기 위해 Transit Gateway를 생성한 후, TGW 라우팅 테이블에 VPC 간 통신이 필요한 구간에 대해서만 라우팅 설정을 추가합니다.

- 이후 외부망 또는 DMZ 망에 접근 통제를 위한 마켓플레이스 보안 상품을 구성하여 외부에서 공개용 웹서버 접근 시 해당 상품이 설치된 인스턴스를 거치도록 설정합니다.



| 그림 2-4-3 | 카카오클라우드 마켓플레이스 상품 소개 페이지

4 참고 사항

- 카카오클라우드 VPC 생성 및 관리 가이드
- 카카오클라우드 서브넷 생성 및 관리 가이드
- 카카오클라우드 라우팅 테이블 생성 및 관리 가이드
- 카카오클라우드 마켓플레이스 상품 안내

1 기준

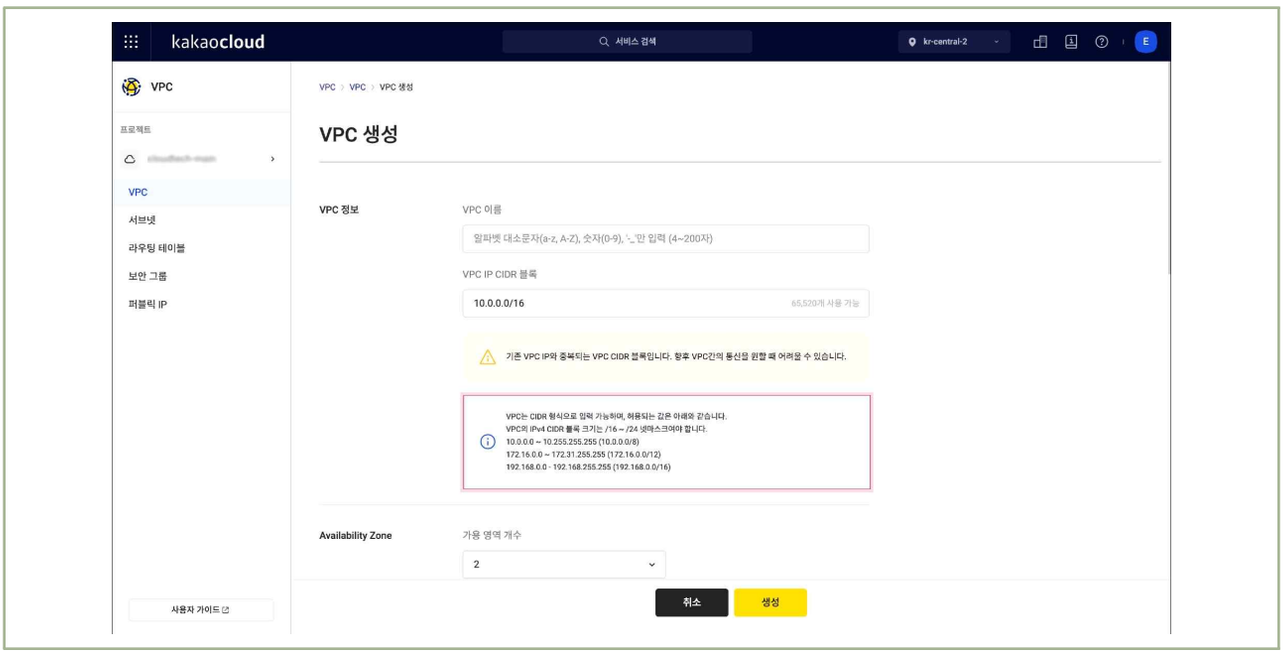
식별번호	기준	내용
2.5.	**네트워크 사설 IP주소 할당 및 관리**	**클라우드 환경을 통한 내부망 네트워크 구현 시 사설 IP 부여 등으로 보안을 강화하고, 내부IP 유출을 금지하여야 한다.**

2 설명

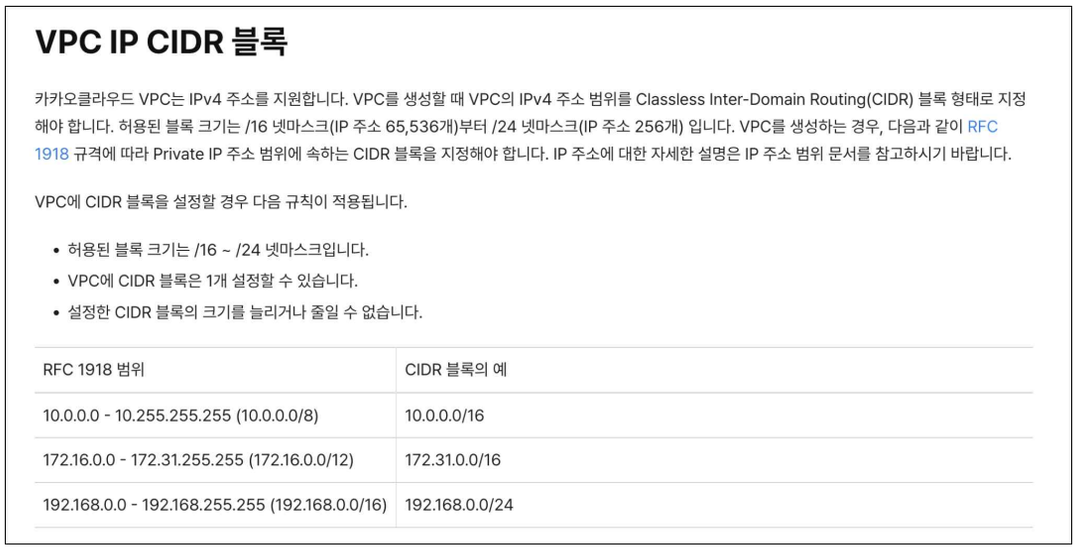
- 클라우드 환경 내 내부망 네트워크 구현 시 사설 IP를 부여하고 주기적으로 현황을 검토하여야 한다.
  - 예시
    1) 인터넷 게이트웨이, NAT 게이트웨이 등 관련 기능을 통해 사설 IP 부여 및 IP 관리 수행
    2) 프라이빗 IP 할당 현황에 대한 주기적 검토 수행

3 우수 사례

- 인터넷 게이트웨이, NAT 인스턴스 등 관련 기능을 통해 사설 IP 부여 및 IP 관리 수행
  - 카카오클라우드에서는 RFC 1918 규격에 따라 사설 IP 주소 범위에서 허용된 블록 크기에 맞춰 VPC를 생성합니다.



| 그림 2-5-1 | VPC 생성 시, RFC 1918 규격에 따른 사설 IP 주소 범위 확인



VPC IP CIDR 블록

카카오클라우드 VPC는 IPv4 주소를 지원합니다. VPC를 생성할 때 VPC의 IPv4 주소 범위를 Classless Inter-Domain Routing(CIDR) 블록 형태로 지정해야 합니다. 허용된 블록 크기는 /16 넷마스크(IP 주소 65,536개)부터 /24 넷마스크(IP 주소 256개) 입니다. VPC를 생성하는 경우, 다음과 같이 RFC 1918 규격에 따라 Private IP 주소 범위에 속하는 CIDR 블록을 지정해야 합니다. IP 주소에 대한 자세한 설명은 IP 주소 범위 문서를 참고하시기 바랍니다.

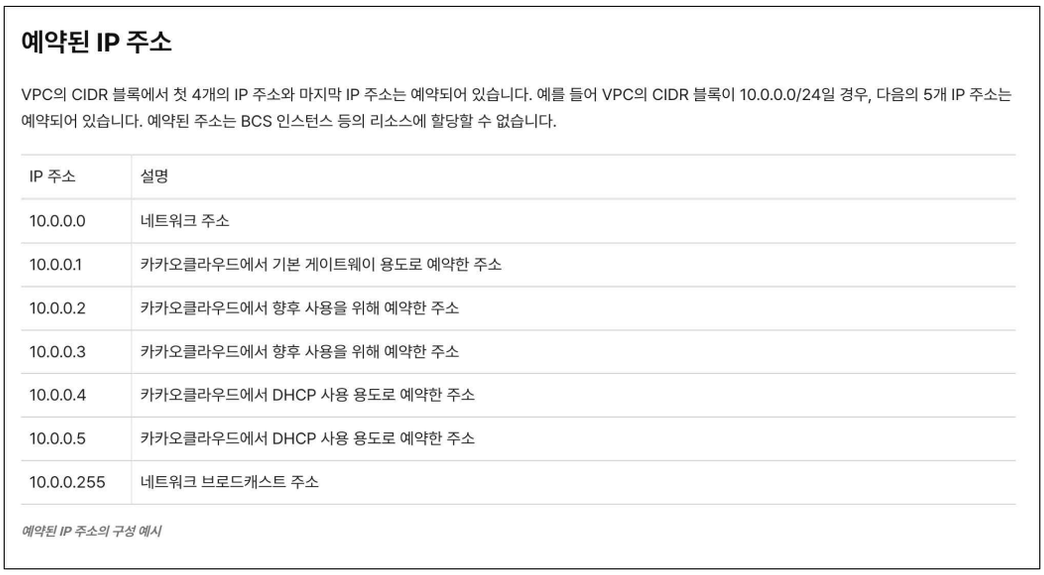
VPC에 CIDR 블록을 설정할 경우 다음 규칙이 적용됩니다.

- 허용된 블록 크기는 /16 ~ /24 넷마스크입니다.
- VPC에 CIDR 블록은 1개 설정할 수 있습니다.
- 설정한 CIDR 블록의 크기를 늘리거나 줄일 수 없습니다.

RFC 1918 범위	CIDR 블록의 예
10.0.0.0 - 10.255.255.255 (10.0.0.0/8)	10.0.0.0/16
172.16.0.0 - 172.31.255.255 (172.16.0.0/12)	172.31.0.0/16
192.168.0.0 - 192.168.255.255 (192.168.0.0/16)	192.168.0.0/24

| 그림 2-5-2 | 카카오클라우드 가이드 문서에 기재된 RFC 1918 규격에 따른 사설 IP 주소 범위

- VPC 에는 예약된 IP 주소가 있습니다. 해당 주소들을 제외한 나머지 주소 범위 내에서 생성된 자원에 사설 IP가 부여됩니다.



예약된 IP 주소

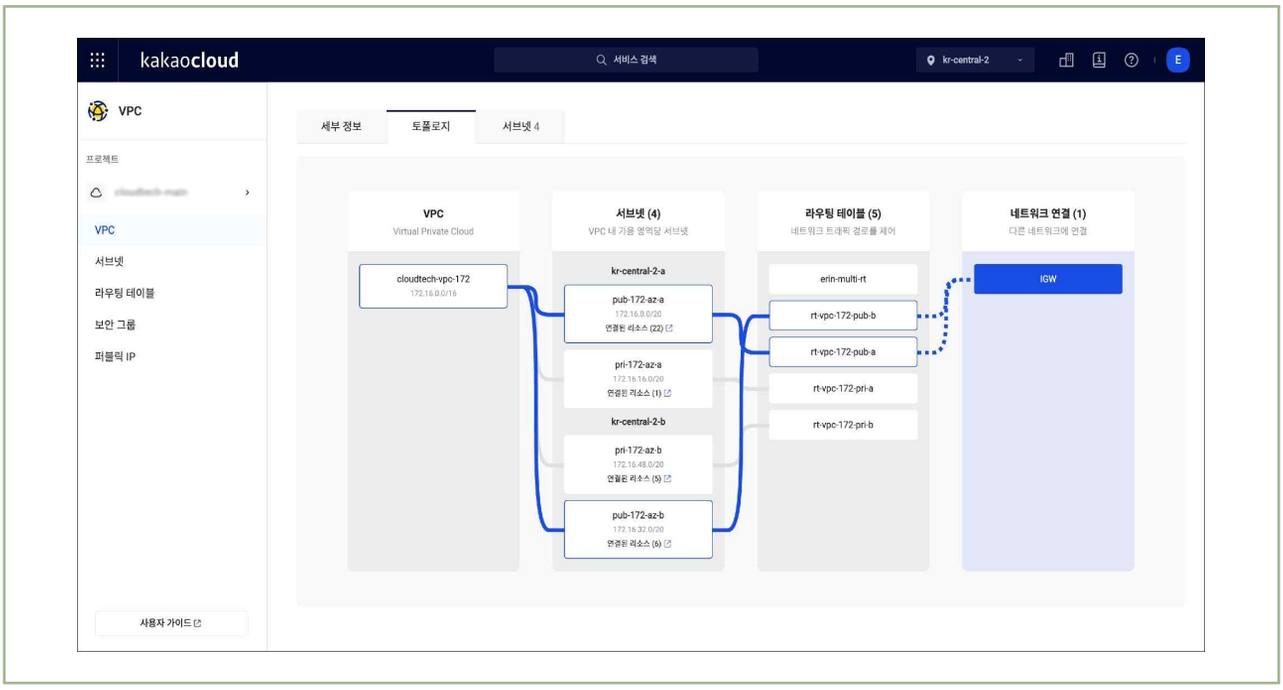
VPC의 CIDR 블록에서 첫 4개의 IP 주소와 마지막 IP 주소는 예약되어 있습니다. 예를 들어 VPC의 CIDR 블록이 10.0.0.0/24일 경우, 다음의 5개 IP 주소는 예약되어 있습니다. 예약된 주소는 BCS 인스턴스 등의 리소스에 할당할 수 없습니다.

IP 주소	설명
10.0.0.0	네트워크 주소
10.0.0.1	카카오클라우드에서 기본 게이트웨이 용도로 예약한 주소
10.0.0.2	카카오클라우드에서 향후 사용을 위해 예약한 주소
10.0.0.3	카카오클라우드에서 향후 사용을 위해 예약한 주소
10.0.0.4	카카오클라우드에서 DHCP 사용 용도로 예약한 주소
10.0.0.5	카카오클라우드에서 DHCP 사용 용도로 예약한 주소
10.0.0.255	네트워크 브로드캐스트 주소

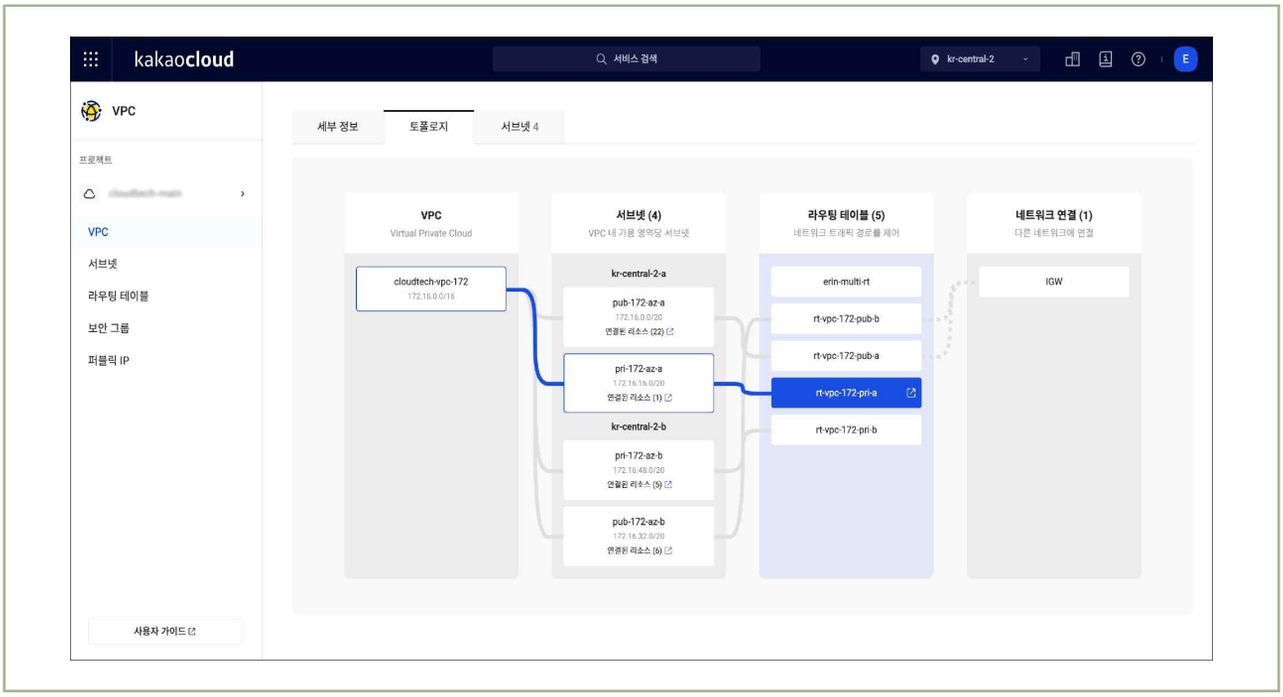
예약된 IP 주소의 구성 예시

| 그림 2-5-3 | 카카오클라우드 가이드 문서에 기재된 예약된 IP 주소

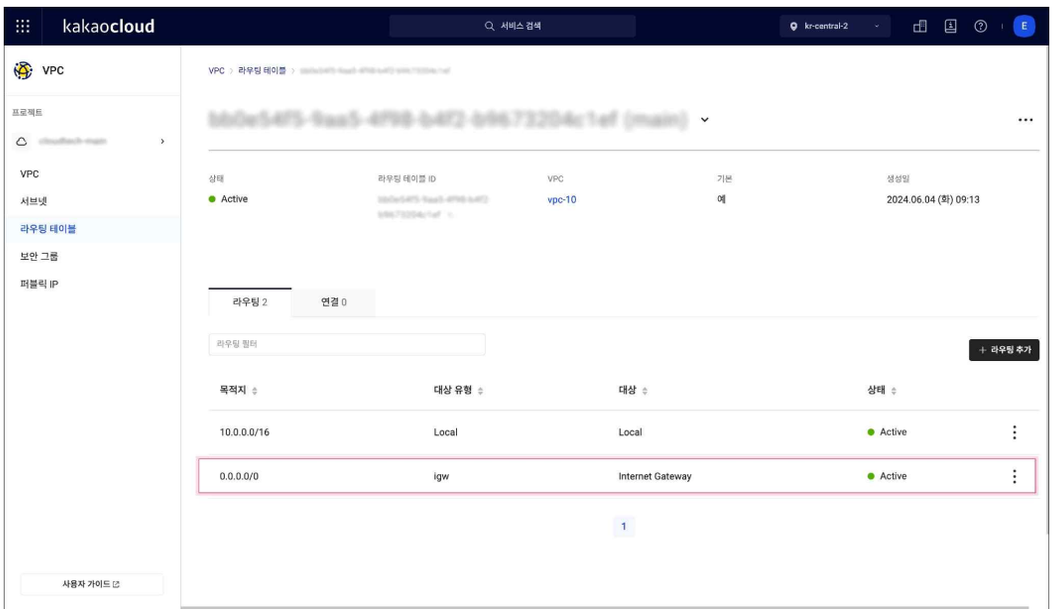
- 하나의 VPC 내에 여러 서브넷을 구성하여 인터넷 통신이 필요한 퍼블릭 서브넷에는 Internet Gateway를 대상으로 하는 라우팅이 설정된 라우팅 테이블을 연결하고, 그렇지 않은 프라이빗 서브넷에는 Internet Gateway를 대상으로 하는 라우팅이 없는 라우팅 테이블을 연결합니다.



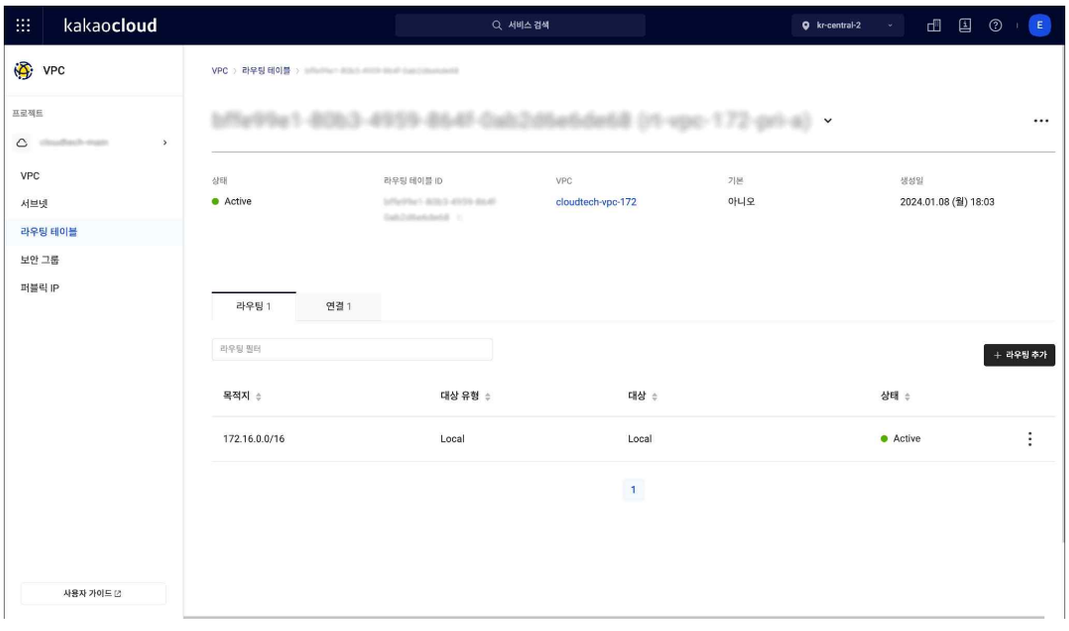
| 그림 2-5-4 | 퍼블릭 서브넷에 연결된 Internet Gateway(IGW)를 대상으로하는 라우팅 테이블



| 그림 2-5-5 | 프라이빗 서브넷에 연결된 라우팅 테이블



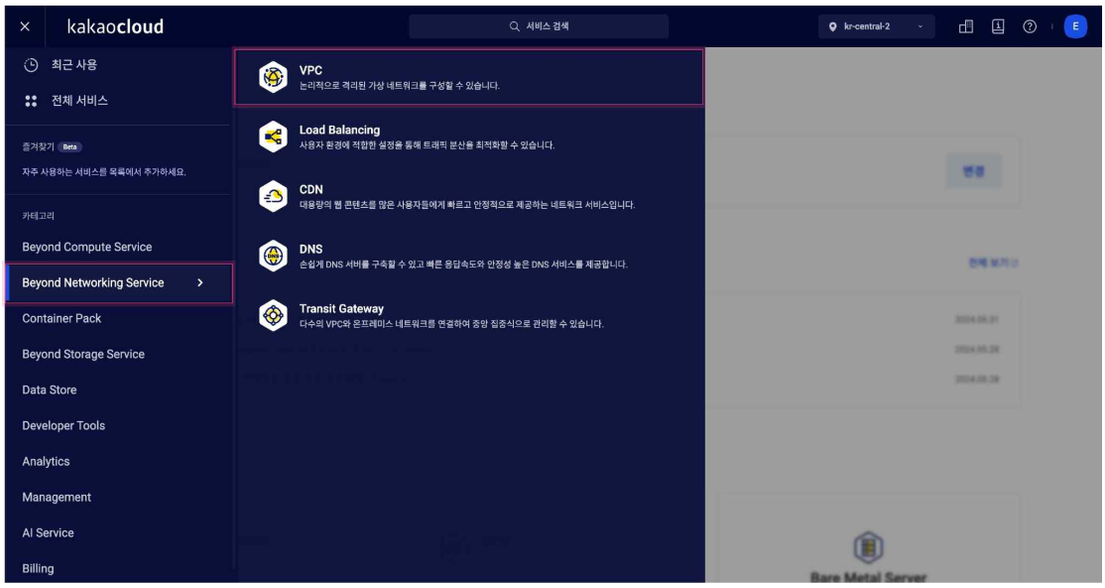
| 그림 2-5-6 | Internet Gateway를 대상으로 하는 라우팅이 있는 라우팅 테이블



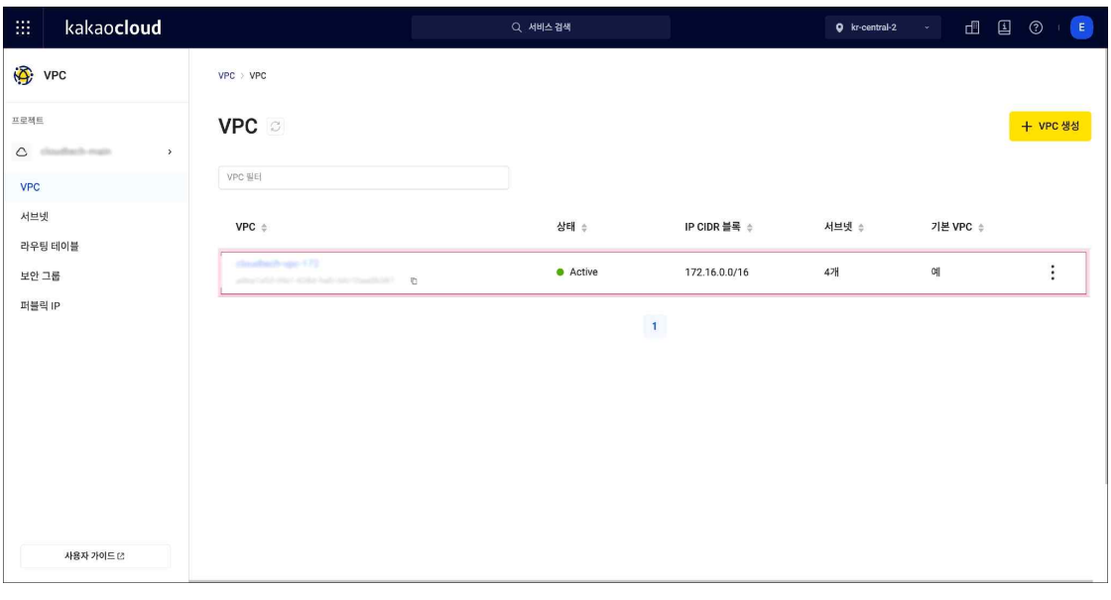
| 그림 2-5-7 | Internet Gateway를 대상으로 하는 라우팅이 없는 라우팅 테이블

- 프라이빗 서브넷에 생성된 자원으로부터 외부 접근이 필요한 경우 NAT 인스턴스를 생성하여 활용하고, 외부에서 프라이빗 서브넷에 생성된 자원으로 접근이 필요한 경우에는 Bastion 서버를 활용하여 접근하도록 합니다. 이때, NAT 인스턴스, Bastion 서버는 퍼블릭 서브넷에 위치합니다.

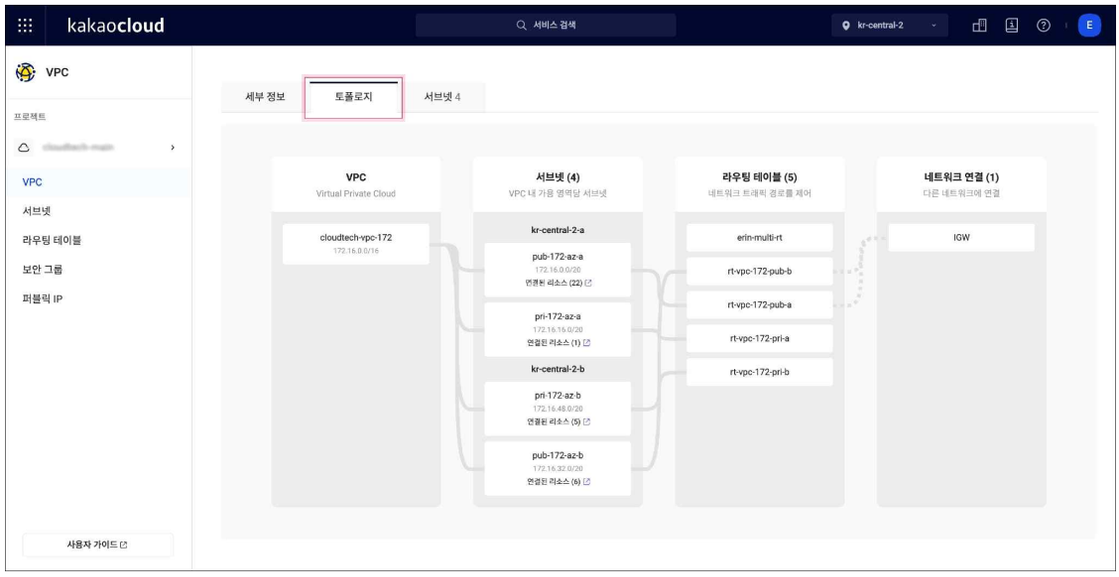
- 사설 IP 할당 현황에 대한 주기적 검토 수행
  - **(Console)** 'Dashboard' → 'Beyond Networking Service' → 'VPC' 페이지에서 사설 IP 할당 현황을 확인하고자 하는 VPC 선택 → '토폴로지' 탭에서 각 서브넷 별 연결된 리소스 정보를 확인하여 해당 서브넷 대역에서 사용 중인 사설 IP 현황을 확인합니다.



| 그림 2-5-8 | 카카오클라우드 콘솔 〉 Beyond Networking Service 〉 VPC 서비스 이동



| 그림 2-5-9 | 사설 IP 할당 현황을 확인할 VPC 선택



| 그림 2-5-10 | 토폴리지 탭에서 할당된 사설 IP 확인

4 참고 사항

- 카카오클라우드 VPC 생성 및 관리 가이드
- 카카오클라우드 서브넷 생성 및 관리 가이드
- 카카오클라우드 라우팅 테이블 생성 및 관리 가이드
- 카카오클라우드 NAT 인스턴스 사용 가이드
- 카카오클라우드 VPC 〉 예약된 IP 주소 안내

1 기준

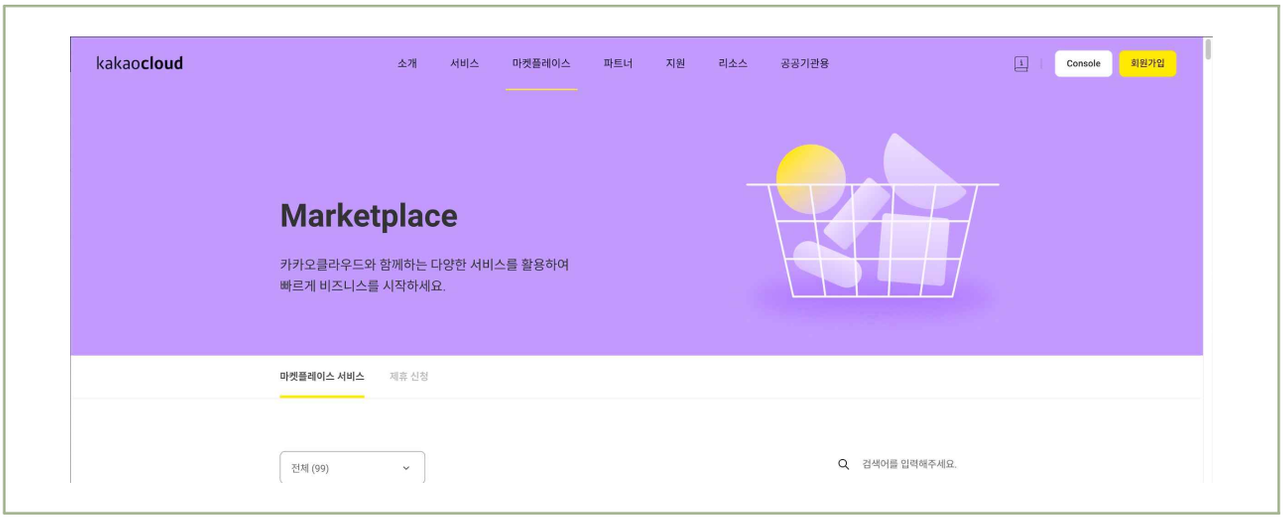
식별번호	기준	내용
2.6.	**네트워크(방화벽 등) 정책 주기적 검토**	**클라우드 서비스를 통해 구현한 네트워크 정책에 대해 주기적 검토를 수행하여야 한다.**

2 설명

- 클라우드 네트워크 관련 서비스 관련 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

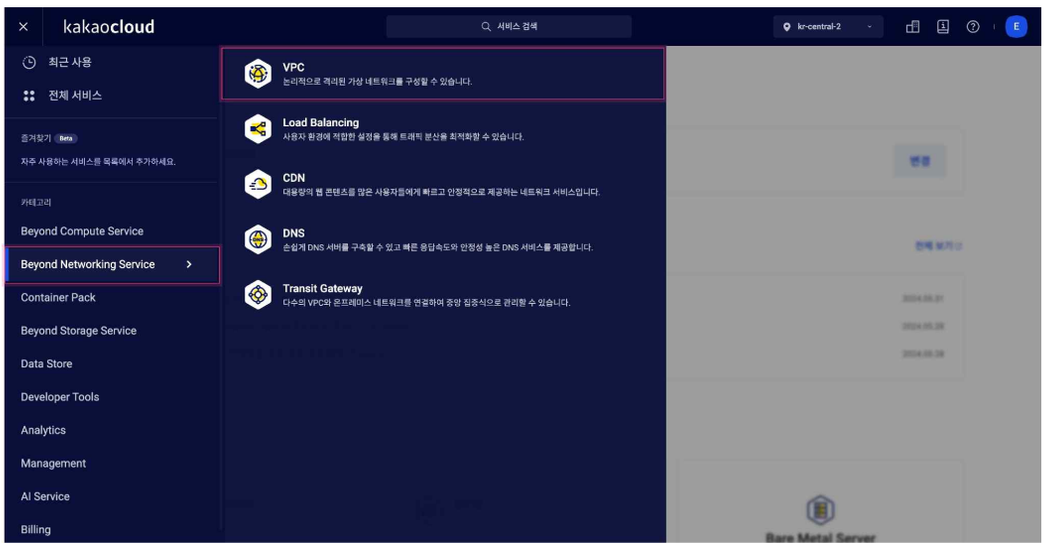
- 방화벽 정책에 관한 주기적 검토 수행
  - 방화벽의 경우 마켓플레이스 상품을 통해 구성 가능하며, 방화벽 설정은 방화벽 솔루션에 접속하여 관리가 가능합니다.



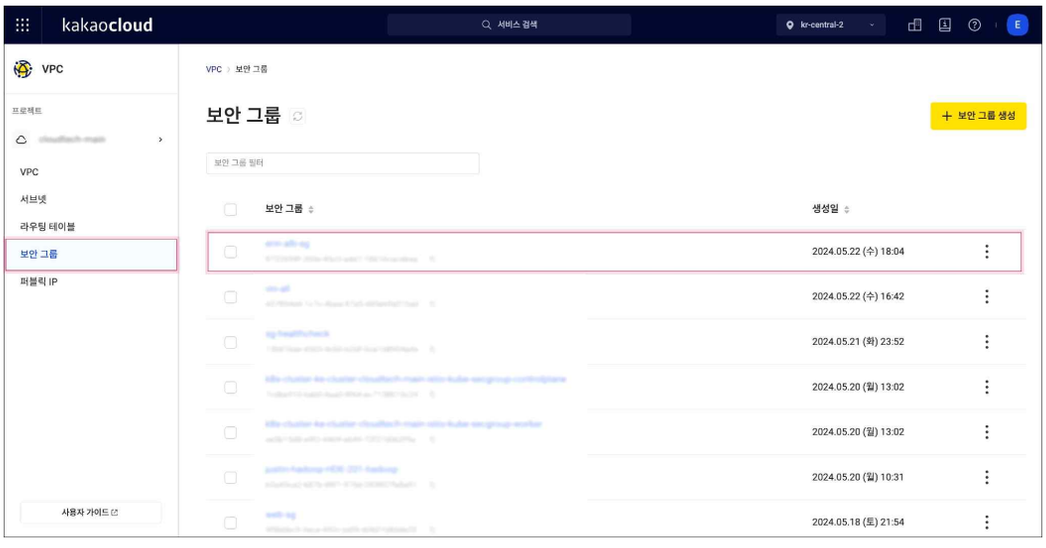
| 그림 2-6-1 | 카카오클라우드 마켓플레이스 상품 소개 페이지

- ACL 정책에 관한 주기적 검토 수행
  - NACL 서비스는 추후 제공 예정입니다.

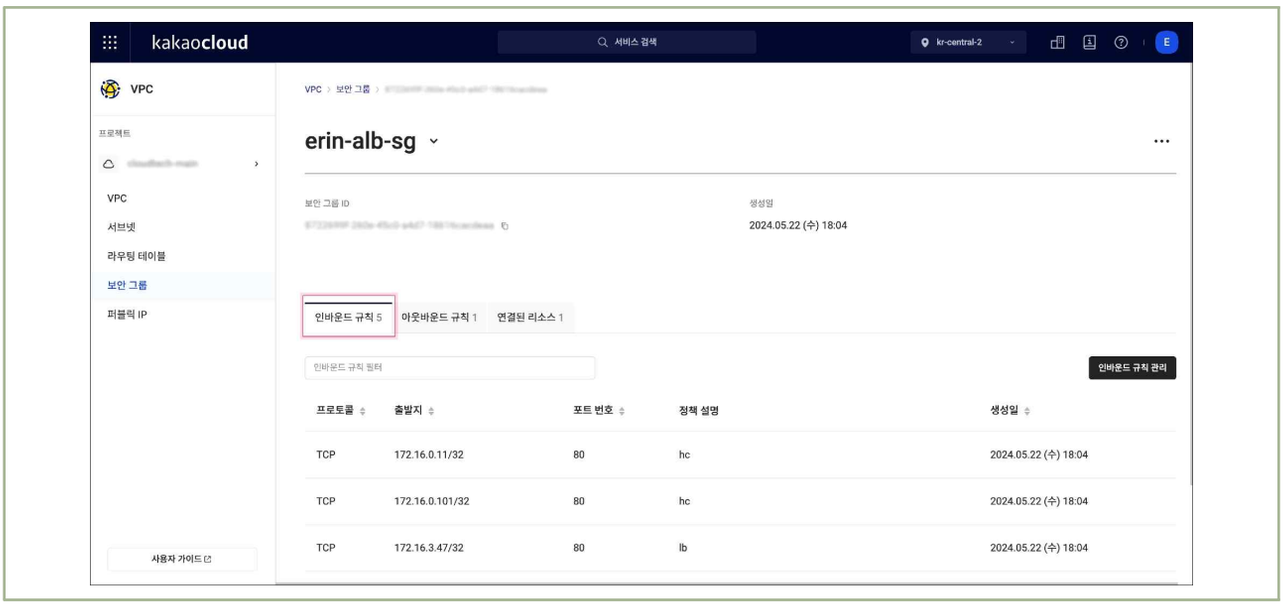
- 보안그룹에 관한 주기적 검토 수행
  - **(Console)** 'Dashboard' → 'Beyond Networking Service' → 'VPC' → '보안 그룹' 페이지에서 보안 그룹 목록을 확인하고, 확인을 원하는 보안 그룹의 이름을 클릭하여 보안 그룹 상세 페이지에서 인바운드 / 아웃바운드 규칙을 확인합니다.



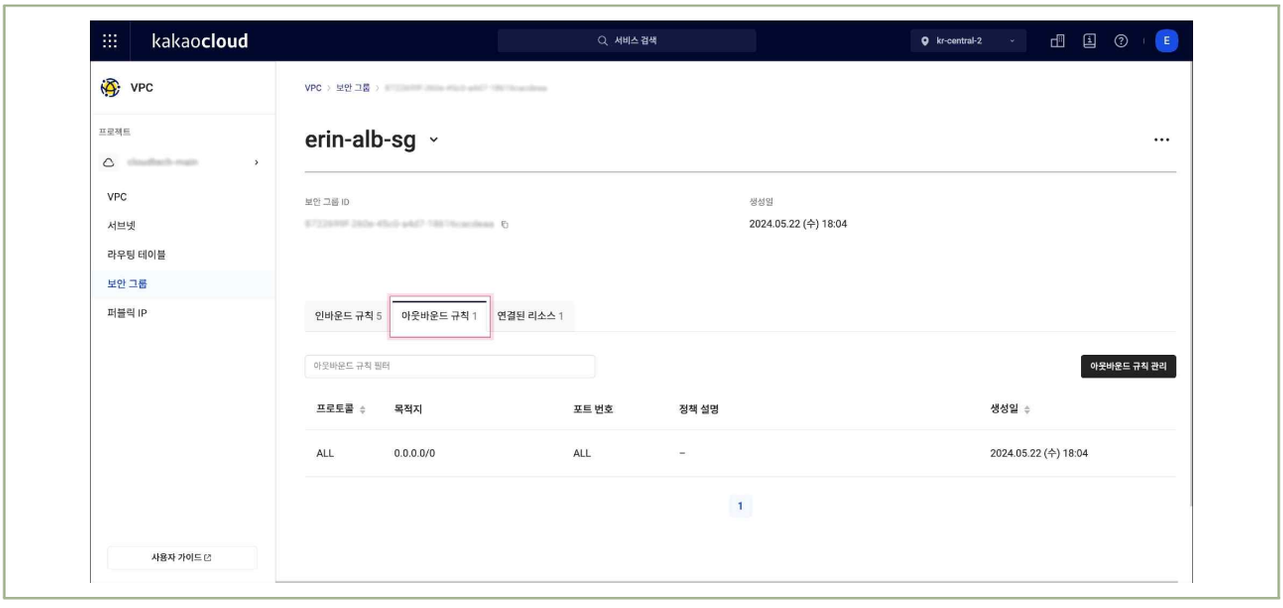
| 그림 2-6-2 | 카카오클라우드 콘솔 〉 Beyond Networking Service 〉 VPC 서비스 이동



| 그림 2-6-3 | 보안그룹 목록 중, 확인을 원하는 보안그룹 선택

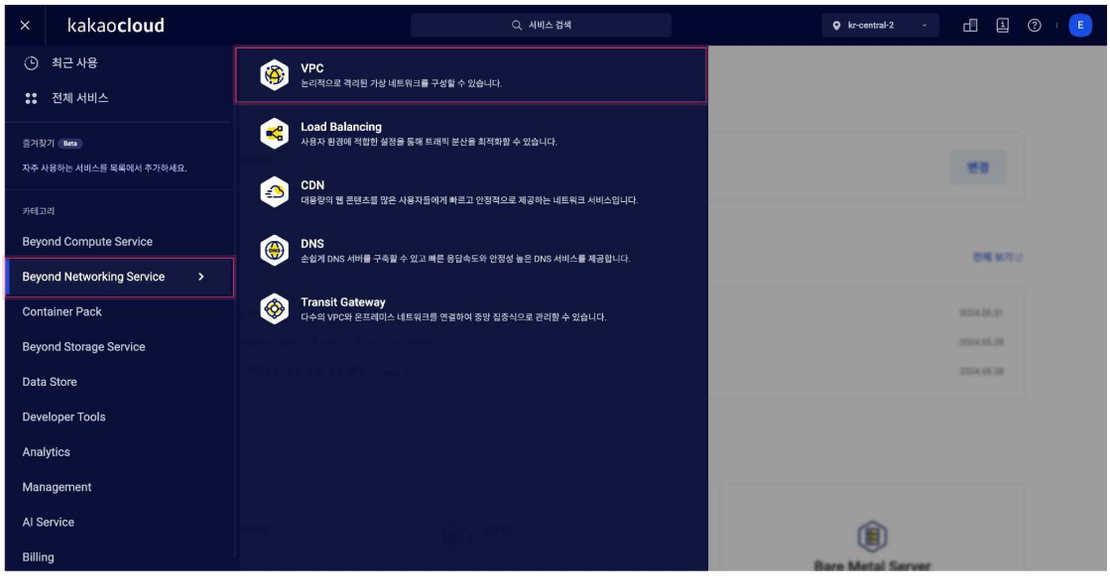


| 그림 2-6-4 | 인바운드 규칙 확인

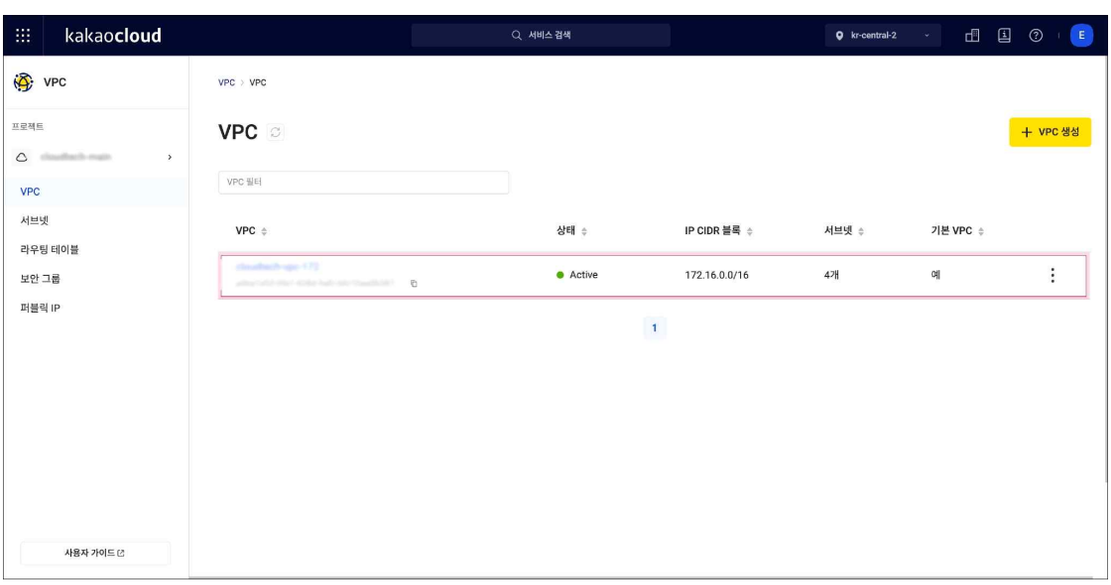


| 그림 2-6-5 | 아웃바운드 규칙 확인

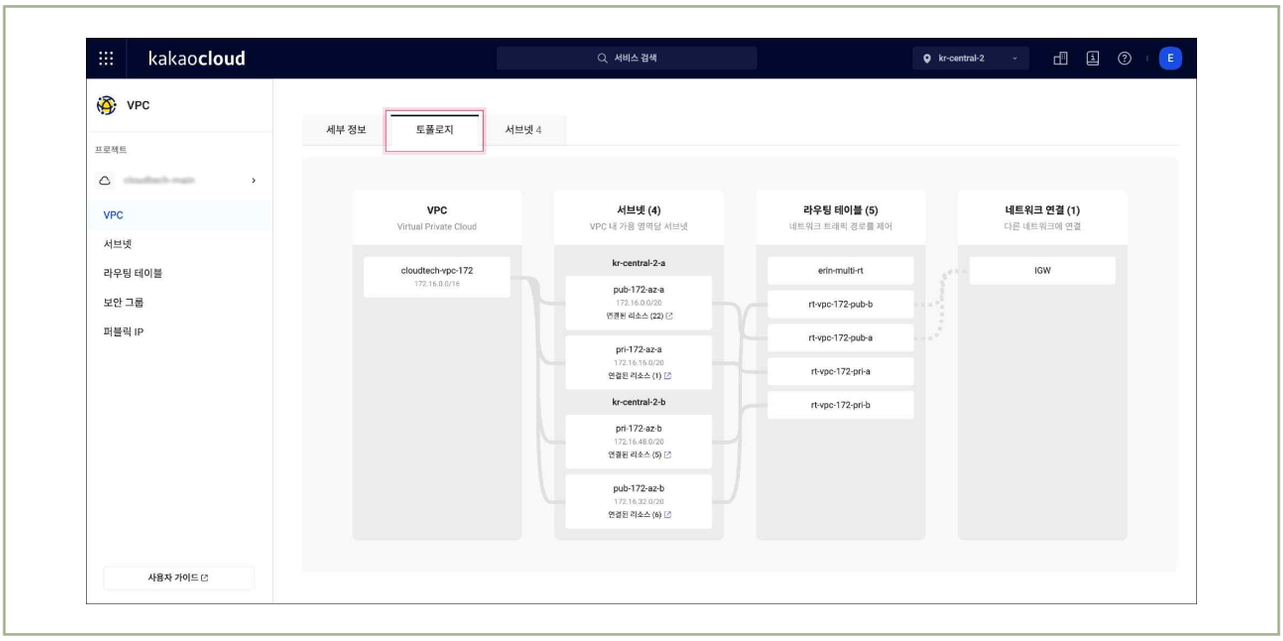
- VPC, 서브넷에 관한 주기적 검토 수행
  - **(Console)** 'Dashboard' → 'VPC' 페이지 에서 검토하고자 하는 VPC 선택 → '토폴로지' 탭 에서 VPC, 서브넷, 라우팅 테이블, 네트워크 연결(IGW, TGW 등) 의 연결 관계를 확인합니다.



| 그림 2-6-6 | 카카오클라우드 콘솔 〉 Beyond Networking Service 〉 VPC 서비스 이동



| 그림 2-6-7 | 프라이빗 IP 할당 현황을 확인할 VPC 선택



| 그림 2-6-8 | 토폴로지' 탭 에서 VPC, 서브넷, 라우팅 테이블, 네트워크 연결(IGW, TGW 등) 의 연결 관계를 확인

4 참고 사항

- 카카오클라우드 마켓플레이스 상품 안내
- 카카오클라우드 보안 그룹 생성 및 관리 가이드
- 카카오클라우드 VPC 생성 및 관리 가이드

3. 계정 및 권한 관리

3.1. 클라우드 계정 권한 관리
3.2. 이용자별 인증 수단 부여
3.3. 인사 변경사항 발생 시 계정 관리
3.4. 클라우드 가상자원 관리 시스템 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.

  - 예시

    1) 자격 증명 등의 기능을 이용하여 계정 권한 관리
    2) 사전에 정의된 행위만이 가능하도록 역할을 생성

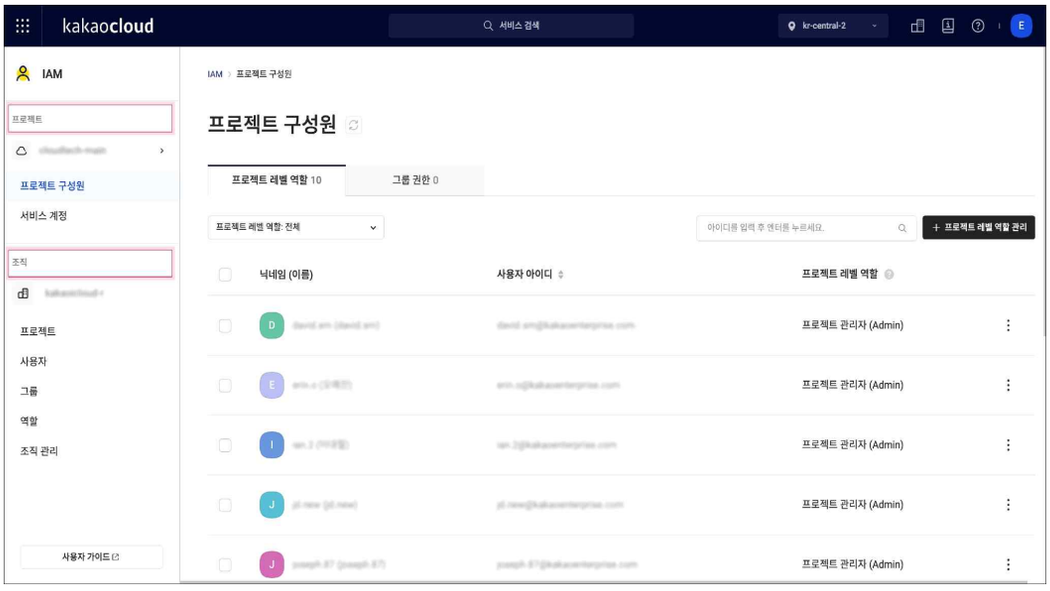
- 콘솔 최상위 관리자(ex. 최초 가입계정 등)는 서비스 운영에 활용하지 않아야 한다.

  - 예시

    1) 부득이 일부 서비스에 대해 관리자 권한이 필요한 경우, 신규로 계정을 생성하여 필요한 권한을 부여한 후 활용
    2) 예외적으로 반드시 최초 콘솔 가입계정을 이용하여야 하는 특정 서비스의 경우에는, MFA등 추가 인증 방식을 구현하고 접속 IP를 제한하는 등 강화된 보안환경 구성

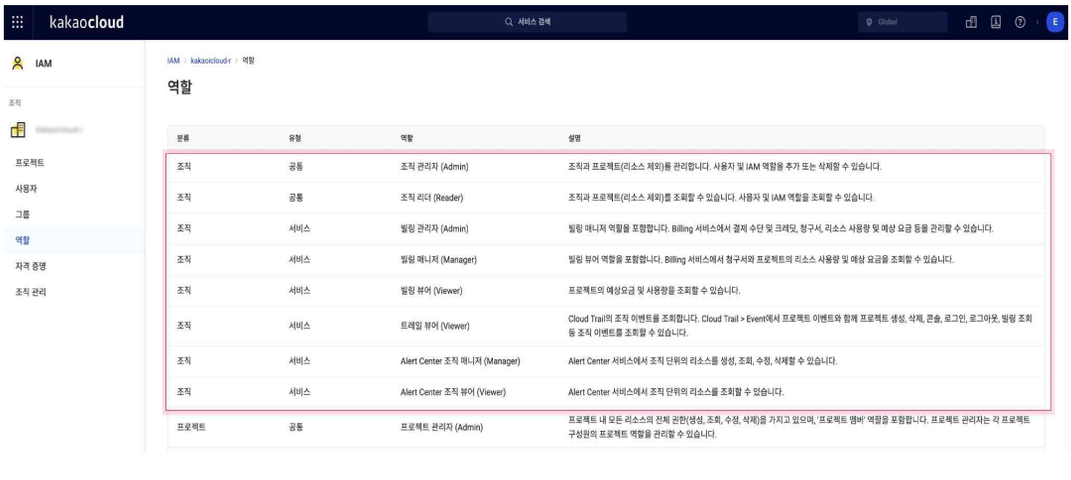
3 우수 사례

- 카카오클라우드의 역할은 크게 조직 레벨과 프로젝트 레벨로 구분하며, 사용자에게 여러 역할을 부여할 수 있습니다.



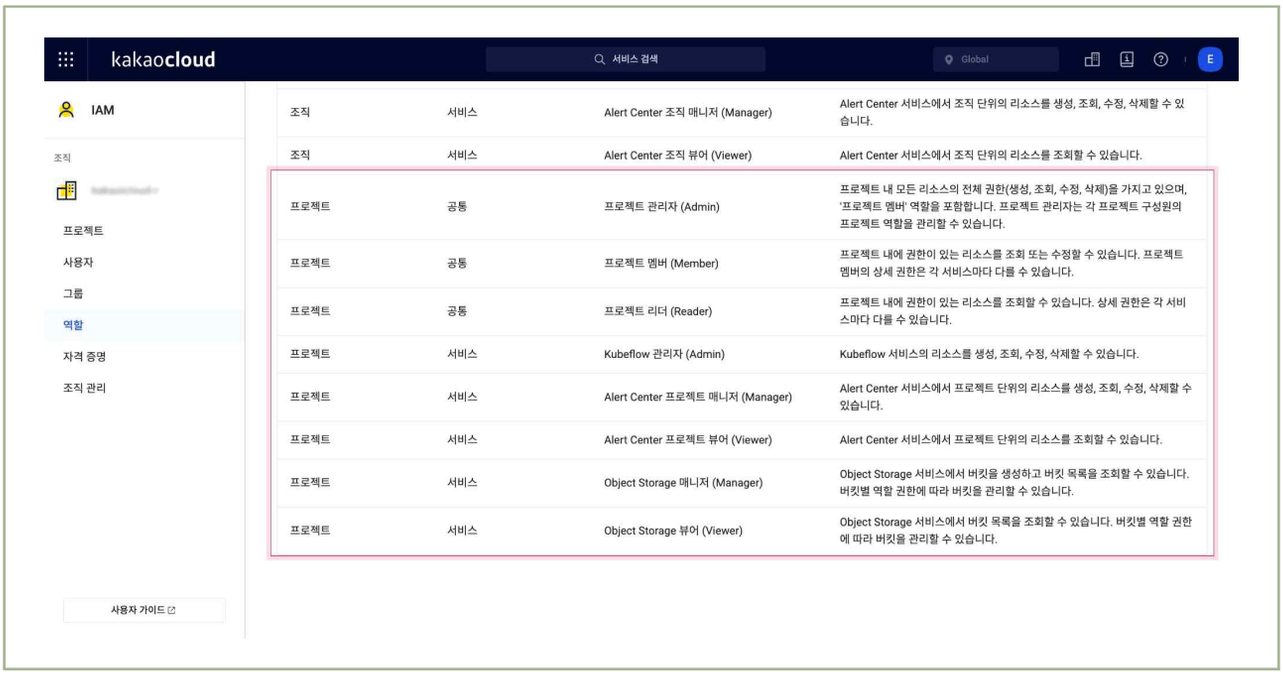
| 그림 3-1-1 | 카카오클라우드 콘솔의 IAM 서비스에서 확인할 수 있는 프로젝트와 조직

- 조직 레벨 역할 유형은 조직 관리자(Admin), 조직 리더(Reader), 빌링 관리자(Admin), 빌링 매니저(Member), 빌링 뷰어(Viewer), 트레일 뷰어(Viewer), Alert Center 관리자(Admin), Alert Center 조직 뷰어(Viewer) 가 있습니다.



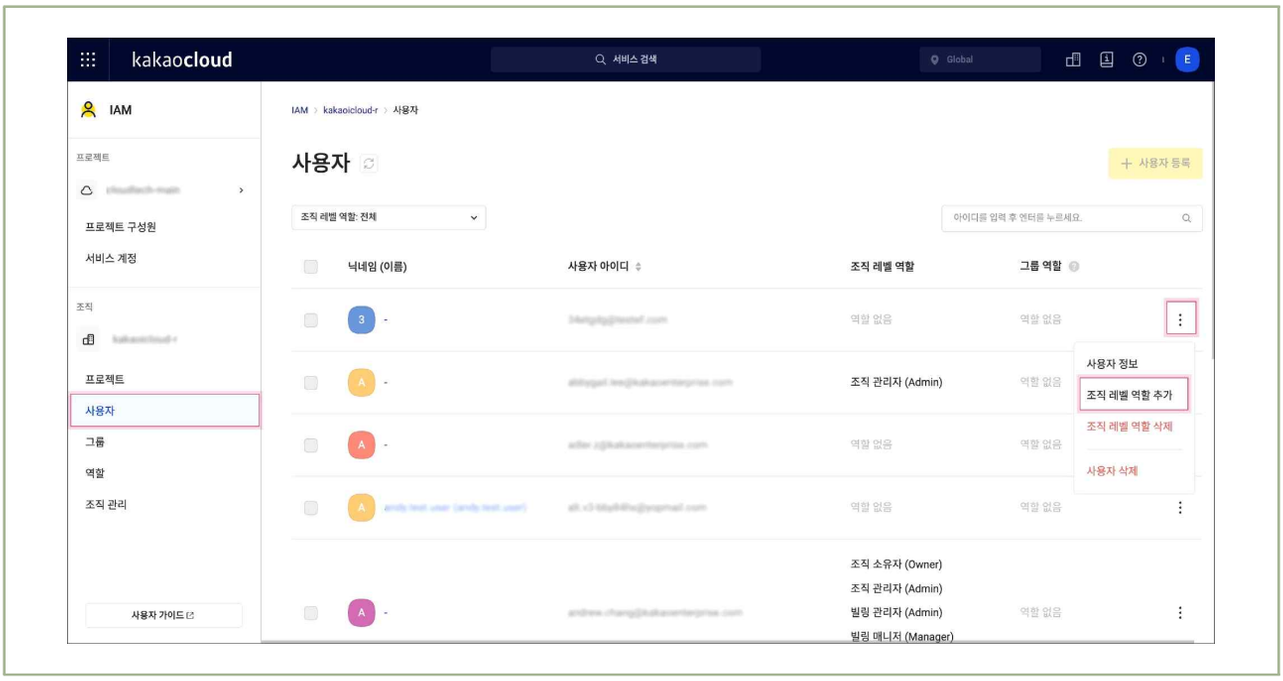
| 그림 3-1-2 | 카카오클라우드 콘솔의 IAM 서비스에서 확인할 수 있는 조직 레벨 역할 유형

- 프로젝트 레벨 역할 유형은 프로젝트 관리자(Admin), 프로젝트 멤버(Member), 프로젝트 리더(Reader), Object Storage 매니저(Manager), Object Storage 뷰어(Viewer), Kubeflow 관리자(Admin), Alert Center 프로젝트 매니저(Manager), Alert Center 프로젝트 뷰어(Viewer) 등이 있습니다.

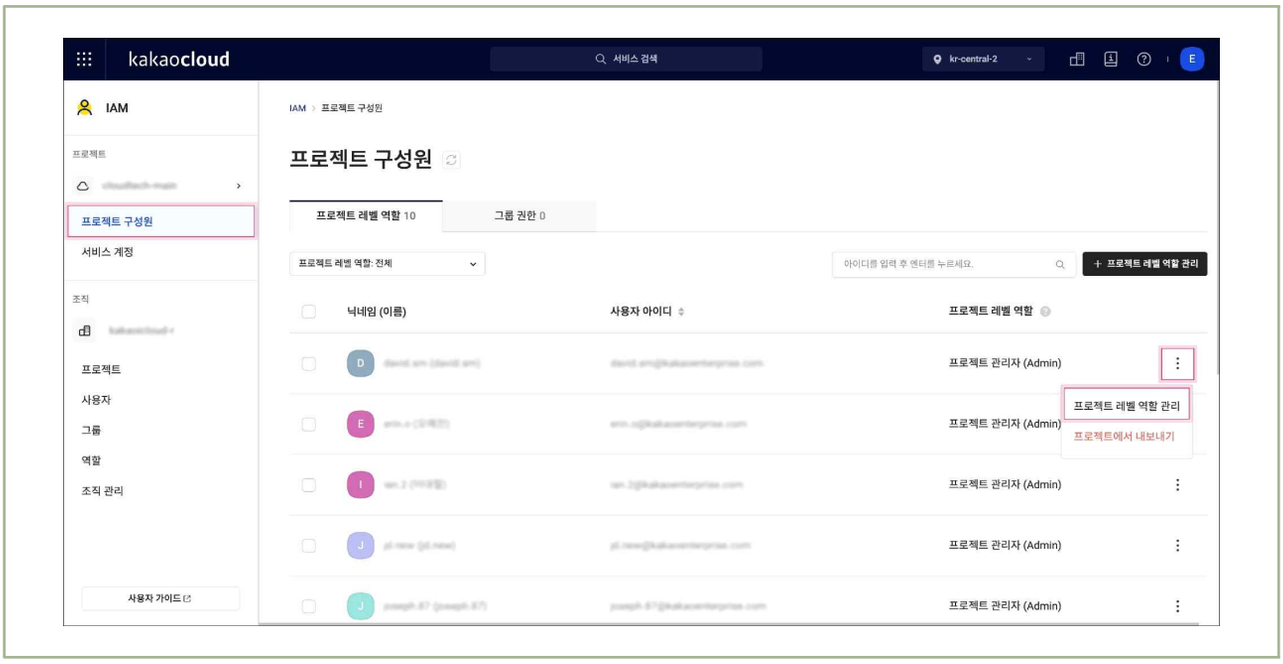


| 그림 3-1-3 | 카카오클라우드 콘솔의 IAM 서비스에서 확인할 수 있는 프로젝트 레벨 역할 유형

- 카카오클라우드에서는 최초 가입된 계정이 조직 소유자가 되며, 조직 소유자 계정은 개인 계정이 아니라 대표 계정으로 가입할 것을 권장합니다.
- 조직 소유자에게는 조직 관리자, 빌링 관리자 역할이 할당됩니다.

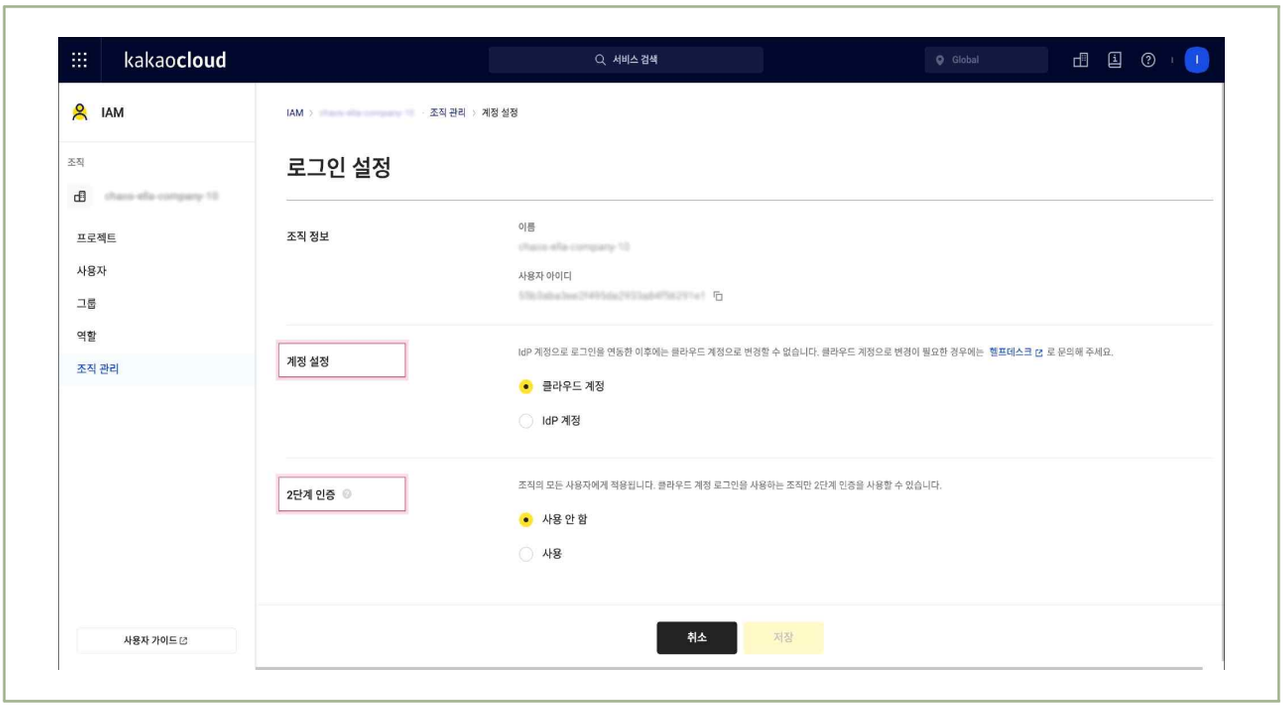


| 그림 3-1-4 | 조직 레벨 역할 추가

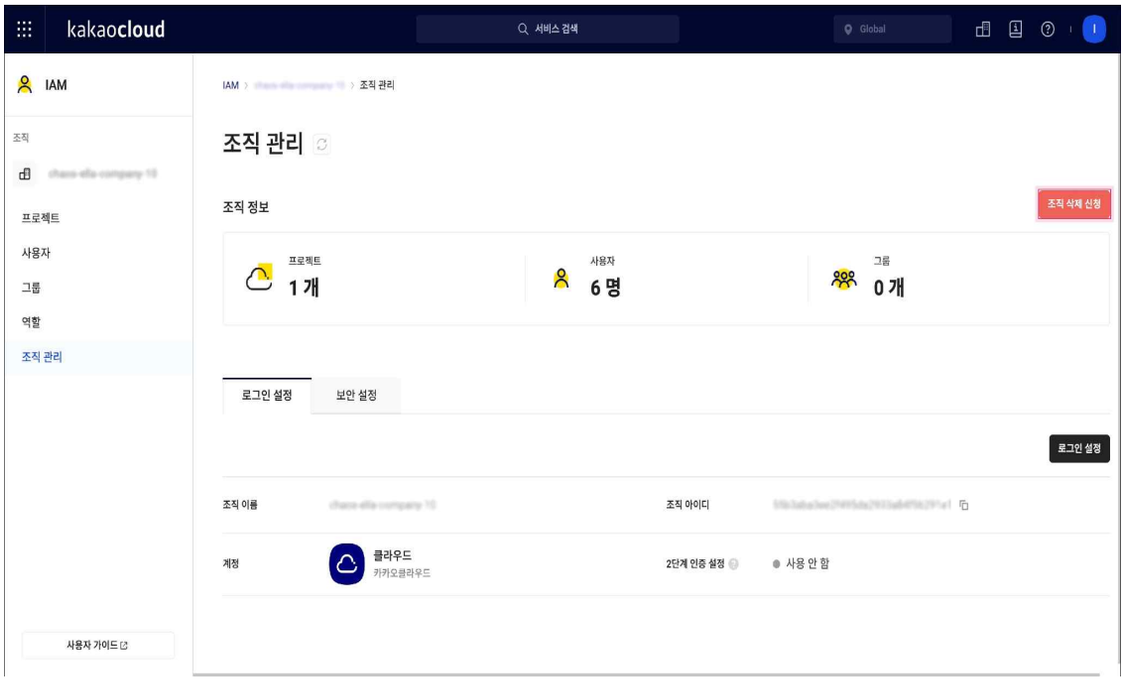


| 그림 3-1-5 | 프로젝트 레벨 역할 추가

- 단, 조직 관리자 역할을 가진 계정으로만 2단계 인증 설정, IdP 연동, 조직 삭제 신청이 가능합니다.

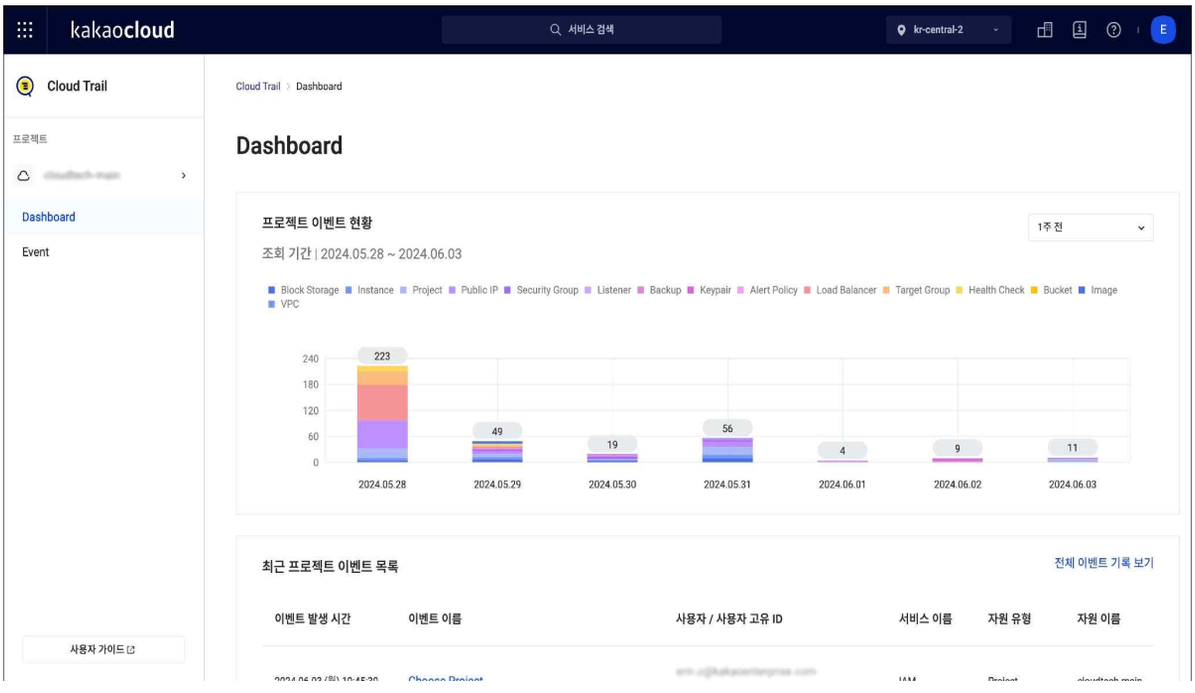


| 그림 3-1-6 | 2단계 인증 및 IdP 연동 설정

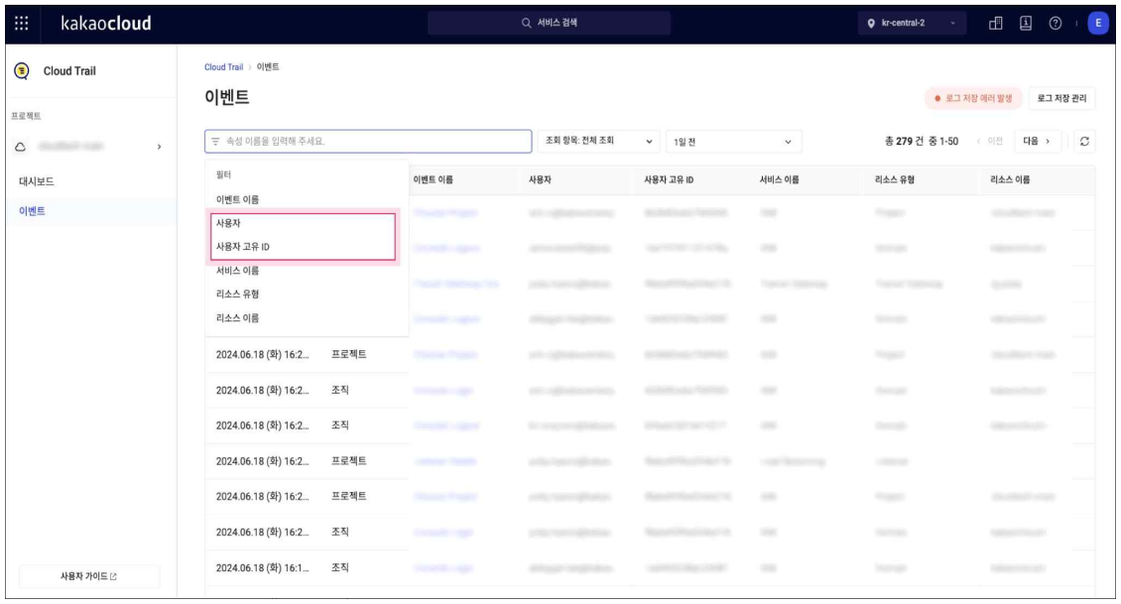


| 그림 3-1-7 | 조직 삭제 신청

- 조직 관리자의 행위는 Cloud Trail 서비스를 통해 추적이 가능하다.

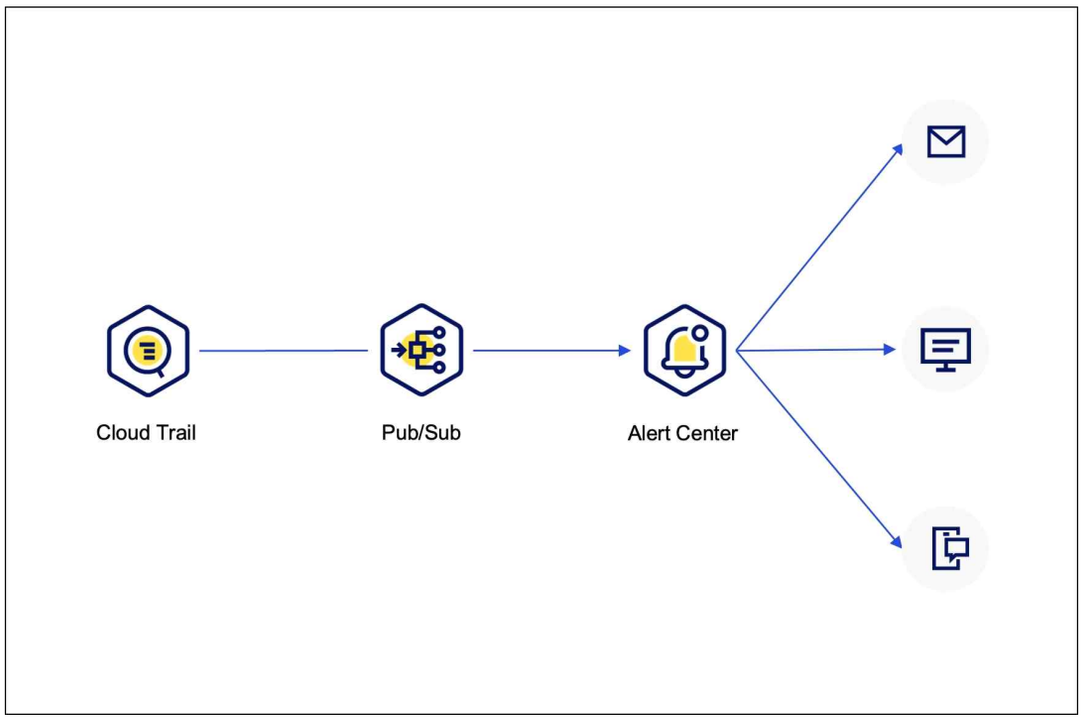


| 그림 3-1-8 | 카카오클라우드 콘솔의 Cloud Trail 서비스



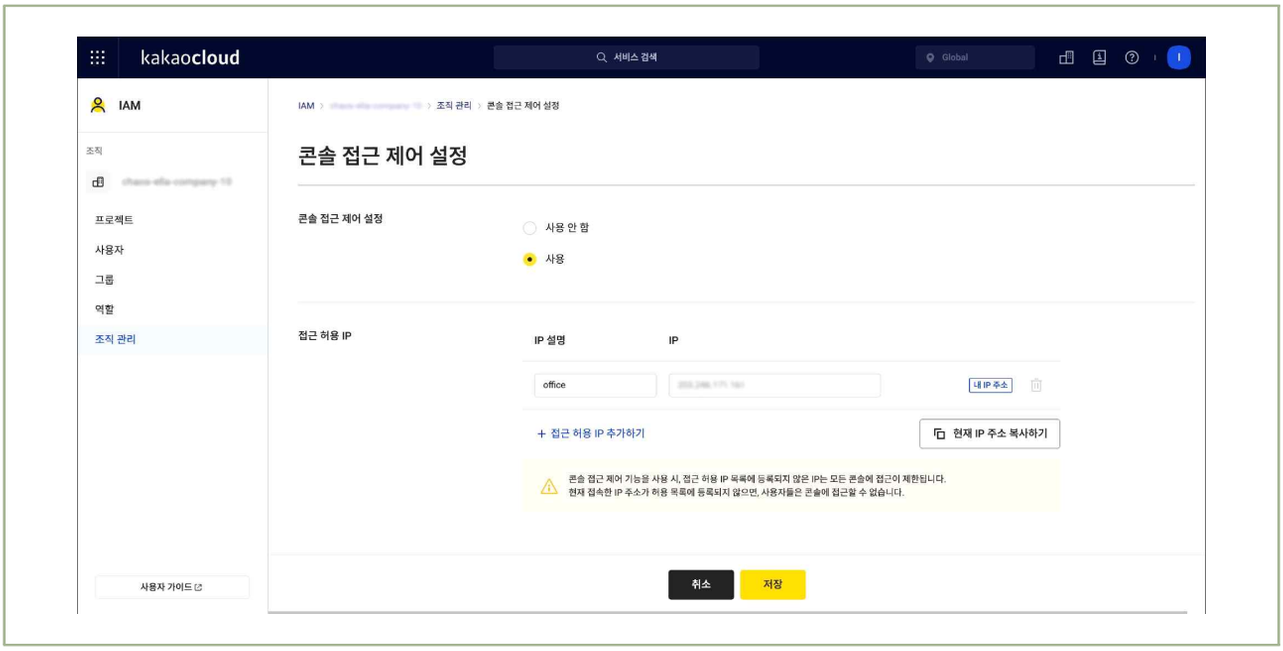
| 그림 3-1-9 | 이벤트 목록에서 사용자, 사용자 고유 ID로 검색하여 계정 관련 로그를 확인

- Cloud Trail에서 발생하는 이벤트 데이터를 Pub/Sub과 Alert Center를 통해 모니터링 알림을 구성할 수 있습니다.



| 그림 3-1-10 | CloudTrail 로그를 Pub/Sub과 Alert Center를 이용한 알림 정책 구성

- 조직 관리자 권한이 있는 경우, IP를 기반으로 콘솔 접근을 제어하여, 허용되지 않은 장소에서 카카오클라우드 사용자가 콘솔을 이용하는 것을 방지할 수 있습니다.



| 그림 3-1-11 | 콘솔 접근 허용 IP 설정

4 참고 사항

- 카카오클라우드 IAM 역할 관리 가이드
- 카카오클라우드 조직 로그인 설정 가이드 (2단계 인증, IdP 연동, 비밀번호 만료 설정)
- 카카오클라우드 콘솔 접근 제어 설정 가이드

1 기준

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

2 설명

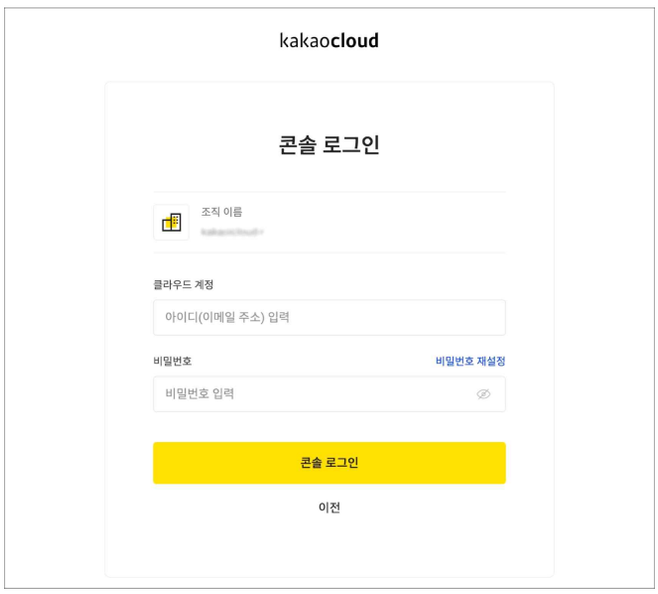
- 클라우드 서비스를 이용하는 임직원(이용자) 별 인증 수단을 부여하여야 하며, 필요시 추가인증을 적용할 수 있어야 한다.(외부직원 포함)

  - 예시

    1) IAM(Identity and Access Management) 기능 등을 이용하여 이용자별 인증수단 적용
    2) 업무 중요도에 따른 MFA 추가 인증(OTP, 바이오인증 등) 고려

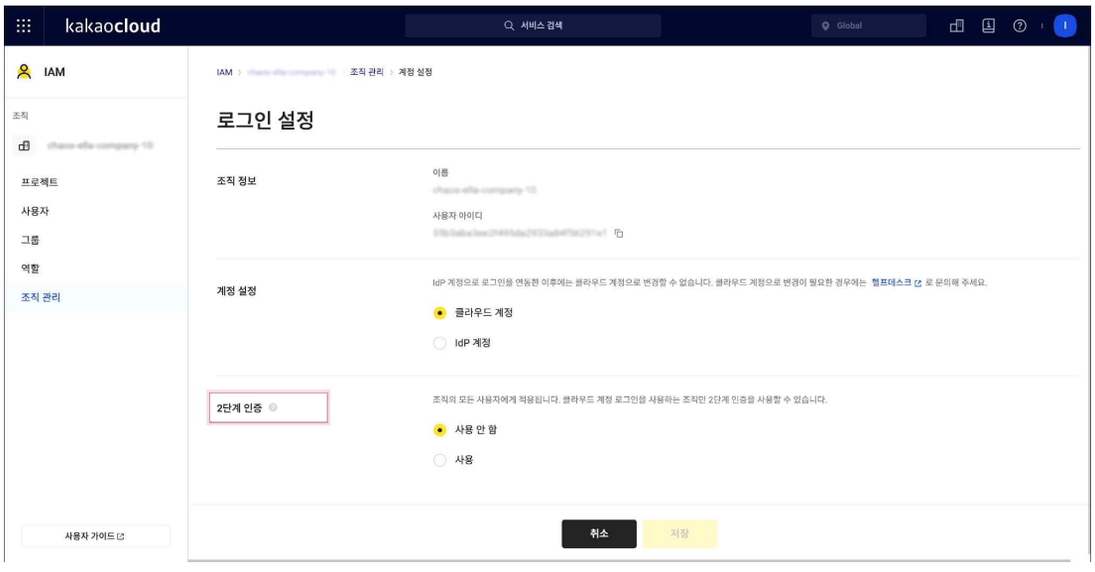
3 우수 사례

- 카카오클라우드에서는 로그인 시 기본 인증 수단으로 사용자 ID 와 암호를 사용합니다.

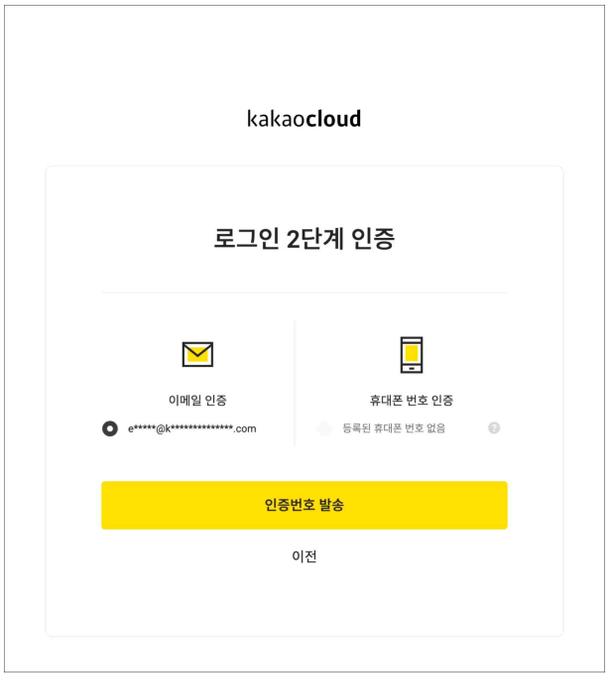


| 그림 3-2-1 | 카카오클라우드 콘솔 로그인 화면

- 추가로 2단계 인증 설정을 통해 메일이나 SMS 로 인증하도록 설정 가능합니다. 단, 해당 설정은 조직 관리자 역할을 가진 계정으로만 가능합니다.

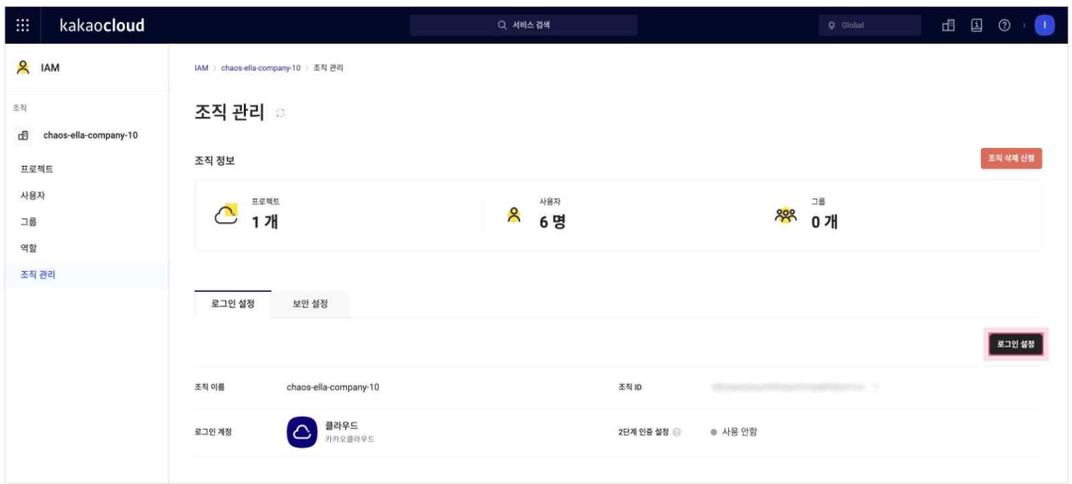


| 그림 3-2-2 | 2단계 인증 설정

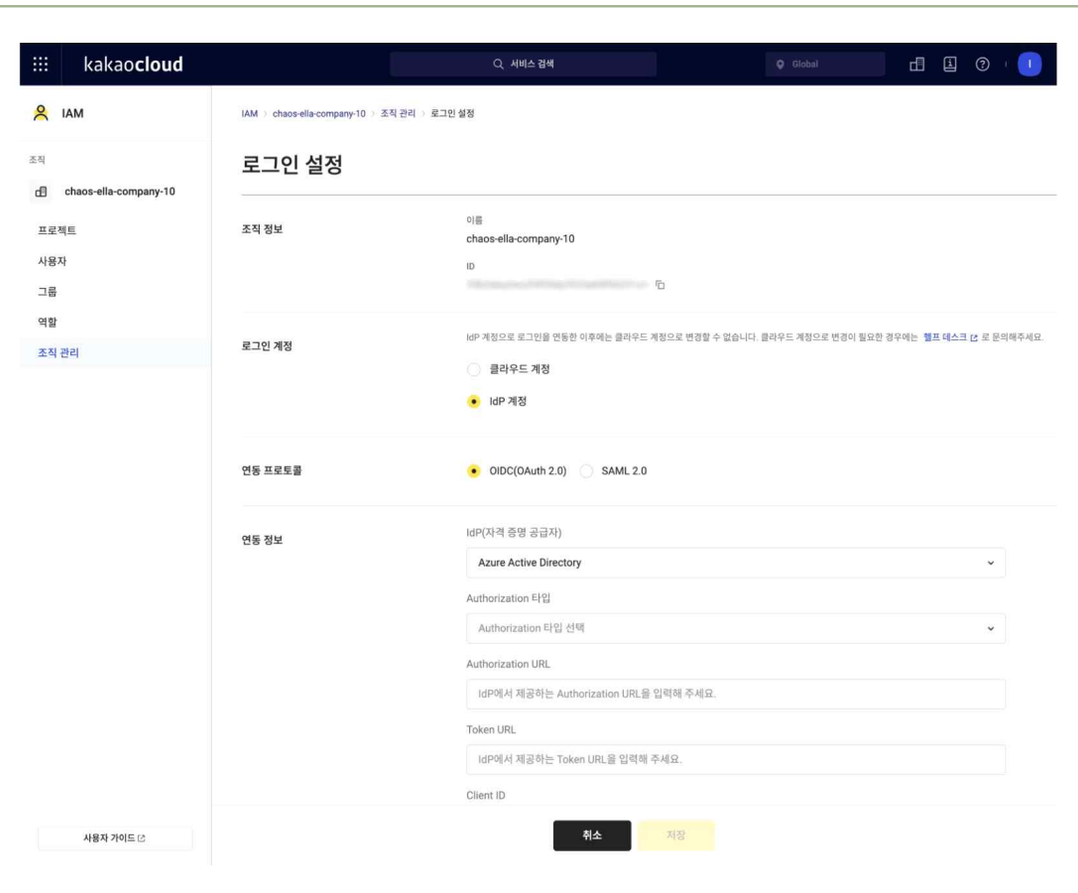


| 그림 3-2-3 | 카카오클라우드 콘솔 로그인 2단계 인증

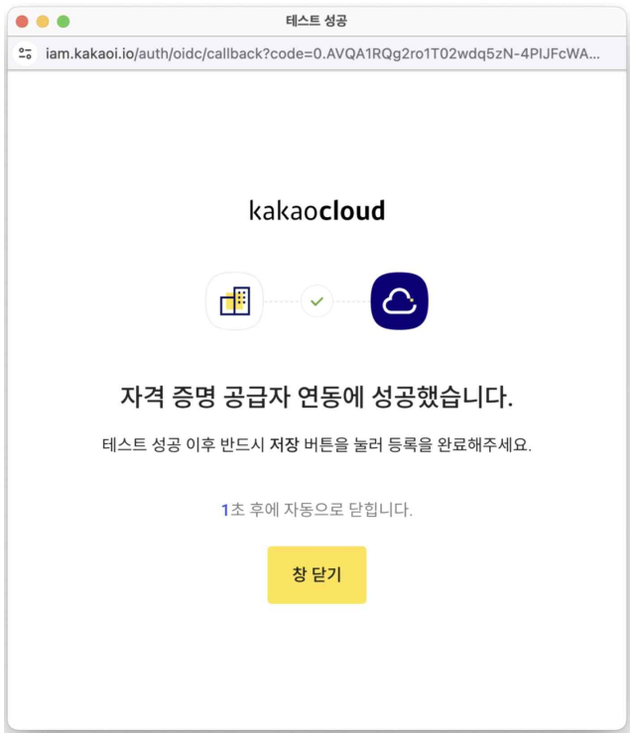
- 그 외에도 IdP 연동을 통해 Microsoft Entra ID 를 연동하여 사용하도록 설정 가능합니다.



| 그림 3-2-4 | 로그인 설정



| 그림 3-2-5 | 연동 정보 입력



| 그림 3-2-6 | 연동 테스트 성공 화면

4 참고 사항

- 카카오클라우드 조직 생성 및 로그인 가이드
- 카카오클라우드 로그인 2단계 인증 가이드
- 카카오클라우드 IdP 연동 가이드

1 기준

식별번호	기준	내용
3.3.	**인사 변경사항 발생 시 계정 관리**	**이용자의 인사변경(휴직, 전출, 퇴직 등) 발생 시 지체없이 이용자 계정 삭제, 중지 등의 조치를 수행하여야 한다.**

2 설명

- 클라우드를 이용하는 임직원의 인사 변경사항 발생 시 지체없이 이용자 계정 삭제, 중지 등의 조치를 수행하여야 한다.

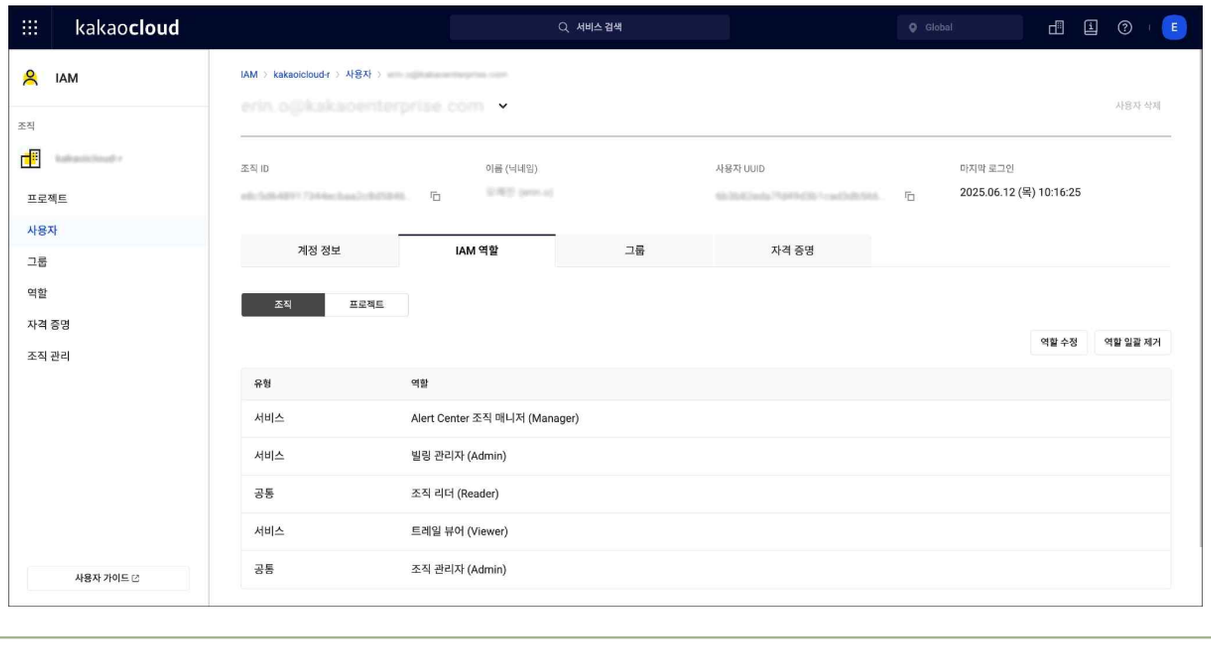
  - 예시

    1) 인사변경이 발생한 이용자의 계정 삭제 또는 중지

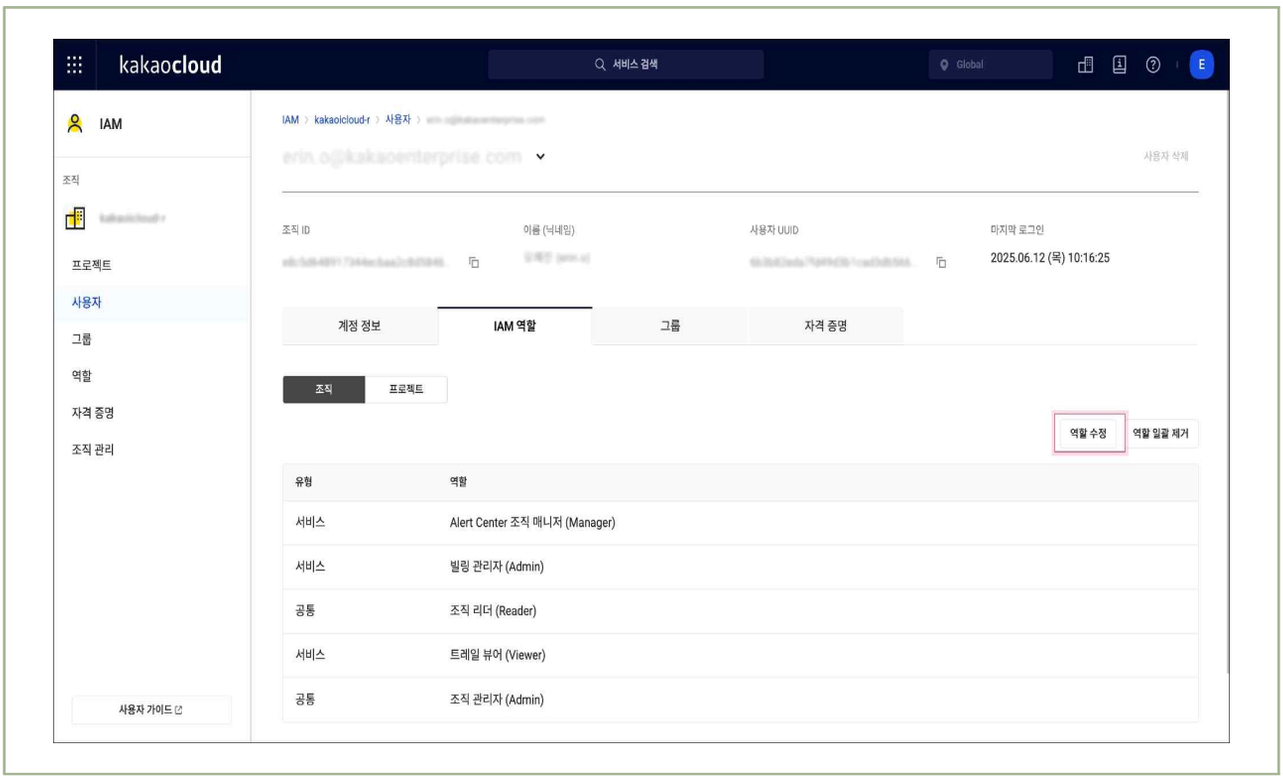
    2) 인사변경이 발생한 이용자가 공용 계정 이용 시 계정 비밀번호 변경 등

3 우수 사례

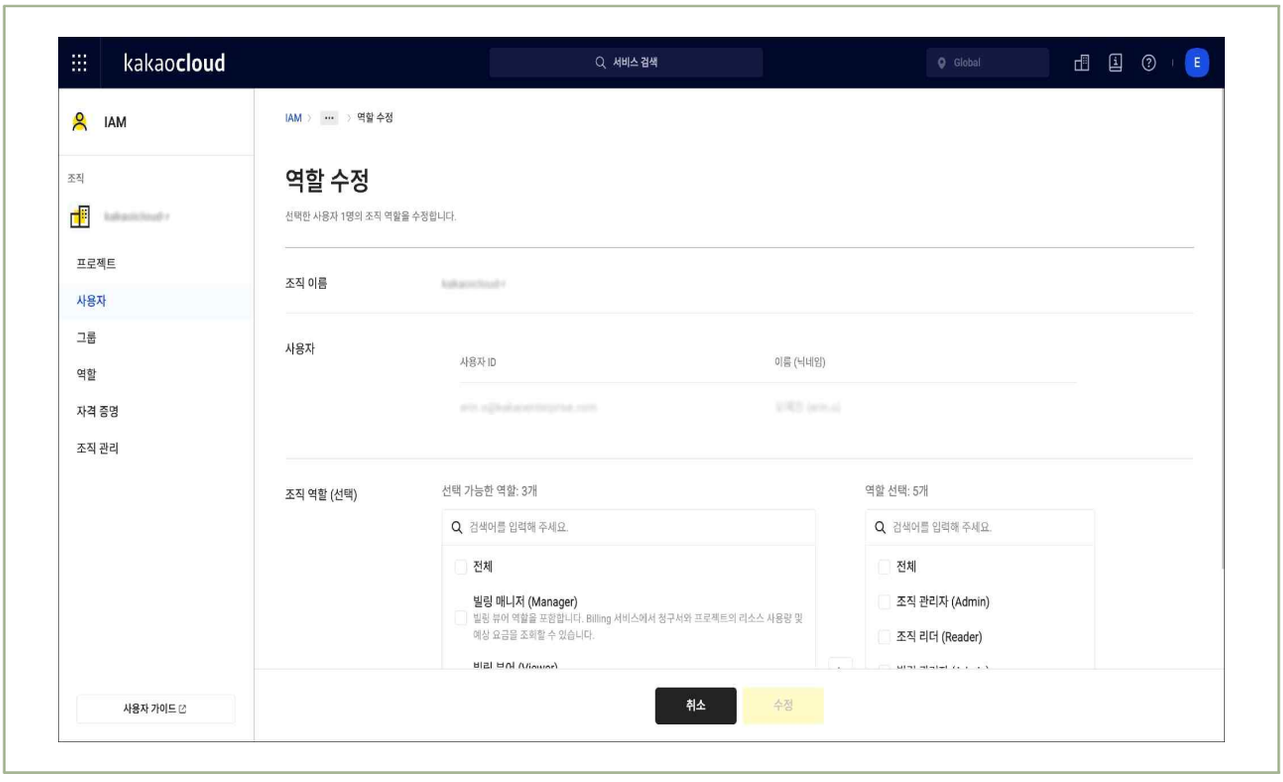
- 카카오클라우드에서는 조직, 프로젝트 단위로 사용자에게 권한을 부여하는 방식을 제공합니다.



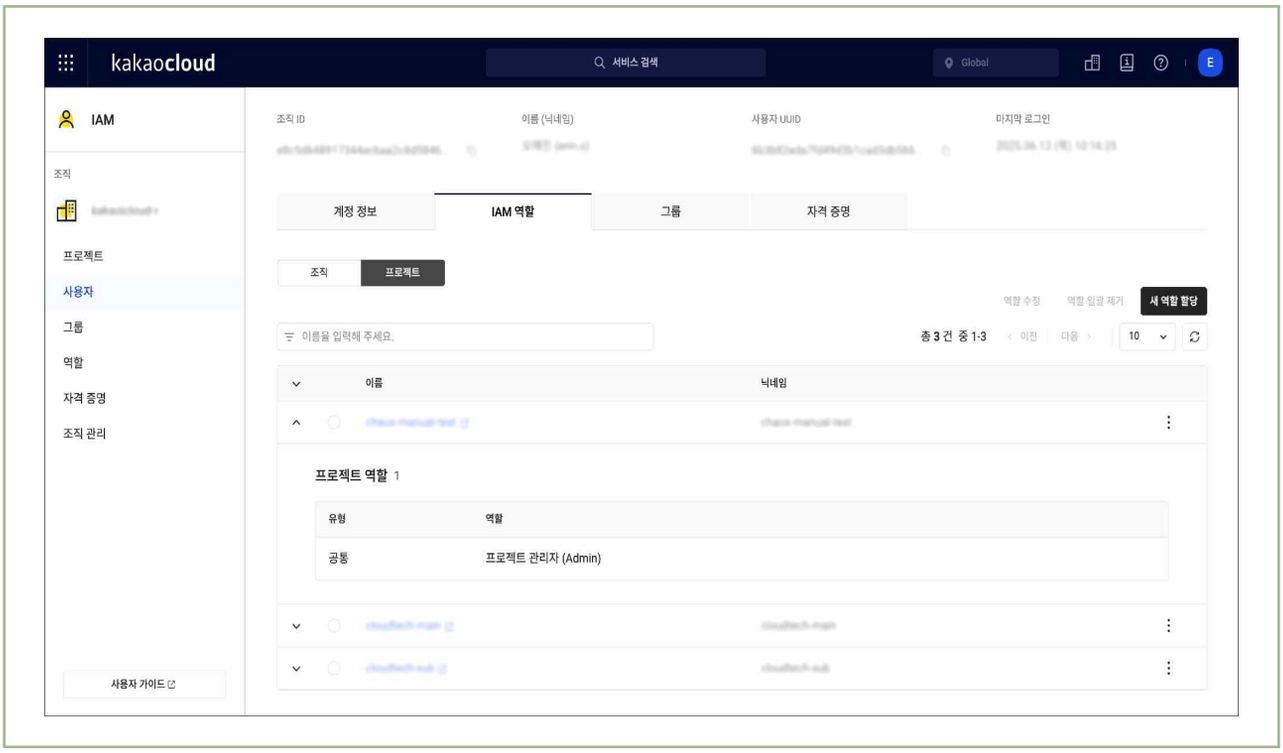
| 그림 3-3-1 | 조직 - 조직 관리 〉 사용자 〉 IAM 역할 〉 조직 탭



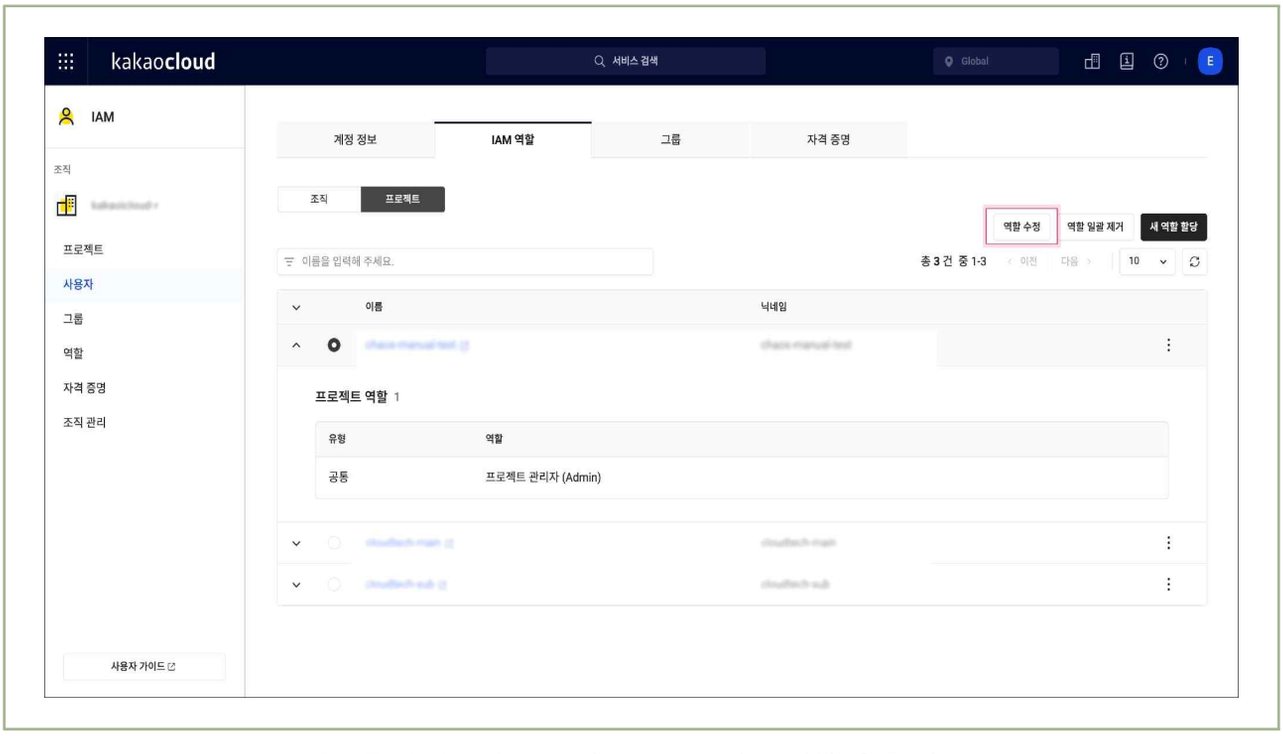
| 그림 3-3-2 | 조직 - 조직 레벨 역할 수정



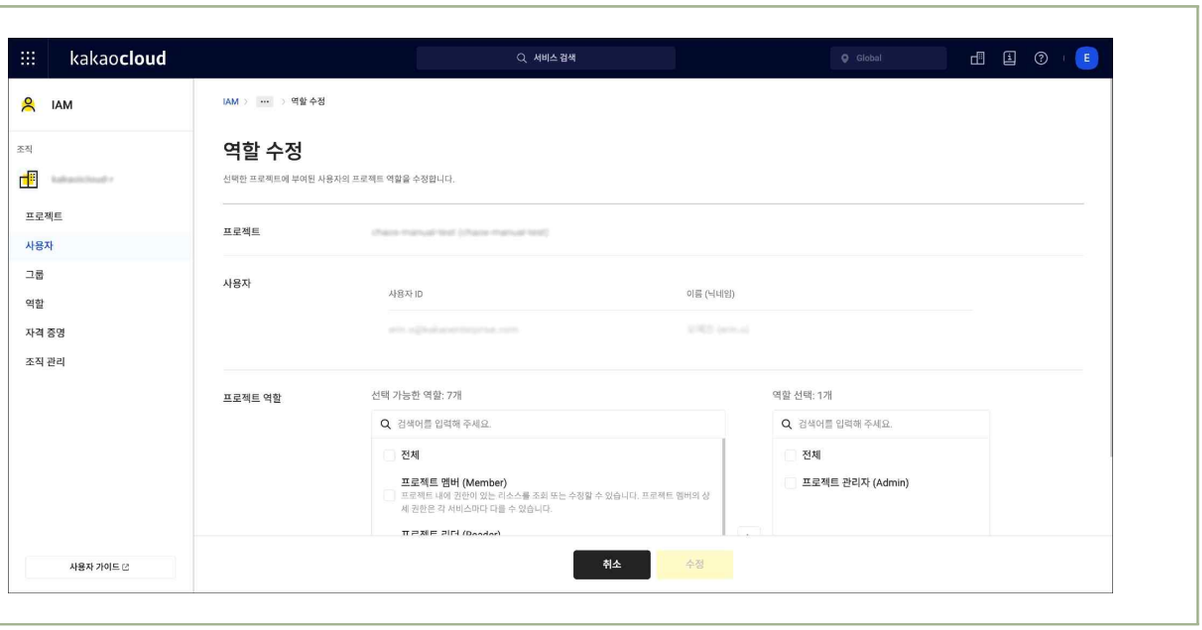
| 그림 3-3-3 | 조직 - 조직 레벨 역할 수정 모달



| 그림 3-3-4 | 프로젝트 – 프로젝트 레벨 역할 확인

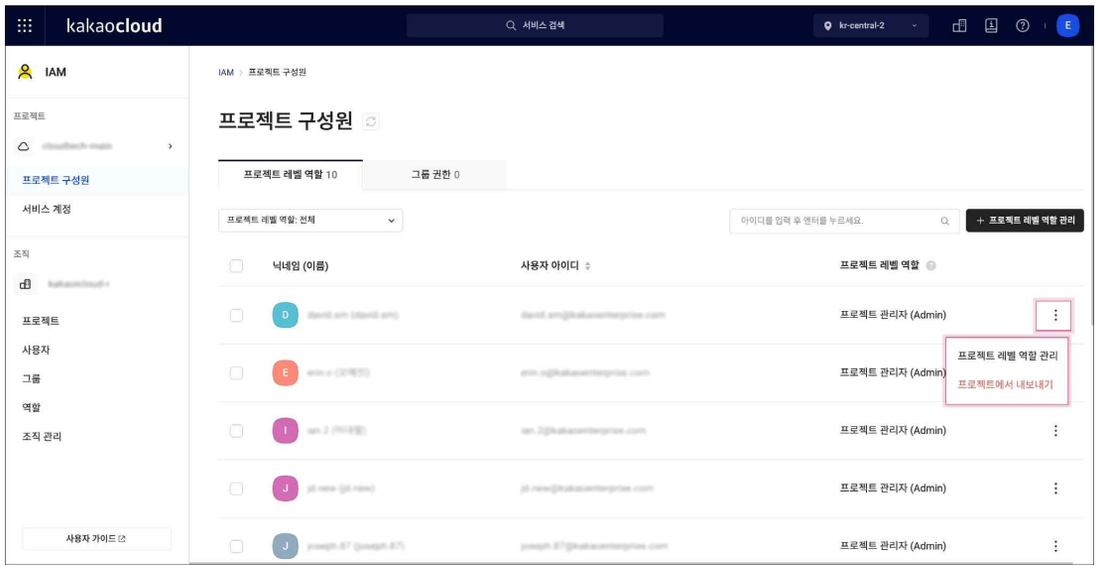


| 그림 3-3-5 | 프로젝트 – 프로젝트 레벨 역할 수정



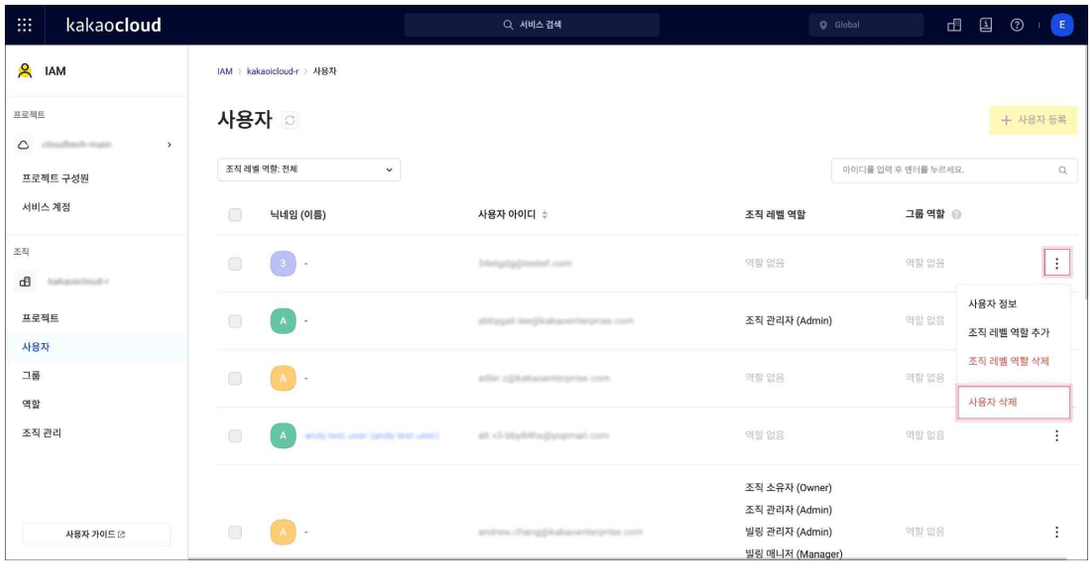
| 그림 3-3-6 | 프로젝트 – 프로젝트 레벨 역할 수정 모달

- 조직, 프로젝트 구분을 회사 및 회사 내 조직 단위의 목적에 따라 구분지어서 구성하고, 인사변경이 발생한 경우 해당 사용자에게 부여한 프로젝트 권한 변경/삭제 및 사용자 삭제 등의 방식으로 인사변경에 따른 조치를 진행합니다.

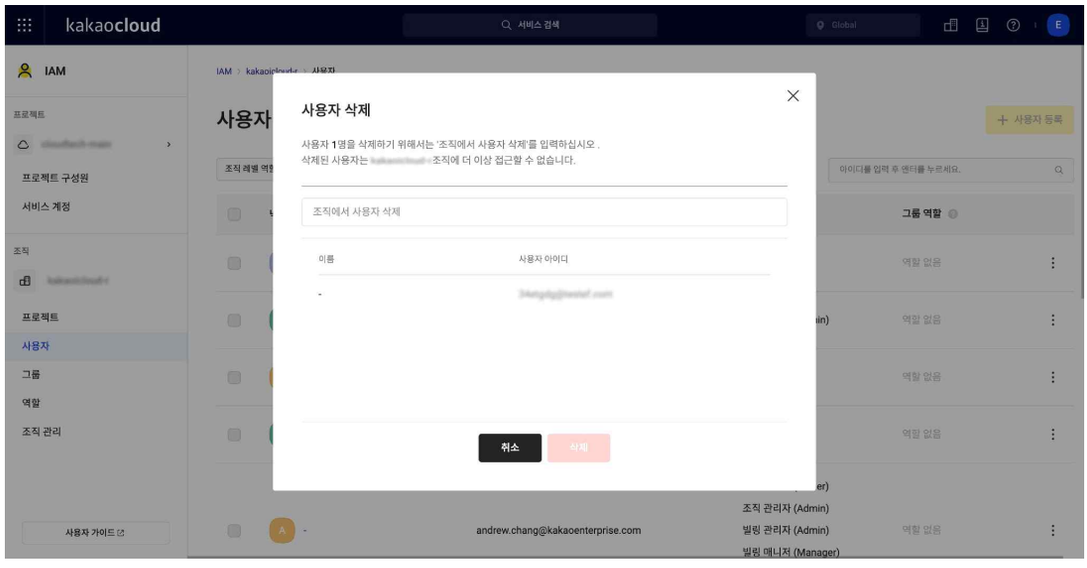


| 그림 3-3-7 | 프로젝트 권한 변경/삭제 및 프로젝트에서 사용자 내보내기

- 예를 들어, 회사 전체를 조직으로 봤을 때 실 또는 팀별로 프로젝트를 생성하여 권한을 부여하고 특정 인원에 대한 인사이동이 발생했을 경우 프로젝트별로 부여한 역할을 변경하면 됩니다. 퇴사의 경우 해당 사용자에 대한 계정을 삭제합니다.



| 그림 3-3-8 | 퇴사자의 경우, 사용자 삭제 진행



| 그림 3-3-9 | 사용자 삭제 모달

4 참고 사항

- 카카오클라우드 IAM 역할 관리 가이드

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

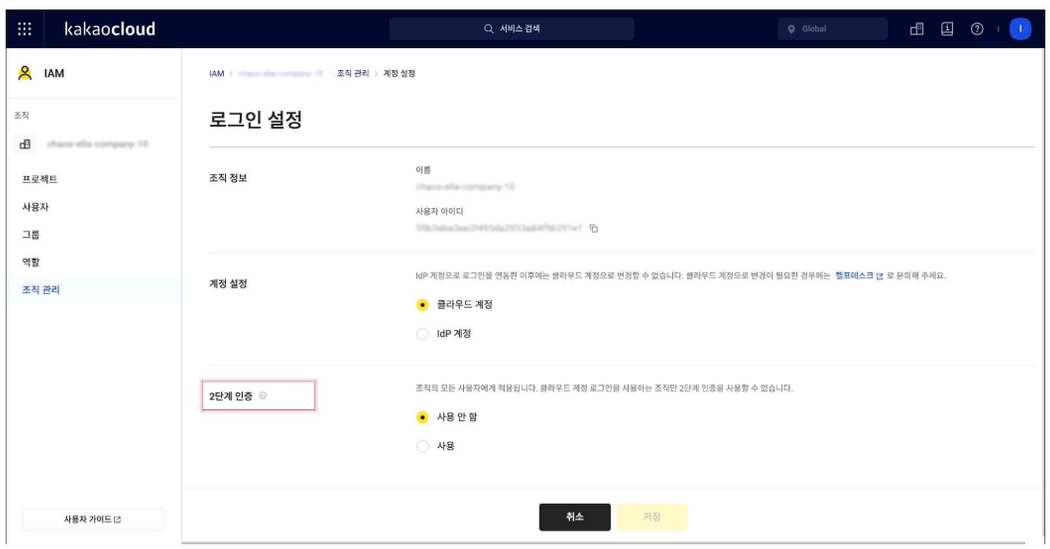
- 클라우드 환경(콘솔 등)에 관리자 권한으로 로그인 시 추가인증 수단을 적용하여야 한다.

  - 예시

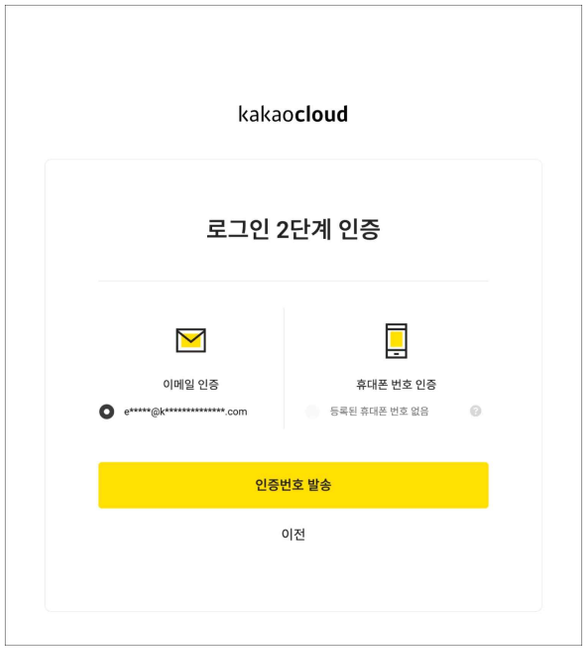
    1) 이메일 인증
    2) SMS 인증
    3) 별도 인증도구(OTP, 바이오인증 등) 활용 등

3 우수 사례

- 카카오클라우드에서는 루트 계정 권한을 조직소유자 권한으로 정의하고, 조직소유자에 한해서 소유한 조직의 2단계 인증 수단을 설정할 수 있도록 합니다. 인증 수단은 이메일 또는 휴대폰 인증을 사용합니다.



| 그림 3-4-1 | 2단계 인증 설정



| 그림 3-4-2 | 카카오클라우드 콘솔 로그인 2단계 인증

4 참고 사항

- 카카오클라우드 로그인 2단계 인증 가이드

1 기준

식별번호	기준	내용
3.5.	**클라우드 가상자원 관리 시스템 로그인 규칙 수립**	**이용자 가상자원 관리 시스템 접근 계정에 대한 안전한 로그인 규칙을 수립하여야 한다.**

2 설명

- 이용자는 패스워드 무작위 대입 공격등에 대응하기 위해 가상자원 관리 시스템 계정에 대한 안전한 로그인 규칙을 수립하여야 한다.

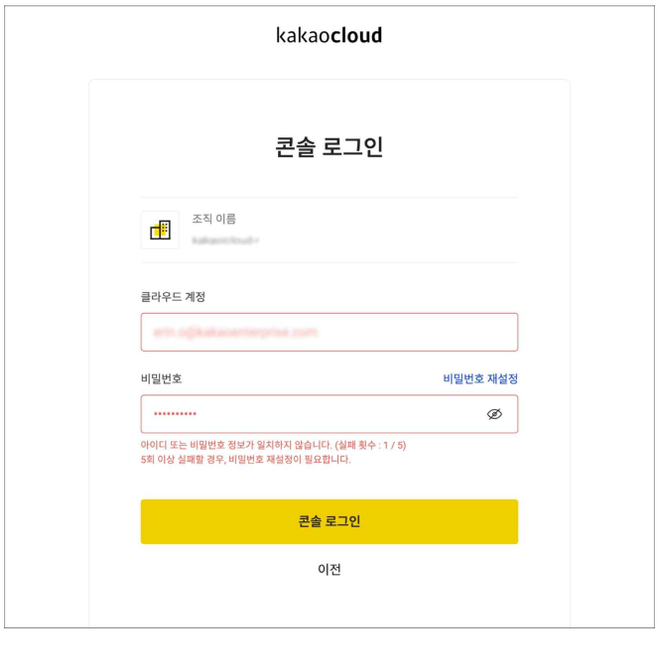
  - 예시

    1) 로그인 오류에 따른 보안통제 방안 수립 등

3 우수 사례

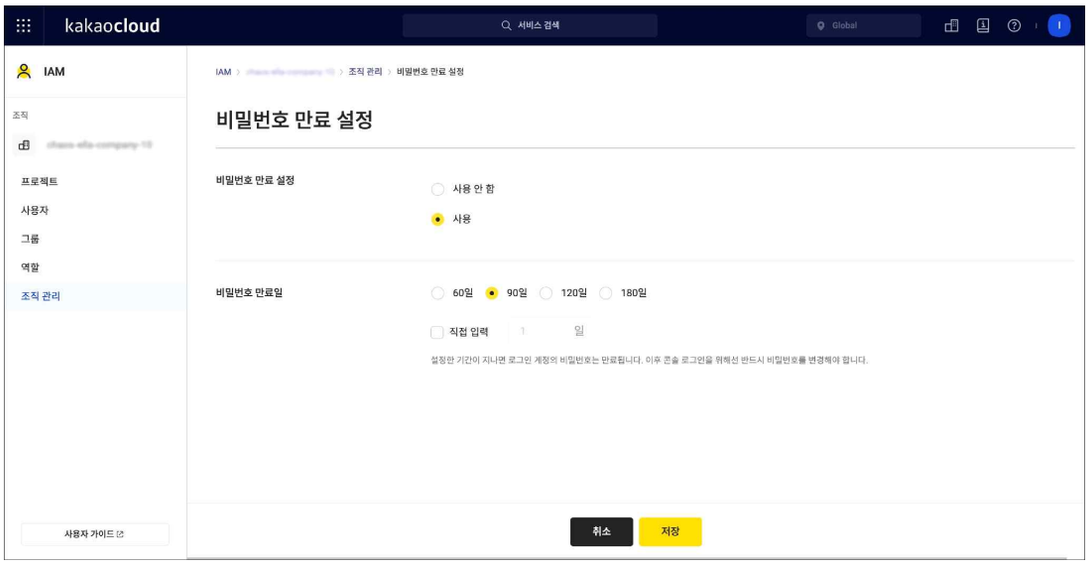
- 로그인 오류에 따른 보안통제 방안

  - 카카오클라우드에서는 비밀번호를 5회 이상 잘못 입력할 경우, 비밀번호 재설정이 필요합니다.



| 그림 3-5-1 | 비밀번호 5회 이상 잘못 입력할 경우, 비밀번호 재설정 경고 문구

- 또한, 비밀번호 만료 설정 기능을 통해 비밀번호를 새로 설정해야하는 주기를 설정할 수 있습니다. 30~180일 이내로 설정 가능합니다.



| 그림 3-5-2 | 비밀번호 만료 설정 기능

4 참고 사항

- 카카오클라우드 로그인하기 가이드
- 카카오클라우드 비밀번호 만료 설정 가이드

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

- 클라우드 가상자원 관리시스템 접근 가능한 계정 생성 시 안전한 비밀번호 규칙을 수립하여 적용하여야 한다.

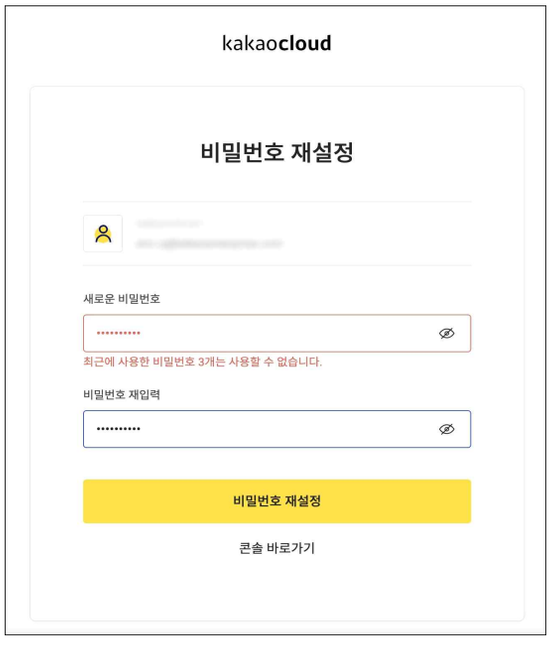
  - 예시

    1) 제3자가 쉽게 유추할 수 없는 비밀번호 작성 규칙 수립

3 우수 사례

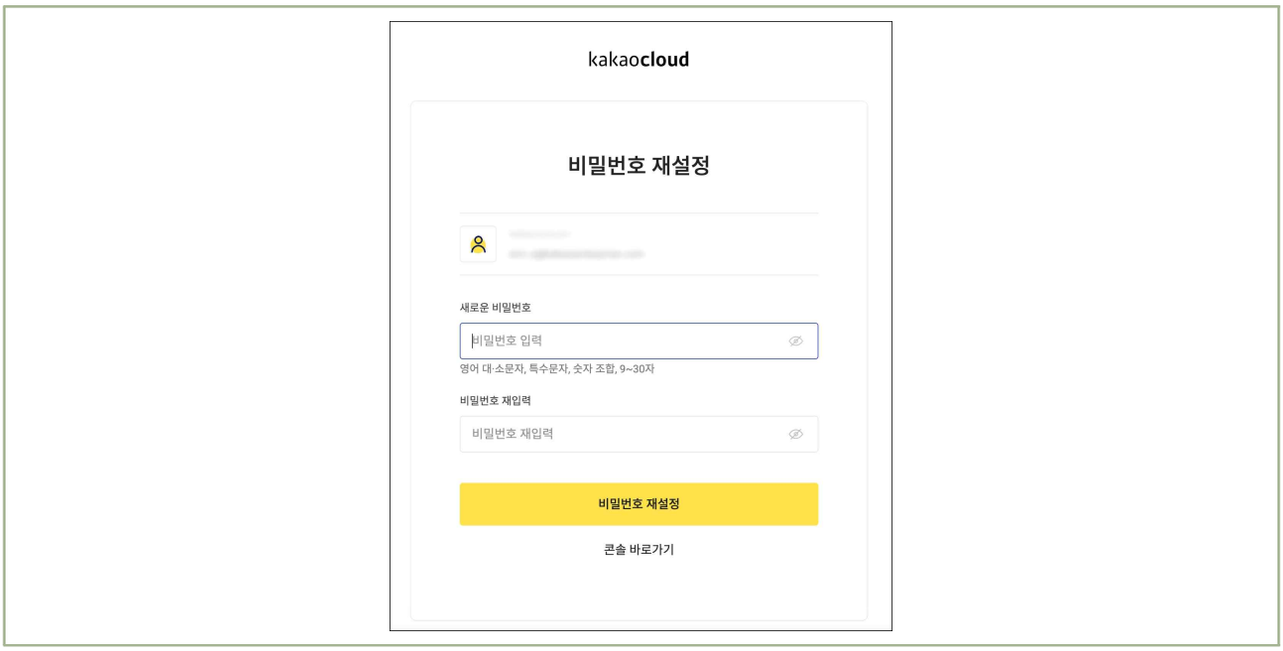
- 제3자가 쉽게 유추할 수 없는 비밀번호 작성 규칙 수립

  - 비밀번호는 최근 사용한 3개의 암호는 재설정 시 사용이 불가능합니다.



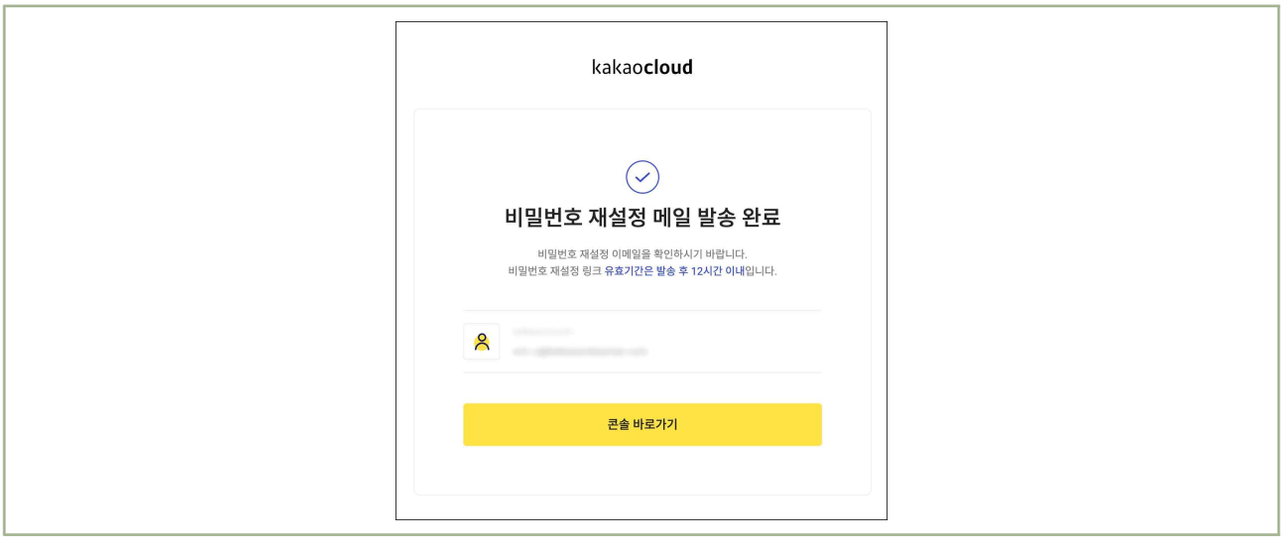
| 그림 3-6-1 | 최근에 사용한 비밀번호 3개는 사용 불가능 문구

- 비밀번호는 영어 대·소문자, 특수문자, 숫자를 조합하여 9~30자로 설정해야합니다.



| 그림 3-6-2 | 비밀번호 재설정 시, 요구 조건

- 비밀번호는 초대 이후 12시간 이내 미설정 시 재설정 요청을 통해서만 설정이 가능합니다.



| 그림 3-6-3 | 비밀번호 재설정 메일 발송 완료 안내

4 참고 사항

- 카카오클라우드 비밀번호 변경/재설정 가이드

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 제한하여야 한다.

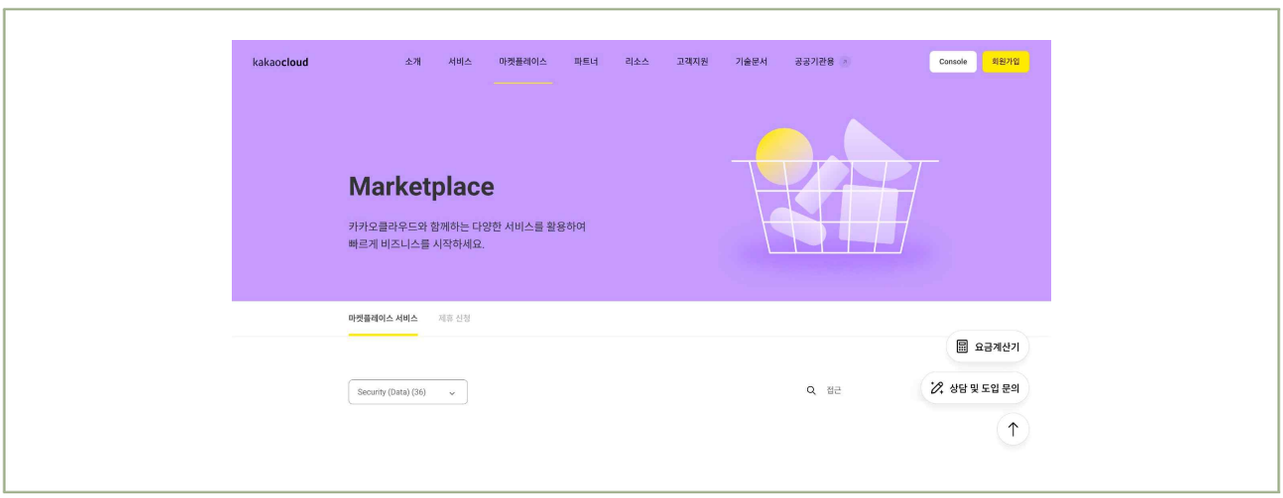
  - 예시

    1) 계정 관리 기능을 통해 공개용 웹서버만 접근 가능한 계정을 개인별 부여하여 관리

    2) 공개용 웹서버에 접근 가능한 계정으로 로그인 시 추가인증 수단 적용 등

3 우수 사례

- 마켓플레이스에 등록된 3rd party 솔루션을 통해 접근제어 설정이 가능합니다.



| 그림 3-7-1 | 카카오클라우드 마켓플레이스 상품 소개 페이지

4 참고 사항

- 카카오클라우드 마켓플레이스 상품 소개

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. 암호키 호출 권한 관리
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.

  - 예시

    1) 클라우드의 키 관리 서비스를 통해 CSP 사업자의 관리형 Key로 암호화
    2) 클라우드의 키 관리 서비스를 통해 이용자 관리형 Key로 암호화
    3) 이용자가 직접 관리하는 Key로 암호화 등

3 우수 사례

* 이용자 제공용 KMS 서비스는 추후 서비스 출시 예정입니다
* 내부 서비스(Storage 류)는 카카오클라우드 내부 사용 KMS로 암호화 하고 있습니다.

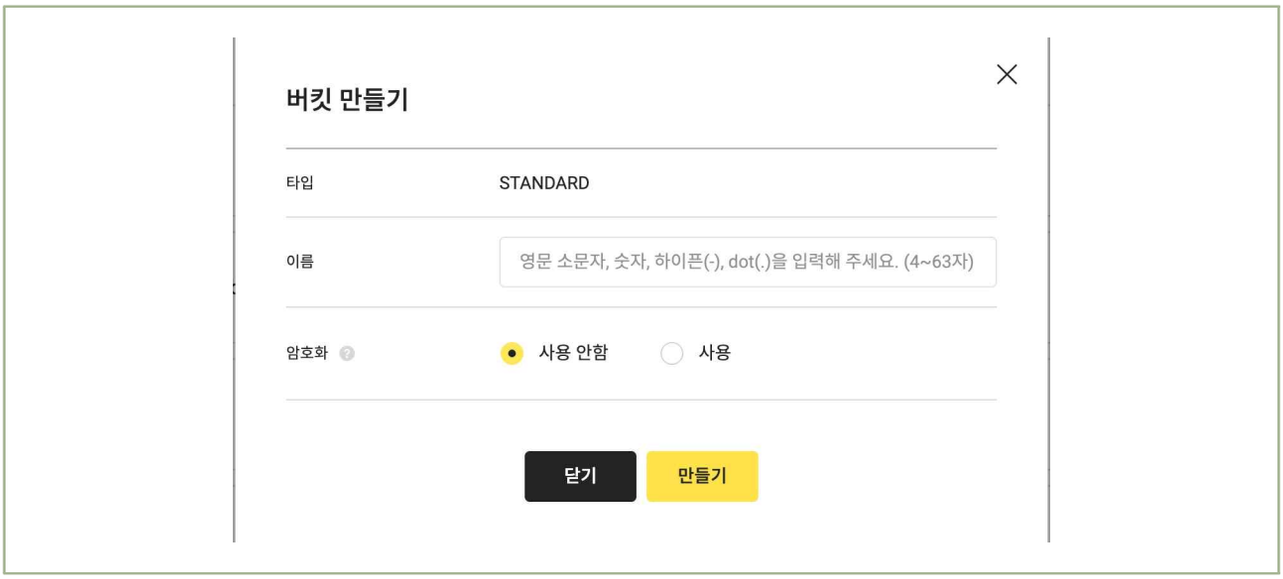
- 이용자가 운영중인 KMS를 활용하여 구성

  - On-premise IDC와 전용선 연결 후 On-premise KMS를 통하여 암복호화 수행(그림 2.1.1 카카오클라우드를 활용한 네트워크 구성도)

- (DISK 암호화) 카카오클라우드 Storage Service는 모두 Disk 암호화가 적용되어 있습니다.

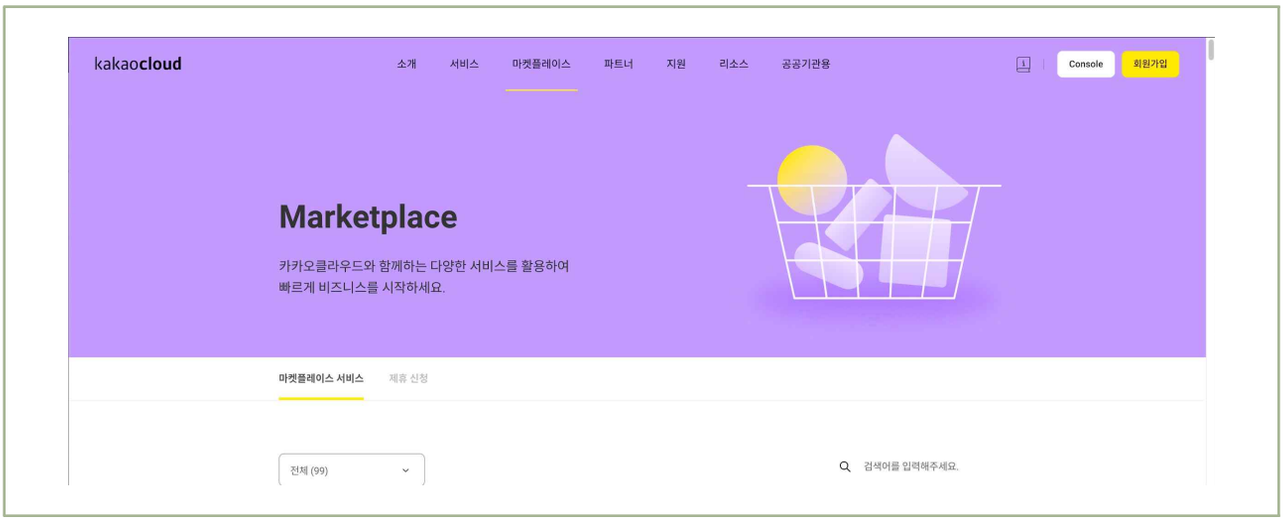
  - [File Storage] 기본 적용으로 별도의 설정 필요 없습니다.

- [Object Storage] (Console) 'Beyond Storage Service' → 'Object Storage' → '버킷 만들기'에서 암호화 "사용"으로 변경 이후 사용합니다.



| 그림 4-1-1 | Object Storage 버킷 생성

- (3rd-party) '마켓플레이스' 상품 중 Security(data) 상품 군 중 암호화 키 관리(KMS) 제품을 통하여 이용자 VPC 내 VM으로 구축하여 사용 가능합니다.



| 그림 4-1-2 | 카카오클라우드 마켓플레이스 상품 소개 페이지

4 참고 사항

- 카카오클라우드 마켓플레이스 상품 안내

1 기준

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

2 설명

- 암호화 기능 이용 시 암호키 관리 방안을 수립하여야 한다.

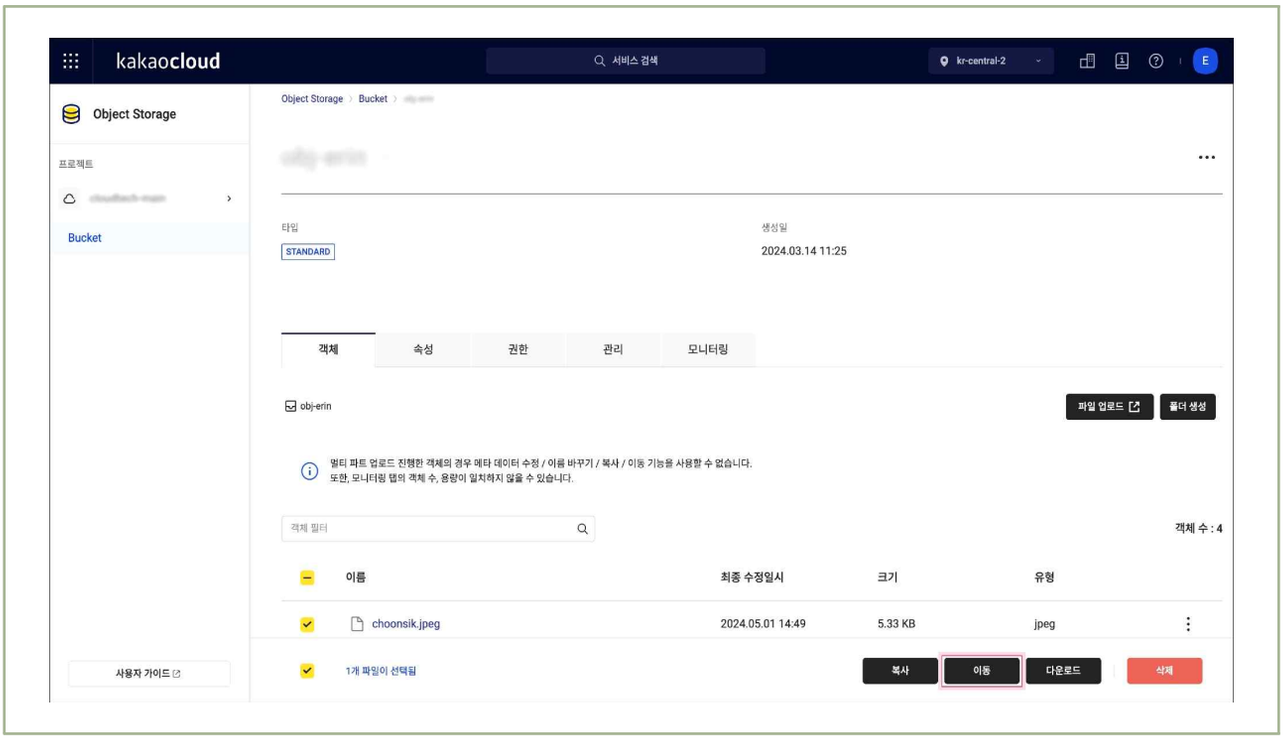
  - 예시

    1) KMS(Key Management Service)를 통한 암호화 키 방안 수립(생성, 변경, 폐기 등)
    2) 클라우드 서비스 제공자가 직접 제공하는 암호화키 이용 시 적절한 관리방안 수립
    3) 키 사용기간 수립 및 암호키 유출등에 대응할 수 있도록 키 삭제 및 재적용 관련 기능 수립
    4) 생성된 암호화키를 안전하게 보관할 수 있는 방안 수립 등

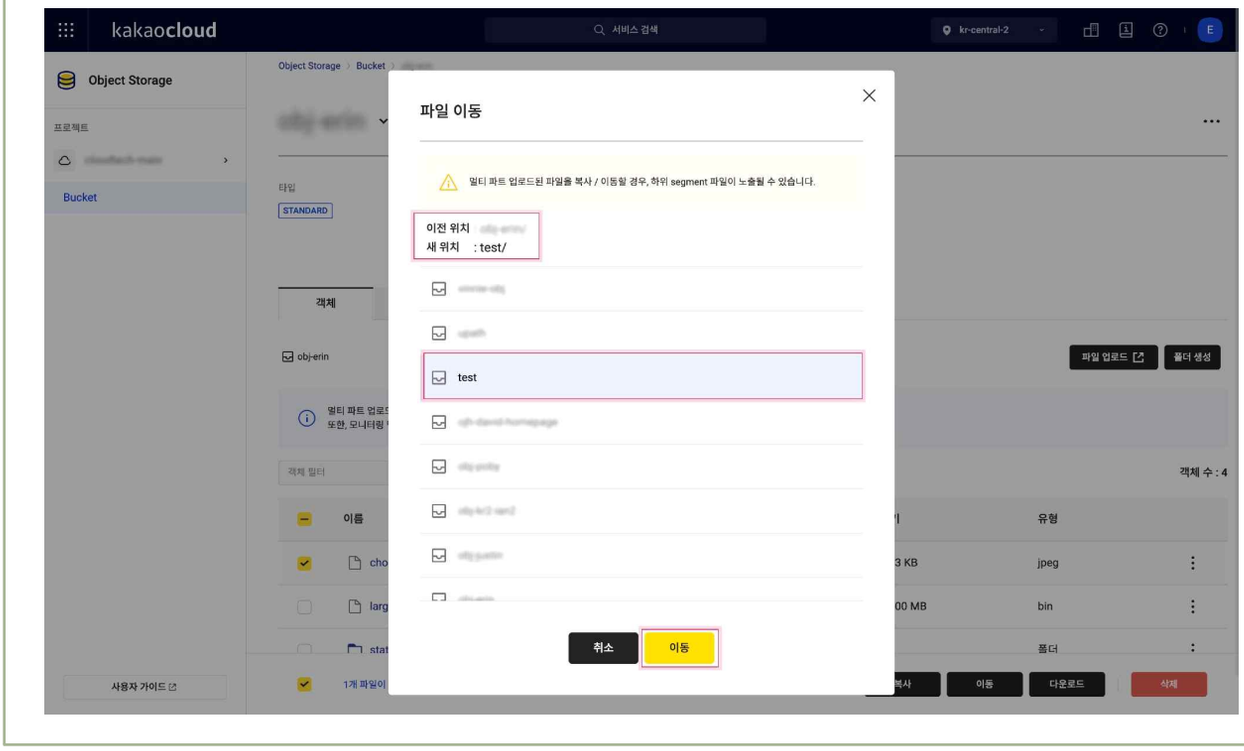
3 우수 사례

- 카카오클라우드에서는 CSP 제공자가 제공하는 암호 키 관리 기능이 없습니다.
- 다만 File, Object Storage 활용시 아래와 같이 암호 키 갱신이 가능합니다.
- [File Storage] Disk 암호키는 2년 주기로 자동 갱신이 됩니다.
- [Object Storage] 버킷별로 암호키가 생성되어 적용되므로, 신규 버킷 생성 후 파일 이동 후 기존 버킷 삭제를 통해 버킷 암호화 키 갱신이 가능합니다.
- (Console) ‘Beyond Storage Service’ → ‘Object Storage’ → ‘Bucket’ → {{기존 Bucket}} 선택 → 이동할 파일 전체 선택 → 하단 이동 → {{옮겨갈 Bucket}} 선택 후 이동 합니다.

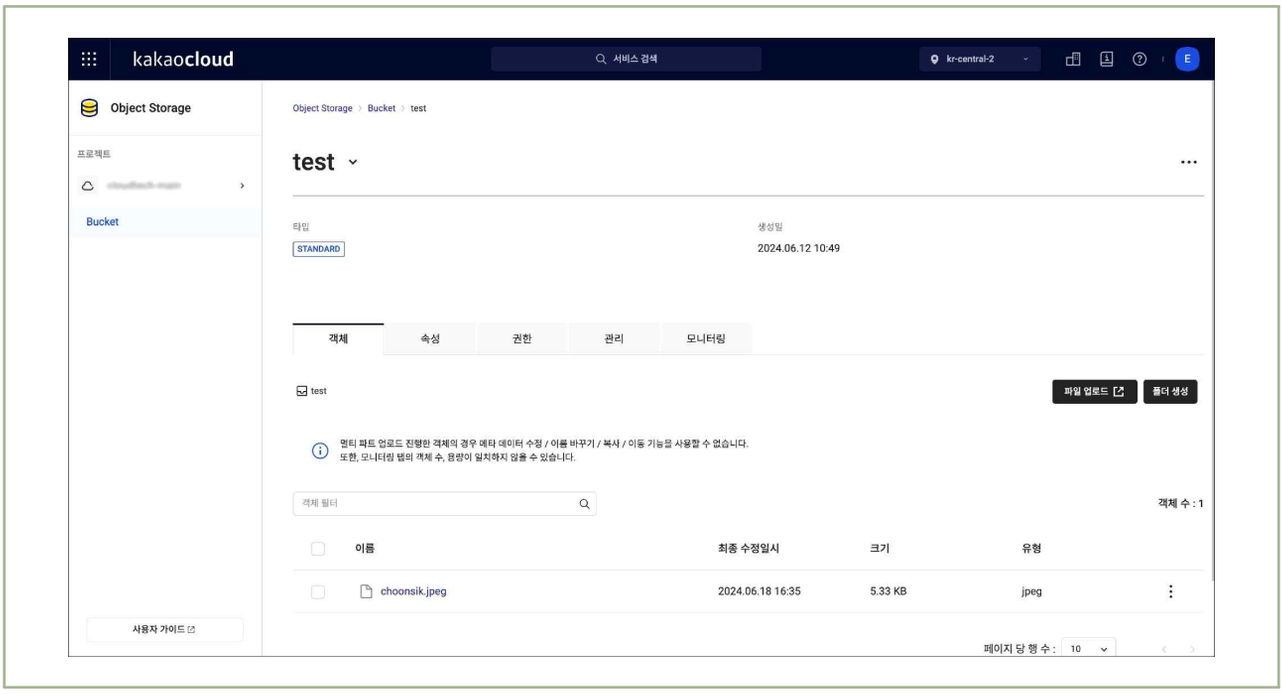
  * BYOK(Bring Your Own Key)는 추후 기능 개선 예정입니다.



| 그림 4-2-1 | Object Storage 콘솔 메뉴에서 이동할 파일 선택



| 그림 4-2-2 | Object Storage 콘솔 메뉴에서 파일 이동 실행



| 그림 4-2-3 | Object Storage 콘솔 메뉴에서 파일 이동 확인

4 참고 사항

- 카카오클라우드 Object Storage 〉 객체/파일 관리 가이드

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(ex. KMS) 이용 시 암호키 서비스 관리자 권한을 적절하게 통제하여야 한다.

  - 예시

    1) 암호키 관리 서비스 관리자 권한은 최소인원에게 부여하고 부여현황에 대해 상시모니터링 수행

    2) 사용자가 생성하는 각 키에 대해서는 관리자를 별도 지정할 수 있어야 하며, 각 조건에 따라 최소한의 권한 부여 등

3 우수 사례

- 카카오클라우드에서는 CSP 제공자가 제공하는 암호 키 관리 기능이 없습니다.
- 카카오클라우드 내부에서 사용하는 암호 키(File, Object Storage 암호화용)관리 시스템의 접근 인원은 최소한(2인)으로 권한을 부여하여 관리하고 있습니다.

4 참고 사항

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.

  - 예시

    1) 암호키 관리 서비스(KMS)를 통해 암호키 호출 시 목적에 따라 권한 부여
    2) 암호키 호출 권한 현황에 대한 모니터링 및 주기적 검토 수행

3 우수 사례

- 카카오클라우드에서는 CSP 제공자가 제공하는 암호 키 관리 기능은 없습니다.
- 카카오클라우드 내부에서 사용하는 암호 키(File, Object Storage 암호화용)는 암호 키를 사용하는 서비스(File, Object Storage)에만 호출 권한을 부여하여 관리하고 있으며, 암호키 호출에 대해서 모니터링을 통해 서비스 외의 호출을 탐지, 검토하고 있습니다.

4 참고 사항

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 적용하여야 한다.(또는 확인하여야 한다.)

  - 예시

    1) 이용자가 관리하는 암호키로 암호화 기능 적용 시 안전한 암호화 알고리즘 적용(금융부문 암호기술 활용 가이드 등 참고)

    2) 클라우드 KMS 서비스를 통해 암호화 시 안전한 암호화 알고리즘을 제공하는지 확인

3 우수 사례

- 카카오클라우드에서는 CSP 제공자가 제공하는 암호 키 관리 기능은 없습니다.
- 카카오클라우드 내부에서 사용하는 암호 키(File, Object Storage 암호화용)는 안전 암호화 알고리즘을 적용(256 bit 이상)하여 암호화하고 있습니다.

4 참고 사항

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 행위에 대한 추적성(로그 등)을 확보하여야 한다.**

2 설명

- 이용자의 가상자원 이용 관련 일련의 행위에 대한 추적성을 확보할 수 있는 방안이 마련되어야 한다.

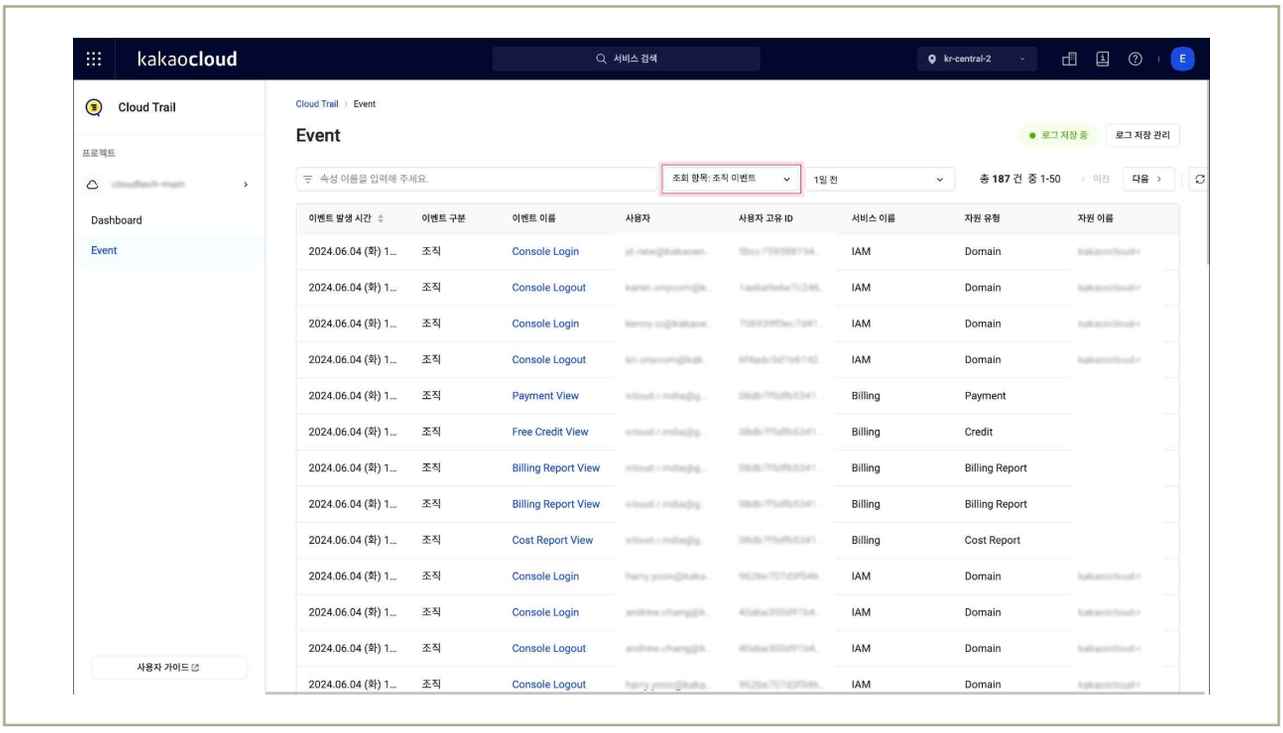
  - 예시

    1) 가상자원 변경 사항에 관한 행위(생성, 변경, 삭제 등)
    2) 가상자원에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근기록
    3) 가상자원을 사용한 일시, 사용자 및 가상자원의 형태(서버, 데이터베이스, 스토리지 등)를 확인할 수 있는 접근기록
    4) 가상자원내 전산자료의 처리 내용을 확인할 수 있는 사용자 로그인, 액세스 로그 등 접근기록

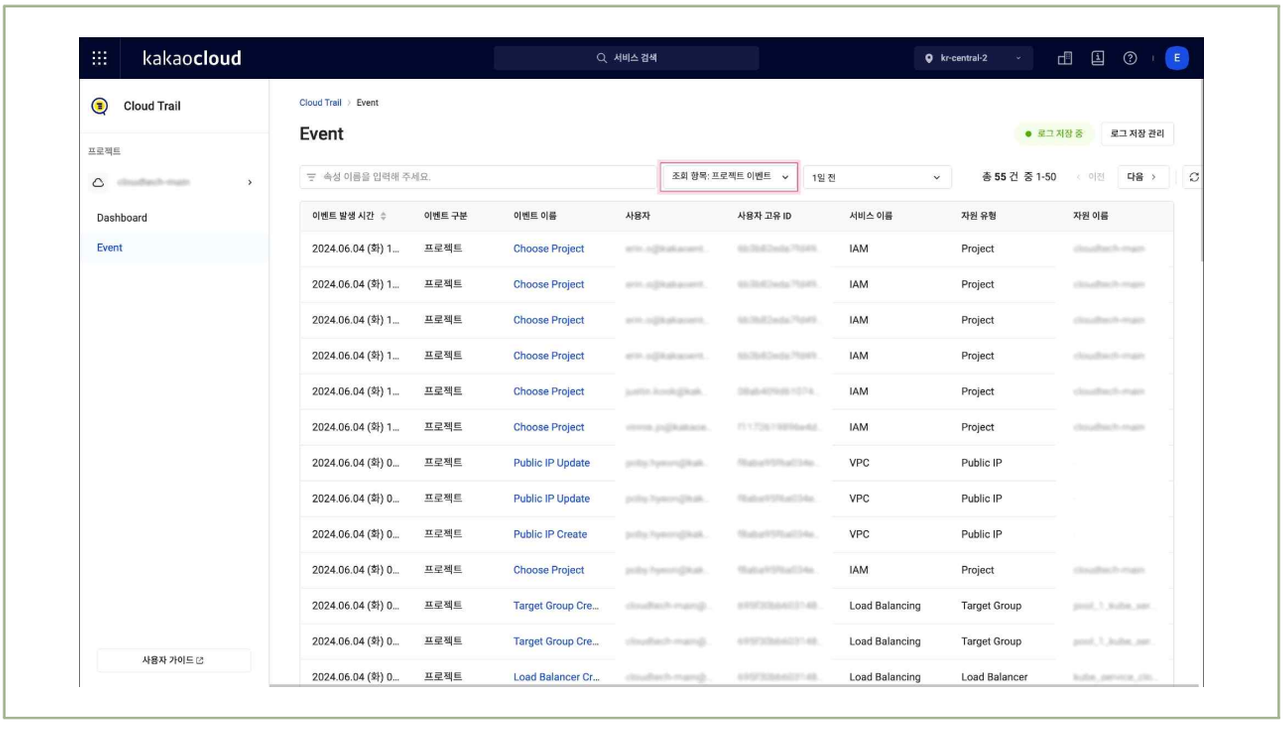
3 우수 사례

- 가상자원 변경 사항에 관한 행위(생성, 변경, 삭제 등)

  - 카카오클라우드에서는 가상자원 이용에 관한 행위에 대해 추적 가능하도록 Cloud Trail 서비스를 제공합니다. Cloud Trail의 이벤트는 조직 이벤트와 프로젝트 이벤트로 구분되며, 가상자원 이용에 관한 행위는 프로젝트 이벤트로 확인이 가능합니다.

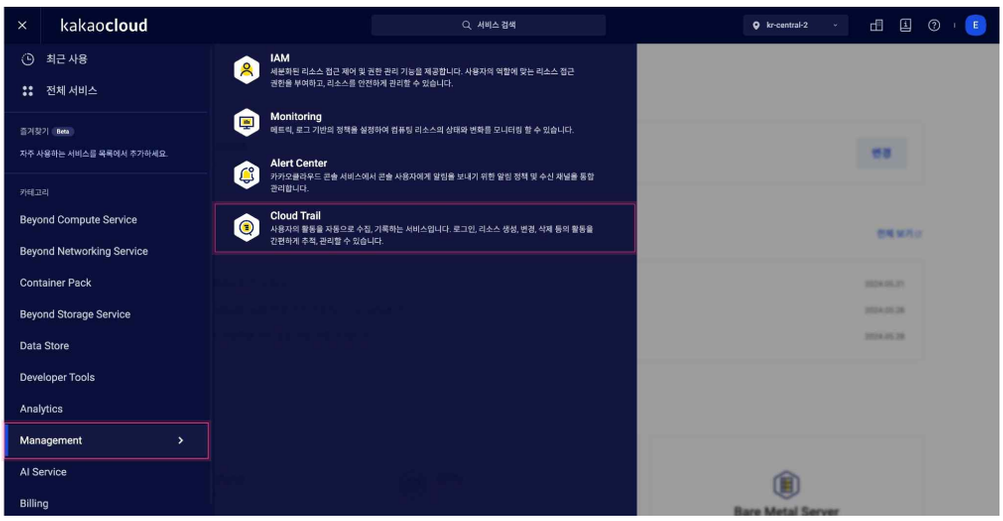


| 그림 5-1-1 | Cloud Trail 의 조직 이벤트 확인

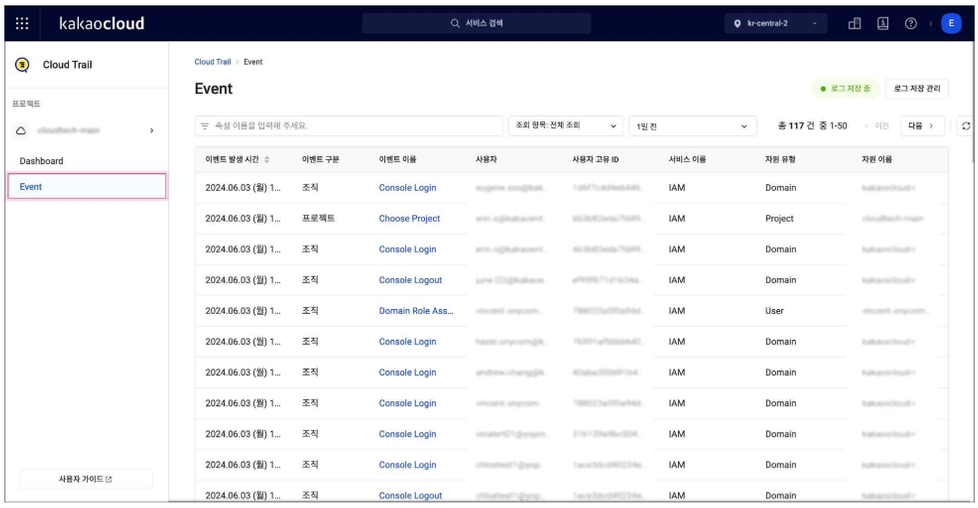


| 그림 5-1-2 | Cloud Trail의 프로젝트 이벤트 확인

- **(Console)** 프로젝트 선택 후 'Dashboard' → 'Management' → 'Cloud Trail' → 'Event' 에서 가상자원 이용에 관한 행위를 이벤트로 확인합니다.



| 그림 5-1-3 | 카카오클라우드 콘솔에서 Cloud Trail 서비스로 이동



| 그림 5-1-4 | Cloud Trail에서 Event 확인

- 가상자원에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근기록

  - VM, BM의 경우 OS에 기록되는 log 를 활용하도록 가이드 필요

    - 카카오클라우드의 Virtual Machine, Bare Metal Server 서비스로 생성된 가상자원의 경우 각 OS 유형에 맞게 OS 내 저장된 system log 를 확인하여 접속 일시, 접속자 등 접근 기록을 확인할 수 있습니다.

    - 예시

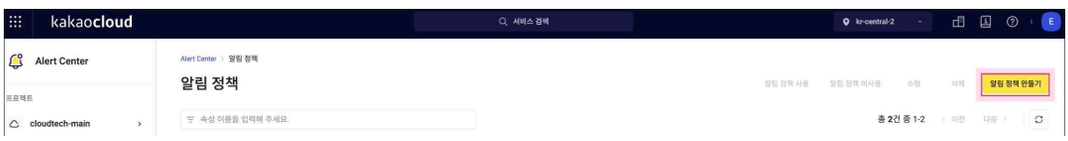
    1) Ubuntu 계열 Linux 의 경우 /var/log/auth.log 파일을 확인합니다.

    2) CentOS 계열 Linux 의 경우 /var/log/secure 파일을 확인합니다.

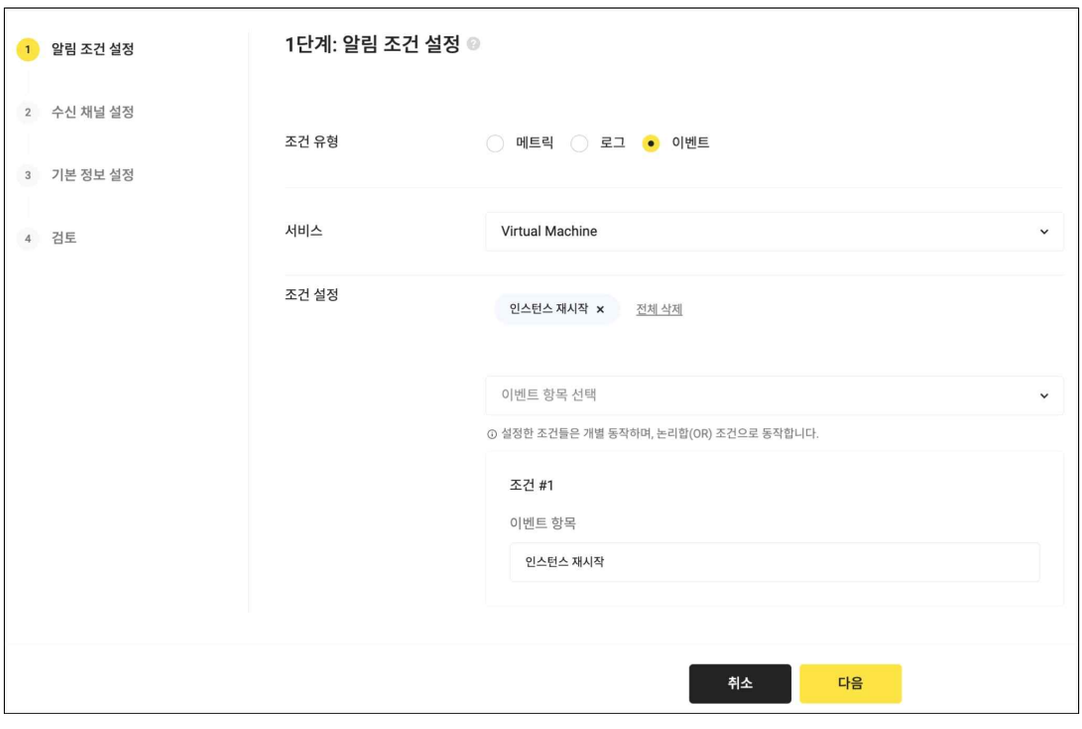
- 카카오클라우드는 Data Store(MySQL, Redis), File Storage 서비스와 같은 Managed Service 의 경우 사용자가 직접 OS에 접근할 수 없습니다. 따라서, 해당 서비스들로 생성된 자원의 경우 접속 일시, 접속자, 접근기록을 필요로 하지 않습니다.

- 가상자원을 사용한 일시, 사용자 및 가상자원의 형태(서버, 데이터베이스, 스토리지 등)를 확인할 수 있는 접근기록

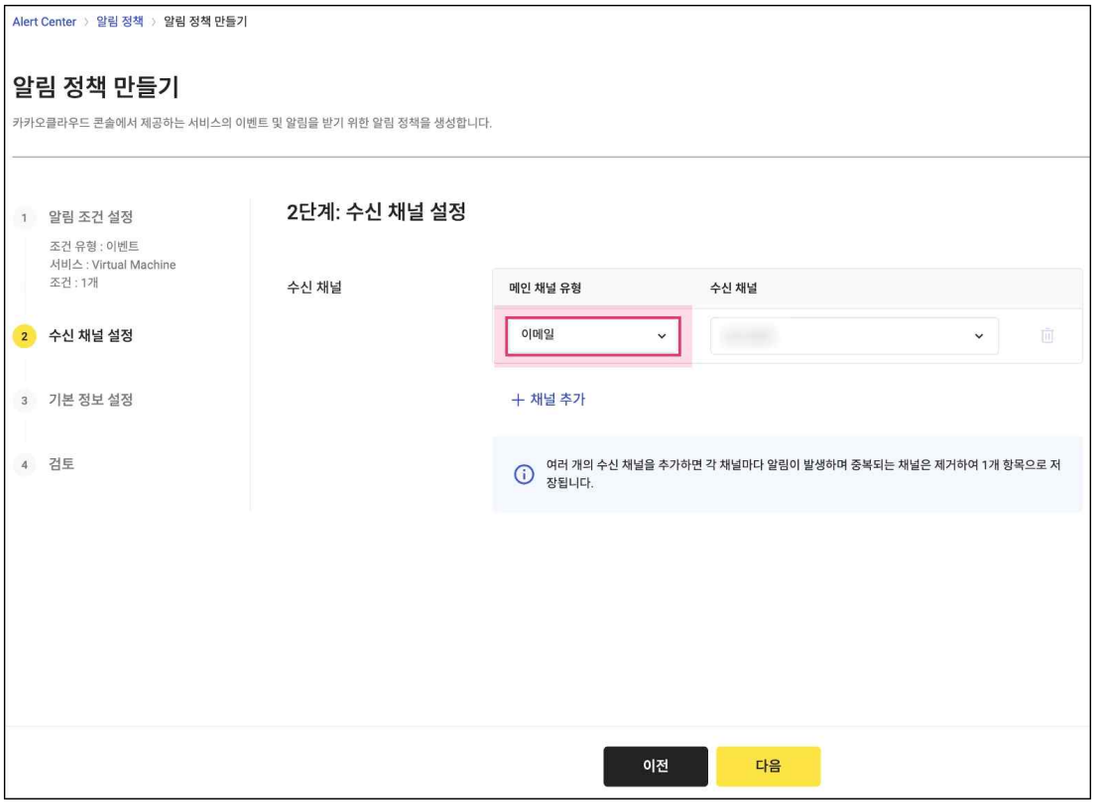
- 카카오클라우드의 Alert Center 기능을 통해 가상 자원의 특정 로그, 이벤트, 메트릭 알림을 다양한 채널로 보낼 수 있습니다.



| 그림 5-1-5 | Alert Center의 알림 정책 만들기



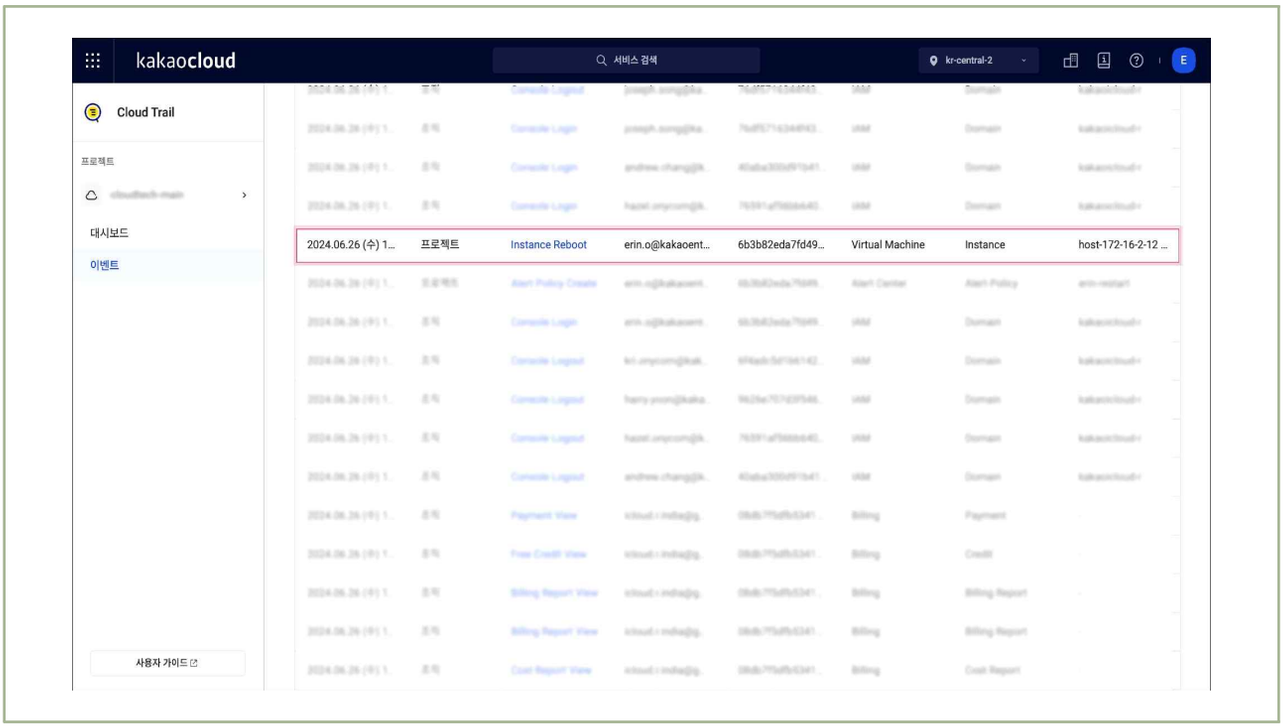
| 그림 5-1-6 | 인스턴스 재시작 이벤트 설정



| 그림 5-1-7 | 이벤트 수신 채널 설정

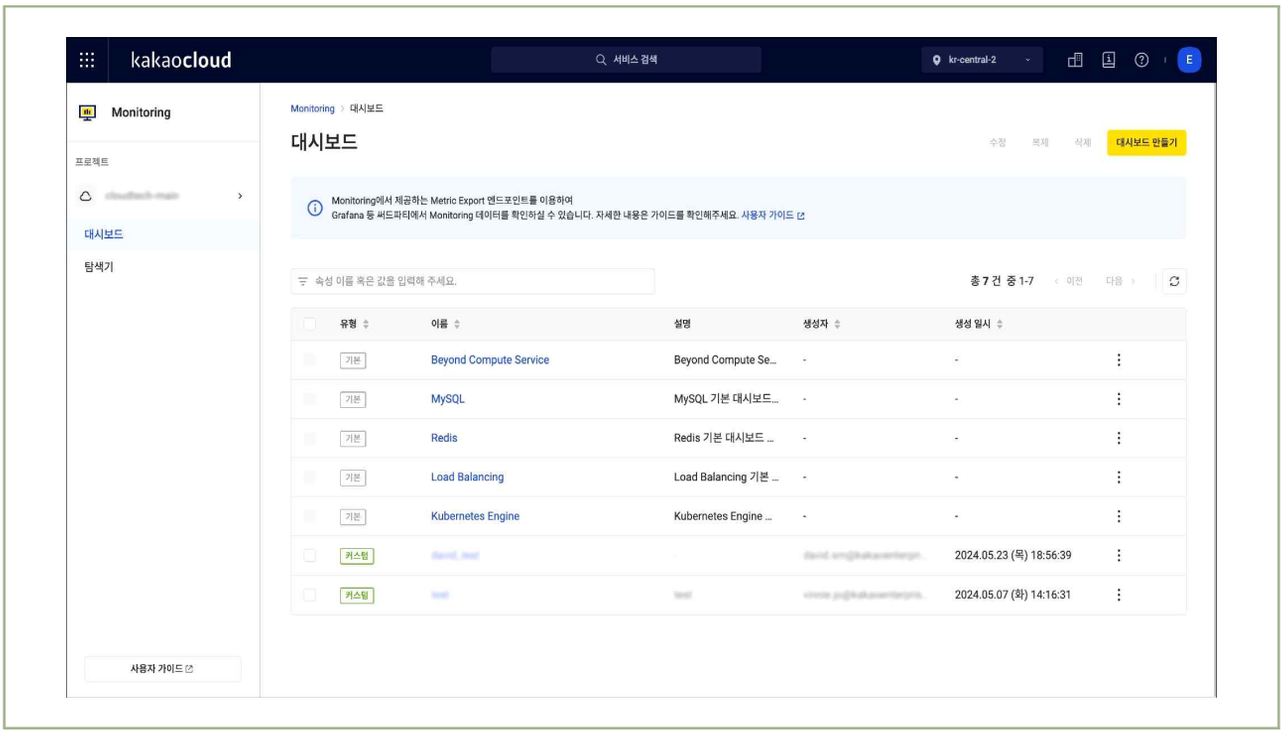
| 그림 5-1-8 | 인스턴스 재시작 이메일 알림

- 카카오클라우드의 Cloud Trail 이벤트 목록에서 가상 자원의 이벤트 로그를 확인할 수 있습니다.

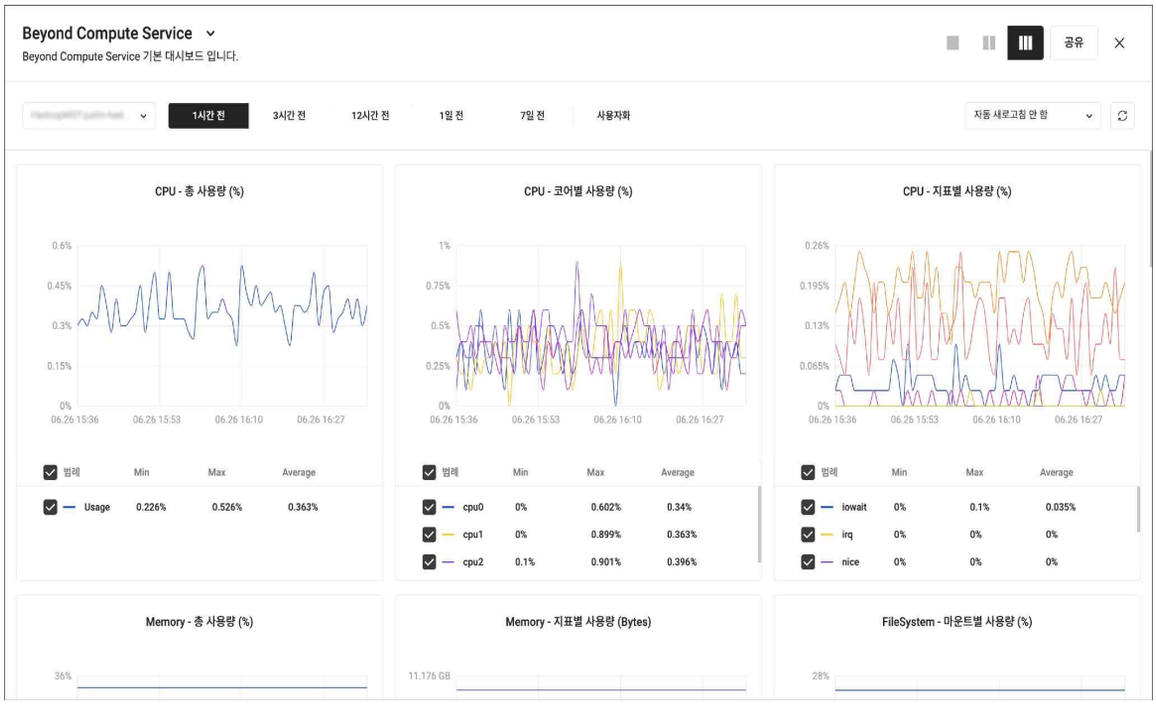


| 그림 5-1-9 | Cloud Trail에서 인스턴스 재시작 이벤트 로그 확인

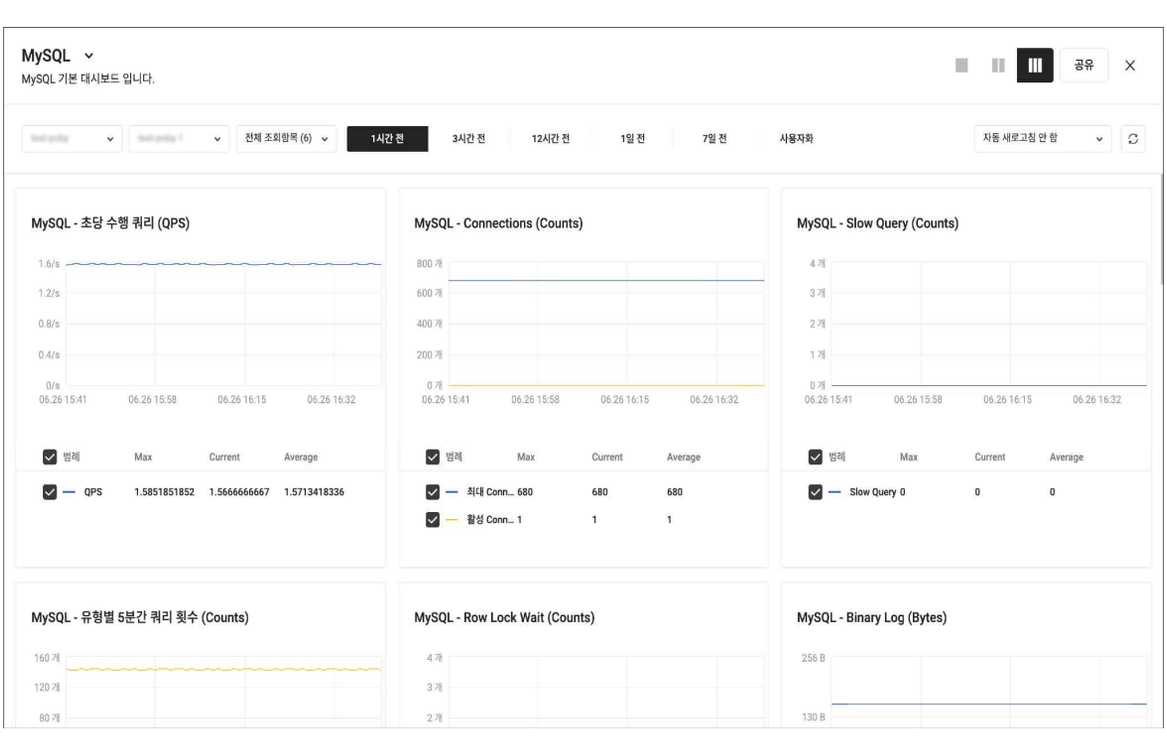
- 카카오클라우드 Monitoring 서비스를 통해 생성된 가상 자원의 주요 메트릭 정보를 확인할 수 있습니다.



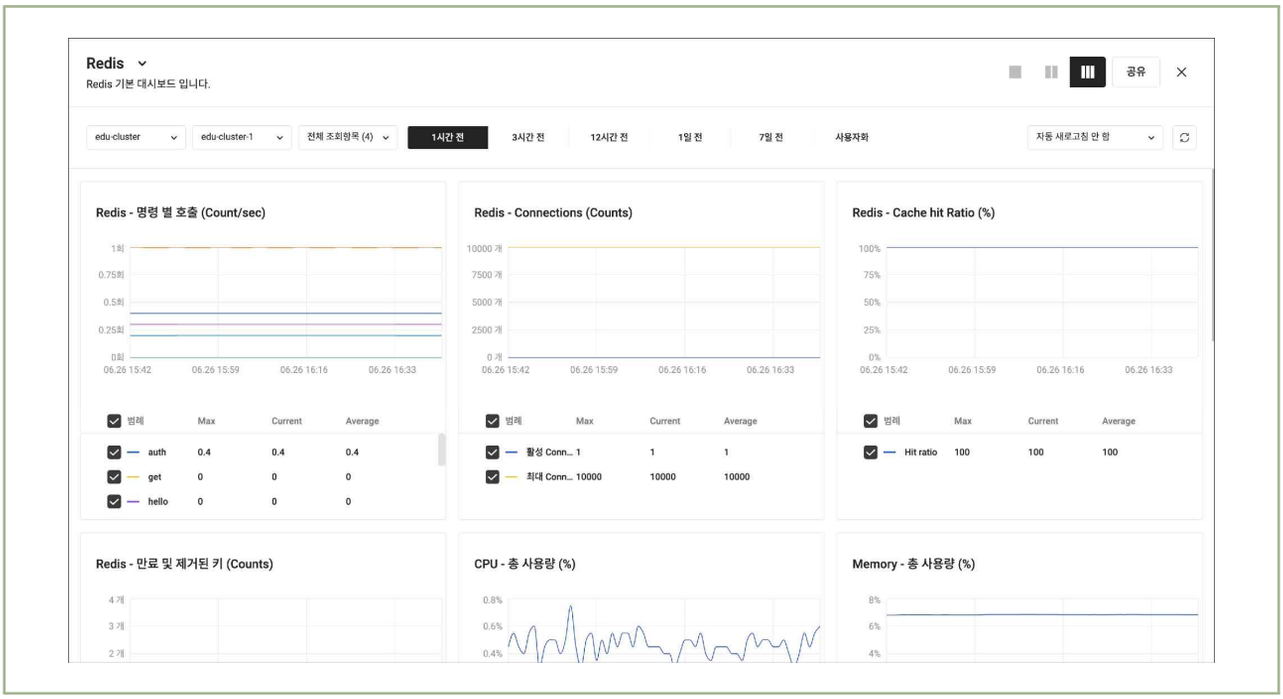
| 그림 5-1-10 | Monitoring 서비스 대시보드 목록



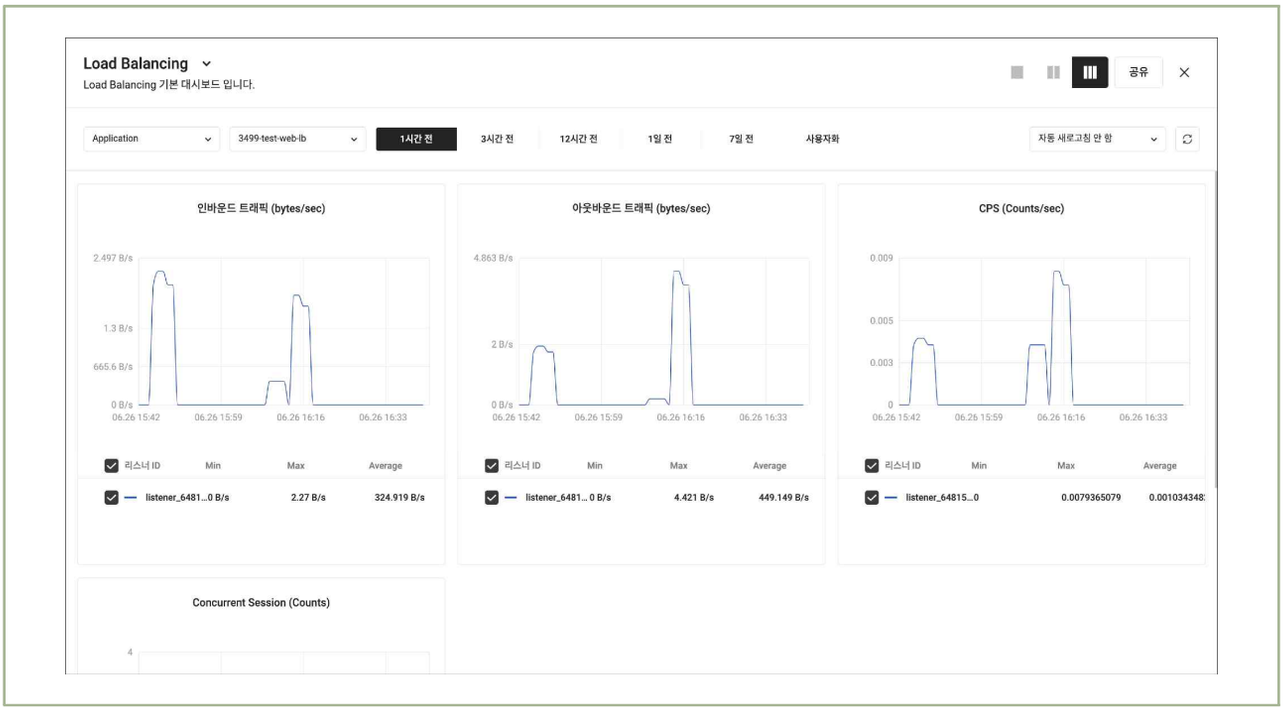
| 그림 5-1-11 | Beyond Compute Service 기본 대시보드



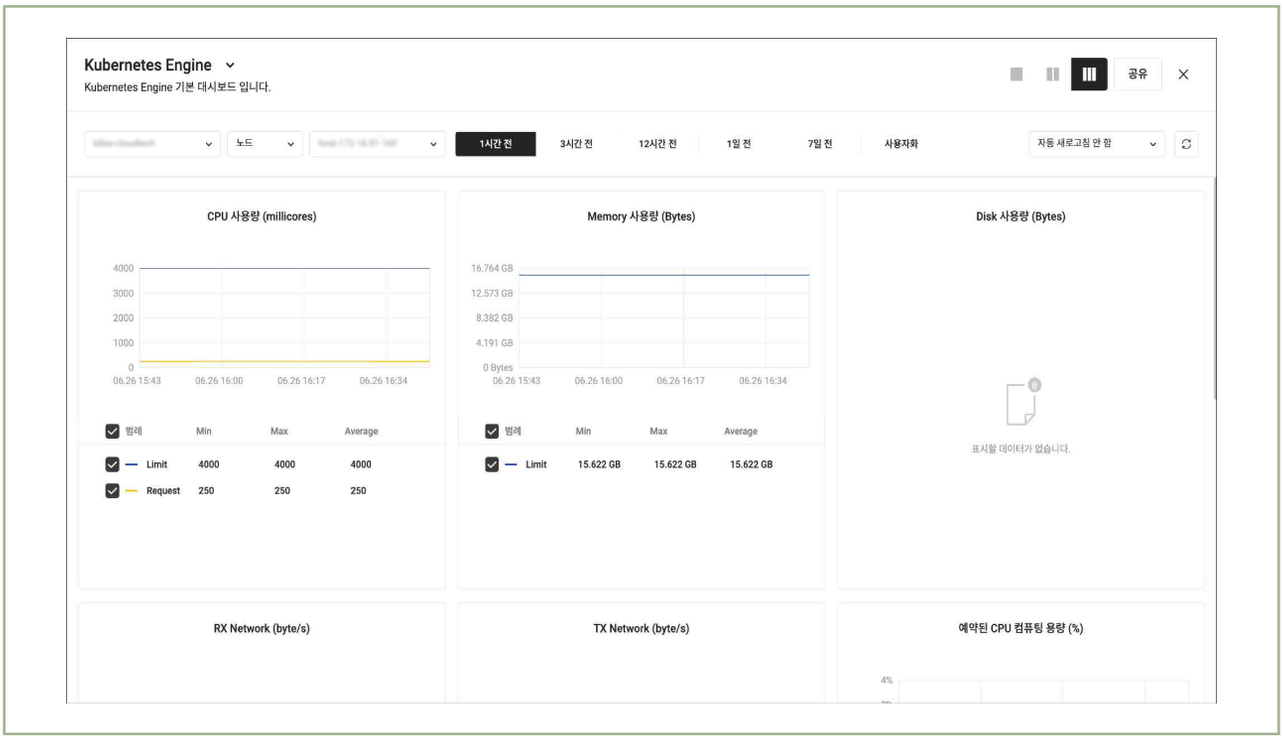
| 그림 5-1-12 | MySQL 기본 대시보드



| 그림 5-1-13 | Redis 기본 대시보드



| 그림 5-1-14 | Load Balancing 기본 대시보드



| 그림 5-1-15 | Kubernetes Engine 기본 대시보드

4 참고 사항

- 카카오클라우드 Cloud Trail 가이드
- 카카오클라우드 Monitoring 가이드
- 카카오클라우드 Alert Center 가이드

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.

  - 예시

    1) 클라우드 가상자원 이용에 관한 행위추적성 증적(ex. 감사로그 등)에 대한 상시 모니터링 수행

    2) 금융회사 내부규정등 관련 규정을 통해 수립된 검토 기간에 맞추어 클라우드 가상자원 이용에 관한 행위추적성 증적에 대한 주기적 검토 수행

3 우수 사례

- 카카오클라우드는 금융회사의 내부 컴플라이언스 기준 충족 가능하도록 클라우드에서 발생 되어진 모든 Audit 로그를 카카오클라우드 콘솔이 아닌 이용자 SIEM 연동 기능을 제공하여 행위추적성에 대한 적극적인 모니터링 가능하도록 지원하고 있습니다.
- KakaoCloud CloudTrail 로그를 Pub/Sub 서비스를 활용하여 이용자가 보유하고 있는 SIEM과 연동할 수 있는 가이드를 제공하며, 이용자가 능동적으로 행위추적성에 대해 모니터링 및 주기적으로 검토할 수 있는 기반 환경을 지원합니다.

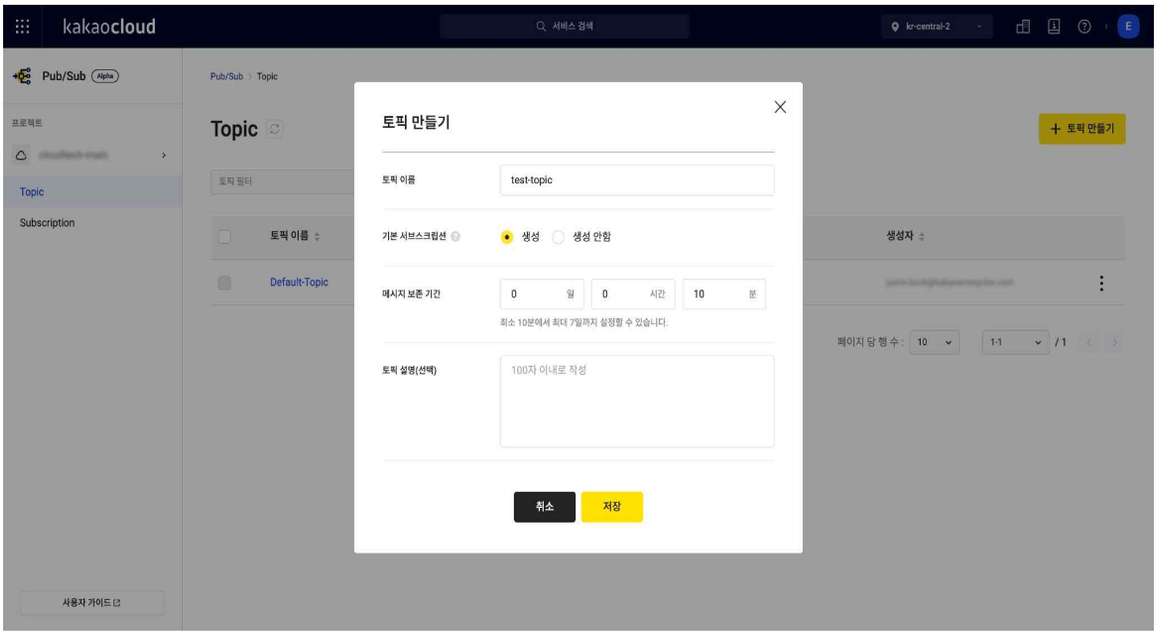
  + 대상 SIEM : Logpresso, Splunk

  1) 공통

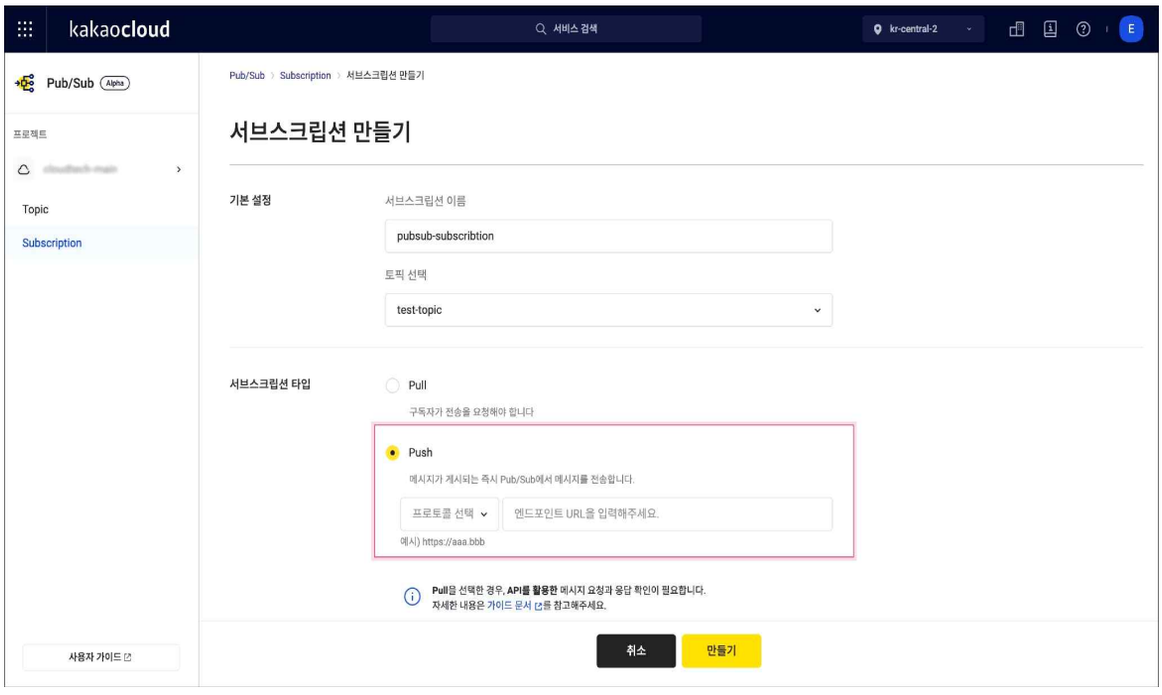
  •카카오클라우드 Audit 행위 로그 설정

  •Pub/Sub 토픽 생성 〉 Pub/Sub 서브스크립션 생성 〉 수신 채널 생성 〉 알림 정책 생성

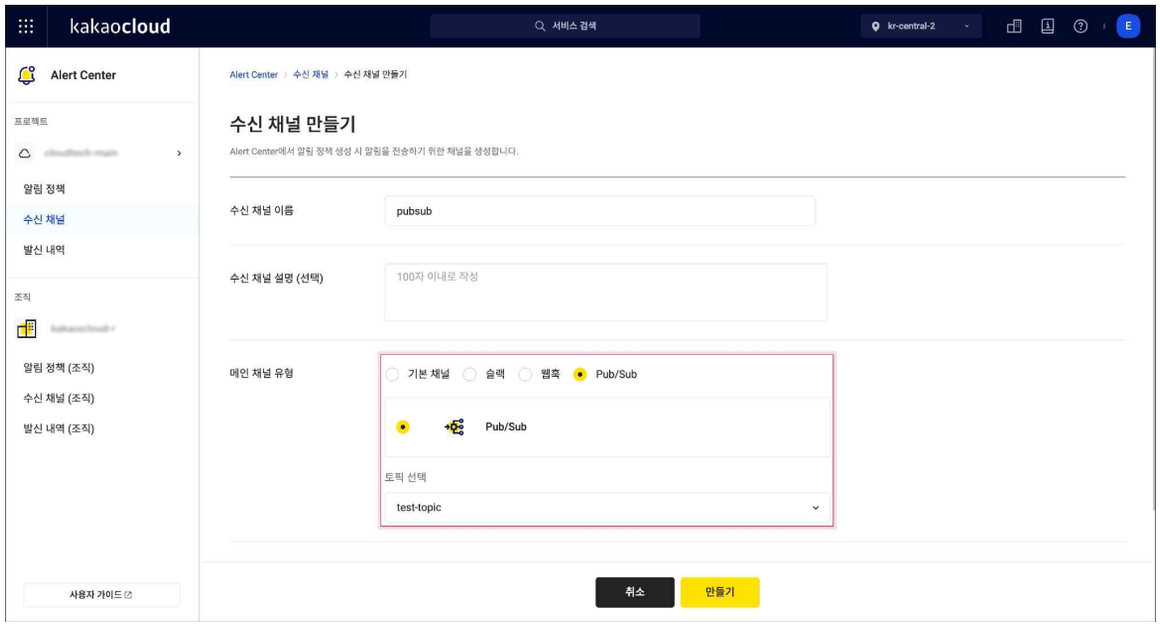
  * 수신 채널 설정은 채널의 유형 선택
  * Pub/Sub 서브스크립션 Push 선택



| 그림 5-2-1 | 토픽 만들기



| 그림 5-2-2 | 서브스크립션 타입을 Push로 하여 서브스크립션 만들기

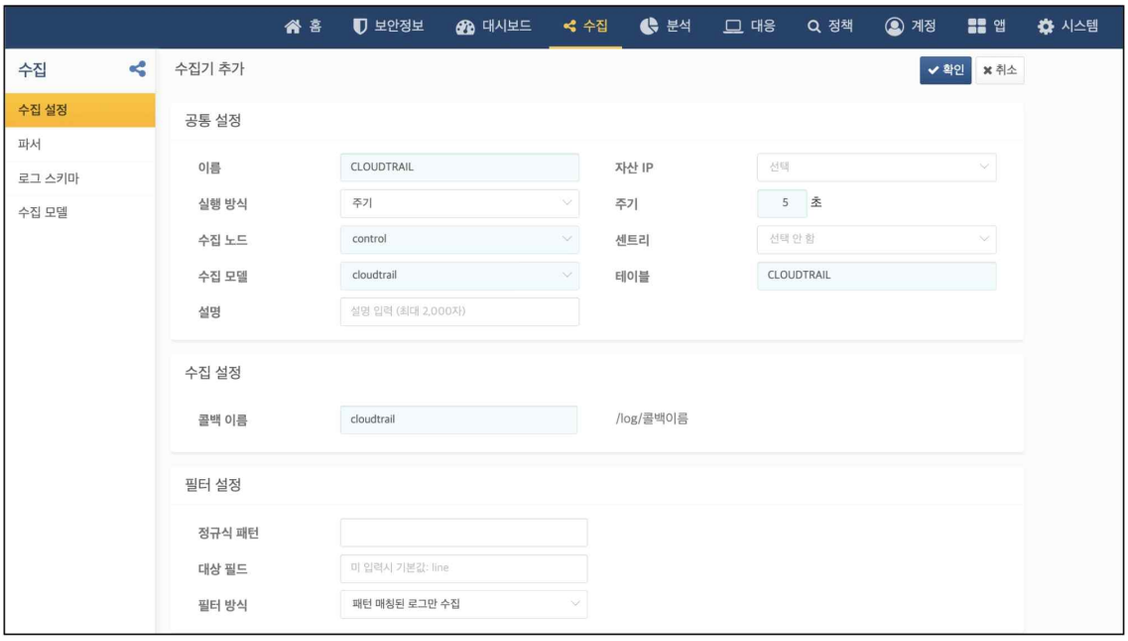


| 그림 5-2-3 | 수신 채널 만들기

| 그림 5-2-4 | 이전에 만들어둔 Pub/Sub 수신채널을 선택하여 알림 정책을 만들기

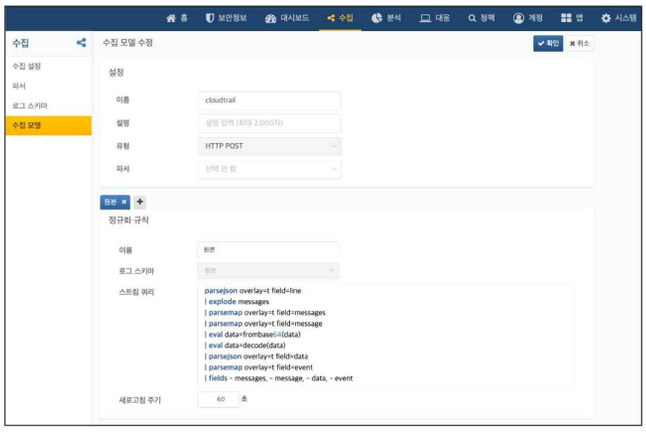
2-1) SIEM(Logpresso) 연동

- Logpresso 수집기 추가
  - 수집 〉 수집 설정에서 수집기 추가를 클릭
  - 수집기 및 테이블 이름을 설정
  - 콜백 이름을 설정 (Subscription Endpoint URL 주소)



| 그림 5-2-5 | Logpresso 수집기 설정 예시화면

- Logpresso 수집 모델 추가, 필드값 디코딩
  - 수집 〉 수집 모델에서 수집 모델 추가를 클릭
  - 수집 모델 이름 설정, 유형을 “HTTP POST”로 설정
  - 정규화 규칙 〉 스트립 쿼리에 아래와 같이 필드값 디코딩 함수를 활용하여 설정



```
parsejson overlay=t field=line
| explode messages
| parsemap overlay=t field=messages
| parsemap overlay=t field=message
| eval data=frombase64(data)
| eval data=decode(data)
| parsejson overlay=t field=data
| parsemap overlay=t field=event
| fields - messages, - message, - data, - event
```

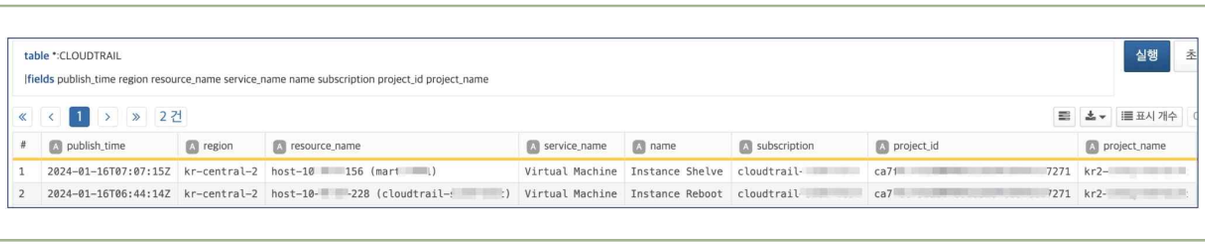
| 그림 5-2-6 | Logpresso 필드 값 Decode 설정 예시화면

- Subscription 설정
  - Pub/Sub 〉 Subscription에서 서브스크립션 타입 “Push”, 엔드포인트 URL을 “Logpresso에서 설정한 콜백 이름”을 주소로 저장

- SIEM에서 인바운드 보안 그룹 또는 ACL 정책 설정 필요 (가이드)

| 그림 5-2-7 | Pub/Sub Subscription 설정 예시화면

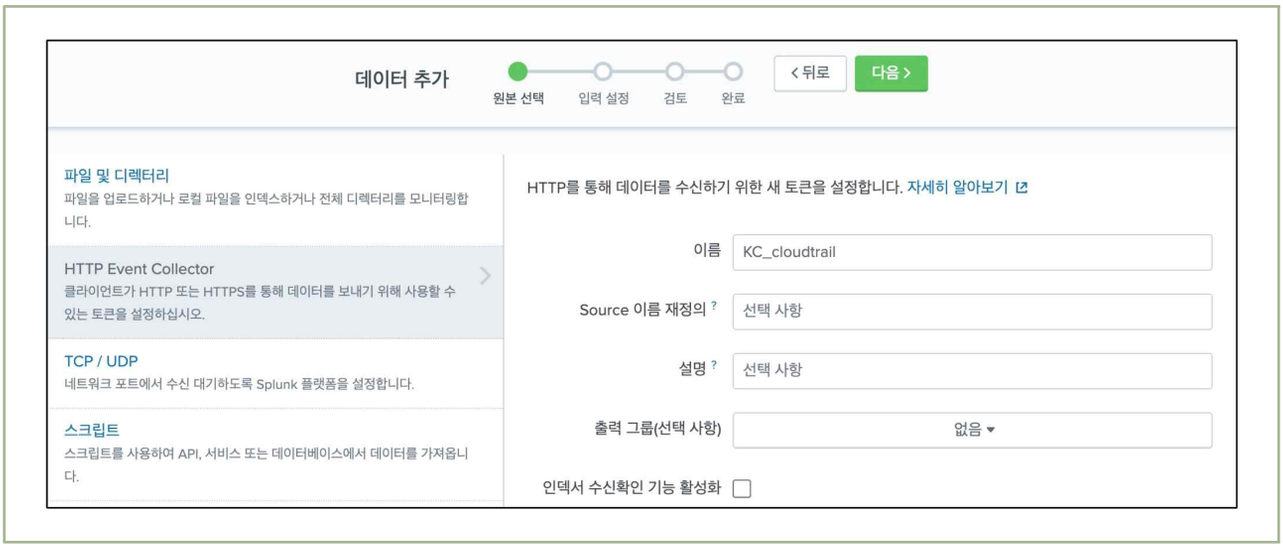
- SIEM(Logpresso) 로그 수신 조회
  - SIEM(Logpresso) 수집기/테이블 조회
  - Cloudtrail Pub/Sub의 주요 데이터 로그는 Base64인코딩 되어 전송되며, 실제 데이터 수신 시 수집 모델을 통해 디코딩



| 그림 5-2-8 | SIEM(Logpresso) 로그 수집 예시화면

2-2) SIEM(Splunk) 연동

- Splunk HTTP Event Collector 설정
  - Splunk Heavy Forwarder Settings(설정) 〉 Data Inputs(데이터 입력) 〉 HTTP Event Collector
  - HTTP Event Collector 화면에서 토큰을 먼저 생성
  - 토큰 새로 만들기 클릭, 토큰 이름을 정의하고 다음을 클릭 (인덱서 수신확인 기능 활성화 체크해제)

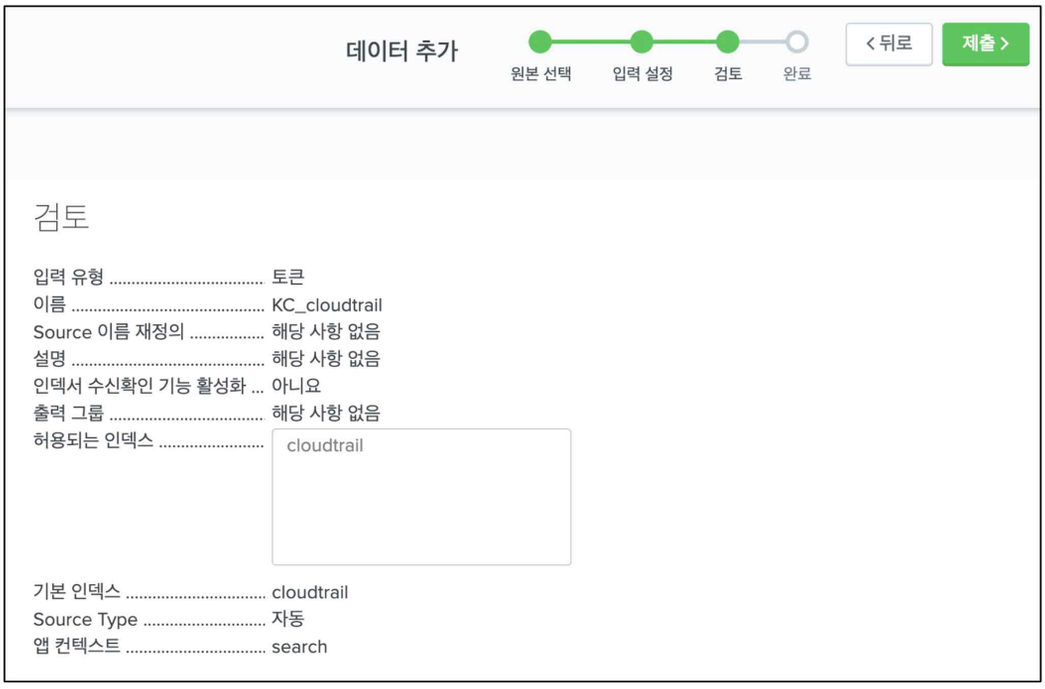


| 그림 5-2-9 | SIEM(Splunk) HTTP Event Collector 설정 예시화면

- Source type, 앱 컨텍스트, 인덱스를 지정. 이때 인덱스는 미리 생성 및 Indexer 서버에 배포되어야 합니다.

| 그림 5-2-10 | SIEM(Splunk) Index 설정 예시화면

- 다음 구성을 검토하고 제출을 클릭하여 저장



| 그림 5-2-11 | SIEM(Splunk) HTTP Event Collector 설정 예시화면

- 토큰이 생성되면 전역 설정 메뉴에서 HTTP Event Collector를 전역 활성화 진행
- HTTP Event Collector 화면에서 전역 설정을 클릭
- 모든 토큰을 활성화하고 HTTP 포트 번호가 8088[사용자 임의 값으로 변경가능]으로 설정되어 있는지 확인한 후 저장을 클릭

| 그림 5-2-121 | SIEM(Splunk) 전역 설정 예시화면

- Splunk NGINX Proxy 구성
  - 본 가이드에서는 HTTP Event Collector용 Proxy 를 구성하기 위해 Nginx 를 사용
  - Nginx 를 설치한 후 nginx.conf 파일을 다음과 같이 설정 (proxy listen 포트 설정)

```
user www-data;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;

events {
        worker_connections 1024;
        # multi_accept on;
}

http {

  log_format  '$remote_addr - $remote_user [$time_local] '
                  '"$request" $status $body_bytes_sent '
                  '"$http_referer" "$http_user_agent" "$gzip_ratio"';

    server {
        # Enable SSL for default HEC port 8088
        #listen 8088 ssl;
        listen 8888;  (기본 값 또는 사용자 임의로 변경한 값 입력)

        # Configure default Splunk Enterprise certificate.
        # Private key is included in server.pem so use it in both settings.
            #ssl_certificate     server.pem;
         #ssl_certificate_key server.pem;


    ...
```

| 그림 5-2-13 | SIEM(Splunk) NGINX 설정 예시화면

- 본 가이드에서는 HTTP Event Collector용 Proxy 를 구성하기 위해 Nginx 를 사용
- Nginx 를 설치한 후 nginx.conf 파일을 다음과 같이 설정 (proxy pass Splunk 주소 설정, header/body 설정, HEC 토큰값 설정 등)
- nginx.conf 파일 설정 후 서비스를 시작

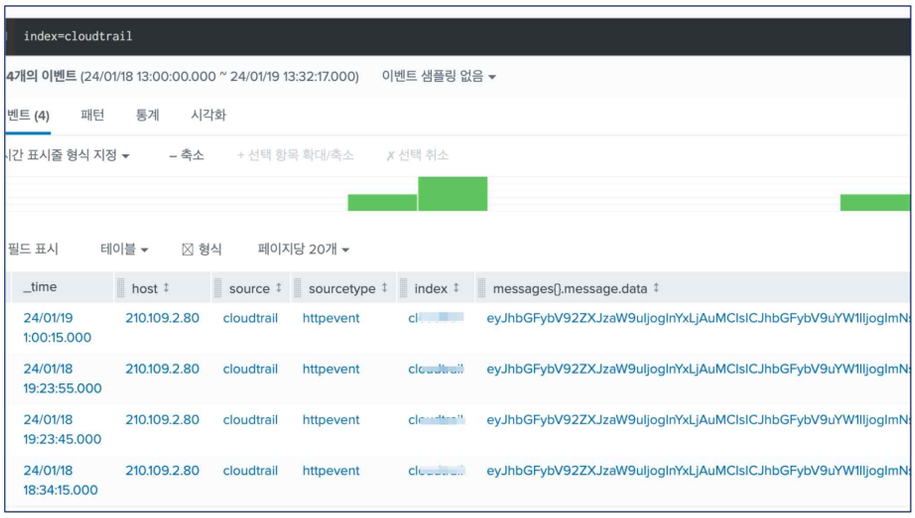
```
    ...

    location / {
        proxy_http_version 1.1;
        proxy_set_header Connection "";
        proxy_pass          https://127.0.0.1:8088/services/collector;  (Port 기본 값 또는 사용자 임의로 변경한 값 입력)
        proxy_read_timeout  90;
        proxy_connect_timeout 90;
        proxy_redirect      off;
        proxy_set_header    Host $host;
        proxy_set_header    X-Real-IP $remote_addr;
        proxy_set_header    X-Forwarded-For $proxy_add_x_forwarded_for;

        # wrap the event body for splunk
        proxy_set_body      "{\"event\":$request_body}";
        # Add the Splunk token into the Authorization header
        proxy_set_header    Authorization "Splunk 3e9d54a0-36cb-4e6c-86ce-d33b6ce7eca8";  (입력 형식 [Splunk 토큰값])
    }
  }
}
```

| 그림 5-2-14 | SIEM(Splunk) NGINX 설정 예시화면

- Subscription 설정
  - Pub/Sub 〉 Subscription 에서 서브스크립션 타입 Push, 엔드포인트 URL 을 설정한 Nginx Proxy 주소 및 포트로 설정하여 저장
  - SIEM 에서 인바운드 보안 그룹 또는 ACL 정책 설정이 필요 (가이드)

| 그림 5-2-15 | Pub/Sub Subscription 설정 예시화면

- SIEM(Splunk) 로그 수신 조회
  - 신규 생성 한 index 값으로 조회
  - Cloud trail Pub/Sub의 주요 데이터 로그는 base64 인코딩 되어 전송되며, 실제 데이터 수신 시에는 직접 디코딩 진행 필요

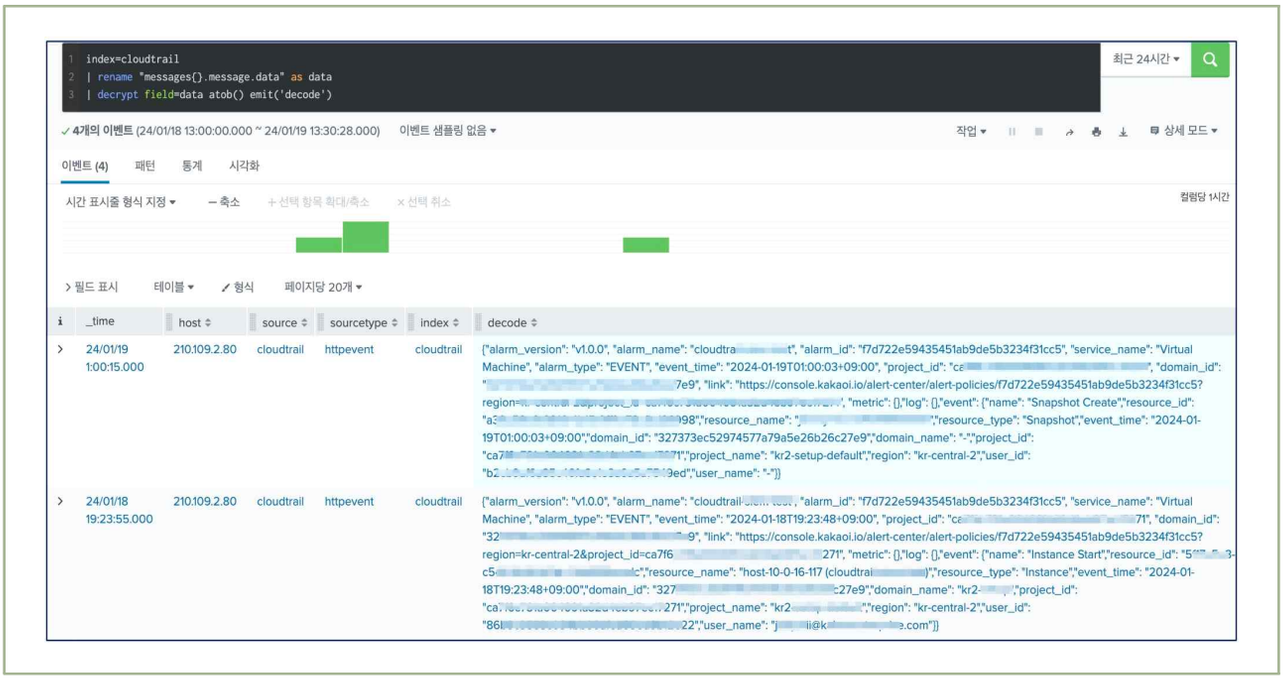


| 그림 5-2-16 | SIEM Splunk 로그 조회 예시화면

- SIEM(Splunk) 필드값 Decode
  - Search Head 서버에 DECRYPT2 앱을 다운로드 후 설치 (App 링크)
  - App 〉 App Upload 〉 파일 선택하여 설치

| 그림 5-2-17 | SIEM Splunk 앱 설치 예시화면

  - 아래와 같이 decrypt 함수를 사용하여 쿼리
  - decrypt field=〈필드명〉 atob() emit('〈변환 필드명〉')



| 그림 5-2-18 | SIEM Splunk 디코드 로그 예시화면

- 카카오클라우드 로그 발송 내역 확인
  - Alert Center 〉 발신 내역 에서 카카오클라우드의 모든 행위에 대해 발신 내역 목록(전송 성공/실패)을 확인할 수 있습니다.

| 그림 5-2-19 | 카카오클라우드 로그 발송 내역 예시화면

4 참고 사항

- 카카오클라우드 〉 AlertCenter 가이드 참고
- 카카오클라우드 〉 Pub/Sub 가이드 참고
- 카카오클라우드에서 연동 제공하는 SIEM은 Logpresso, Splunk 대상이며, 이 외의 SIEM은 추가적인 검토가 필요합니다.

1 기준

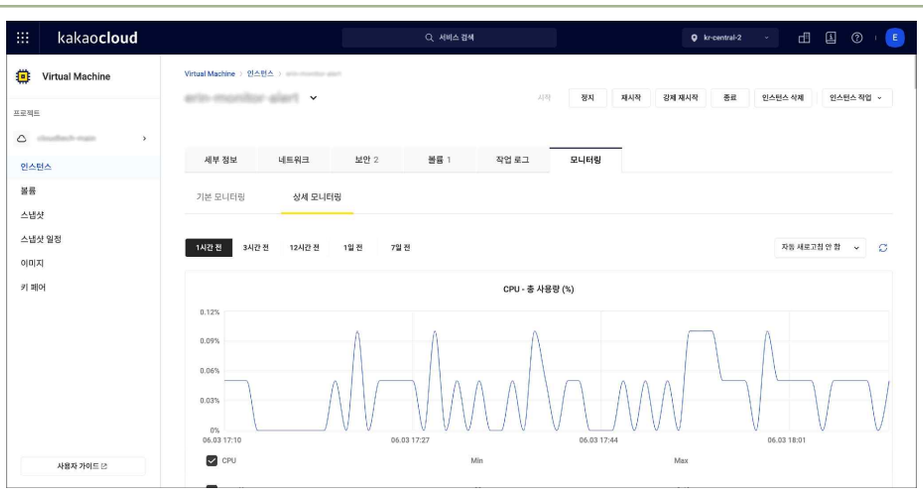
식별번호	기준	내용
5.3.	**이용자 가상자원 모니터링 기능 확보**	**이용자 가상자원 운용에 관한 모니터링 기능을 확보하여야 한다.**

2 설명

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

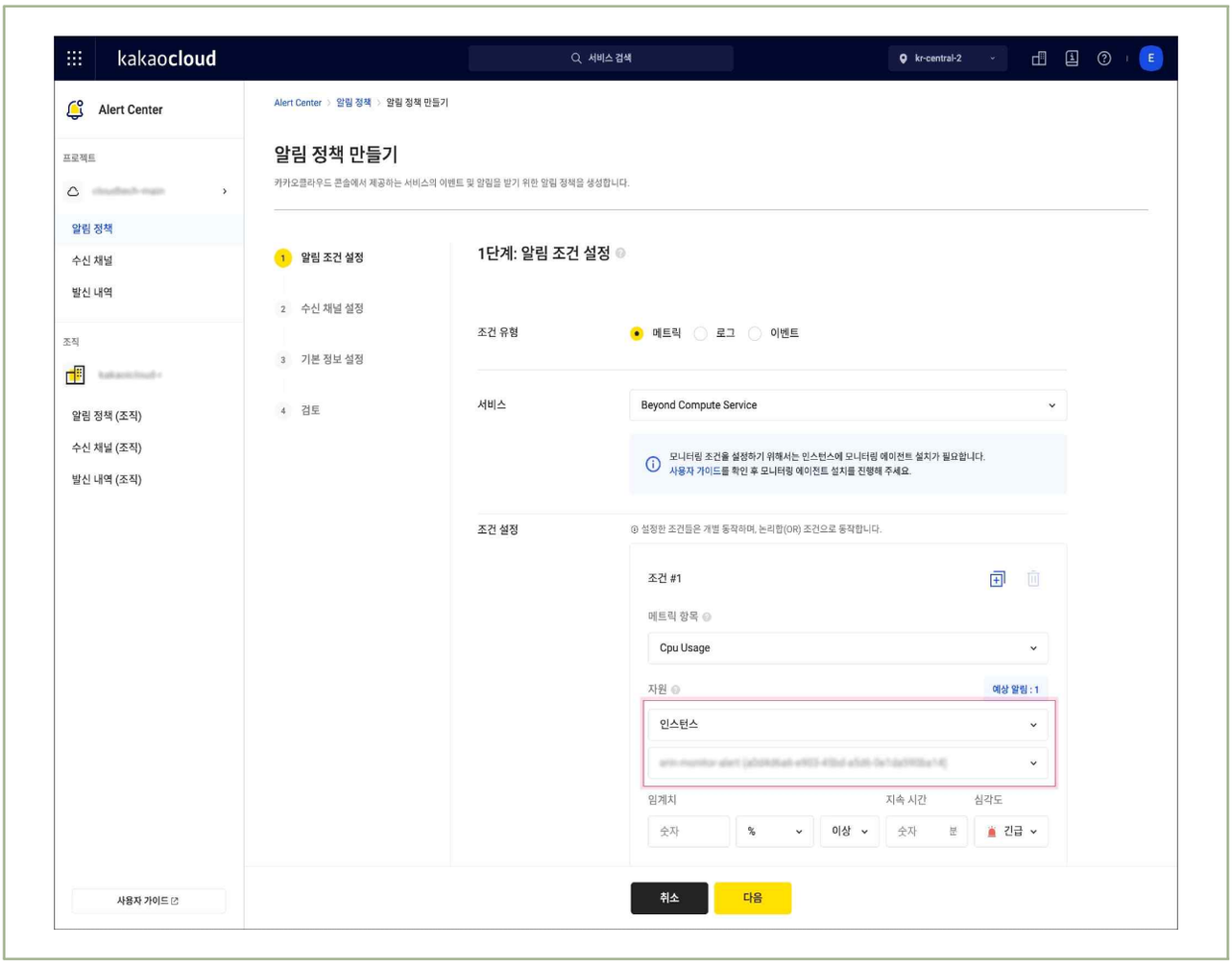
3 우수 사례

- 가상자원 상태 모니터링(사용량, 트래픽 용량 등)
  - Virtual Machine 이나 Bare Metal Server 같은 가상 자원의 경우 모니터링 에이전트 설치 후 모니터링 서비스를 통해 상세 모니터링이 가능합니다.



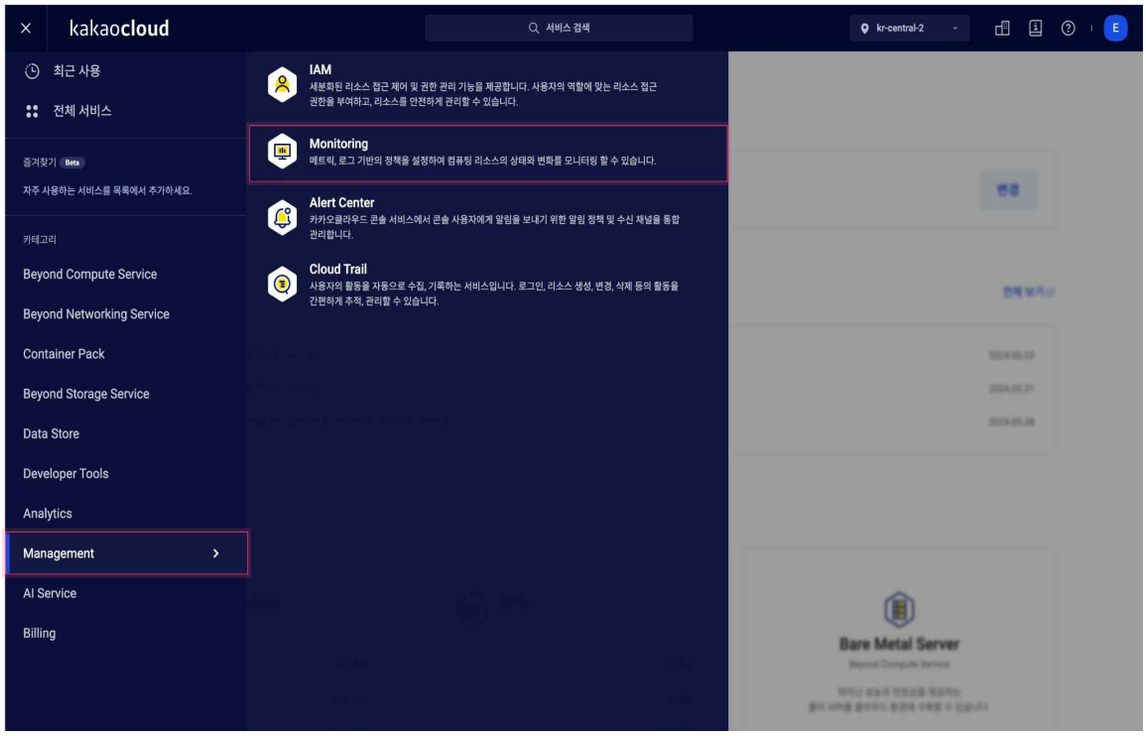
| 그림 5-3-1 | Virtual Machine의 모니터링 상세페이지

- 모니터링 에이전트가 설치된 상태에서 Alert Center 서비스의 수신 채널 설정 및 알림 정책 설정 후 메트릭, 로그, 이벤트를 트리거로 알림을 수신할 수 있도록 설정 가능합니다.

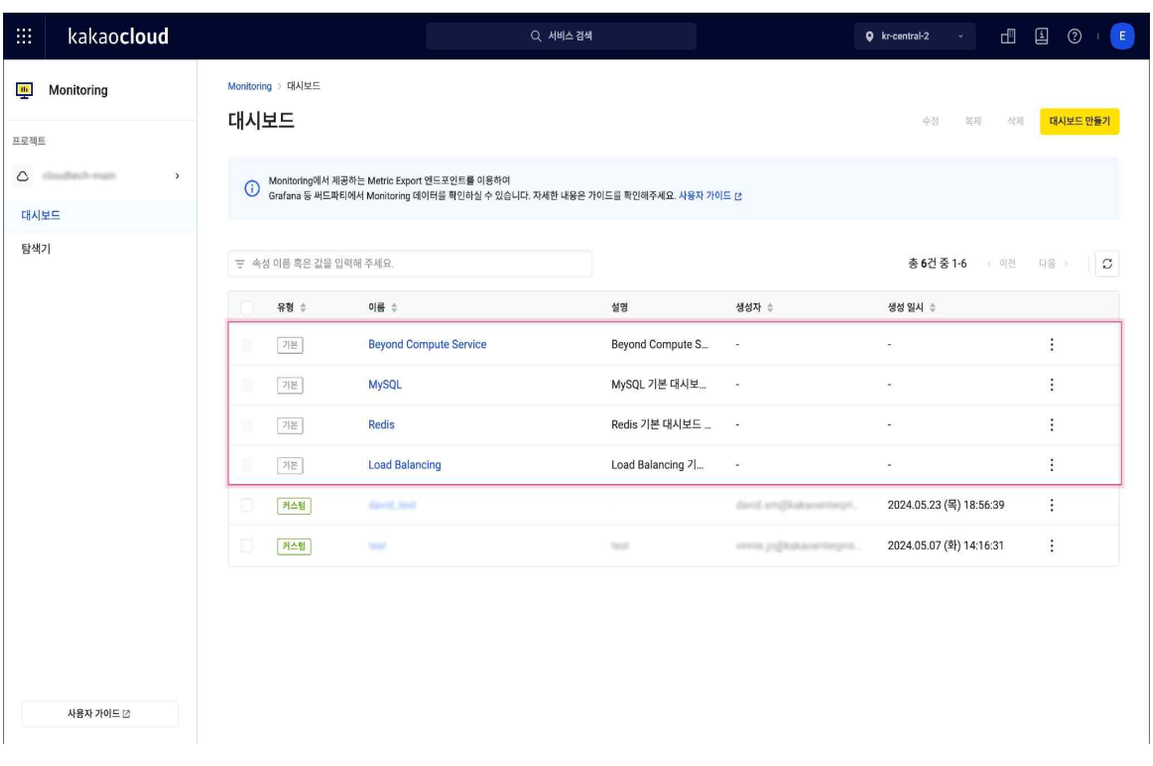


| 그림 5-3-2 | 모니터링 에이전트가 설치된 인스턴스에 수신 채널 설정하기

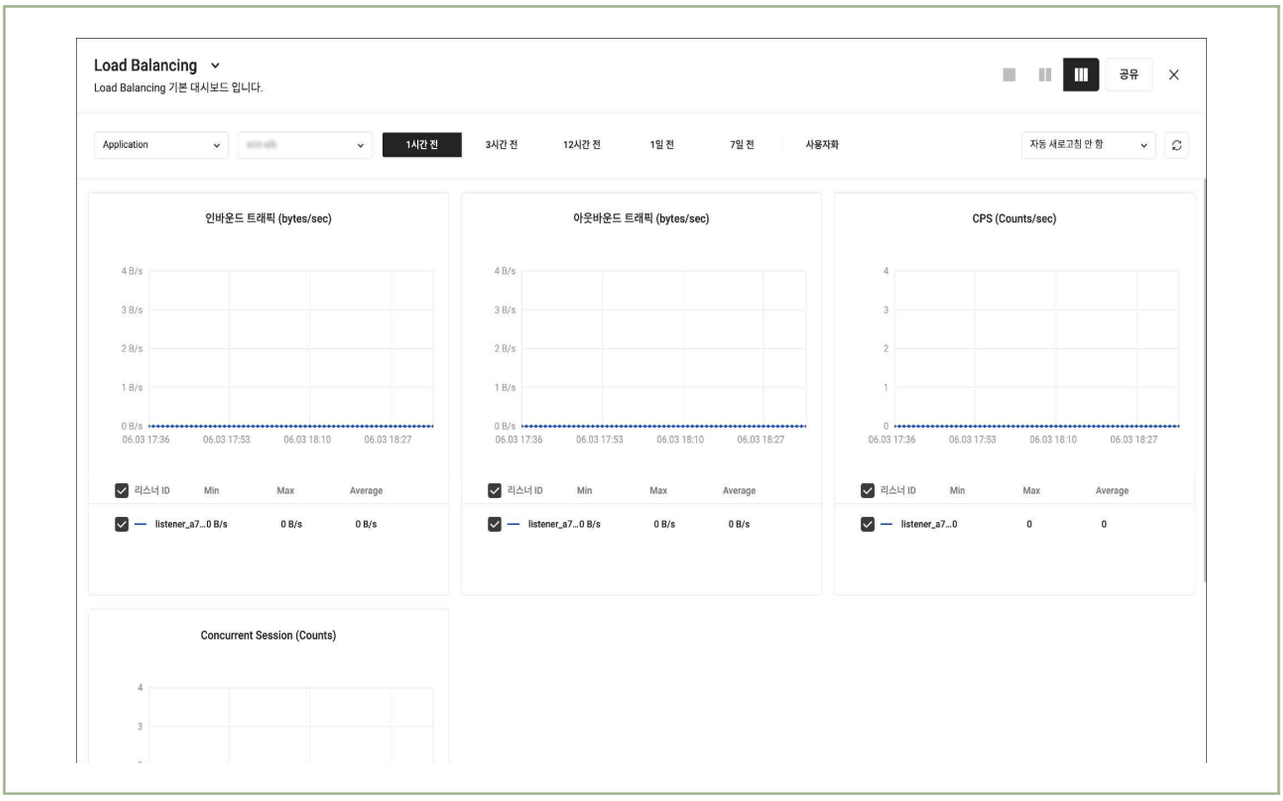
- 그 외 Managed 형태의 서비스 중 일부(Load Balancing, MySQL, Redis)는 기본 대시보드를 통해 모니터링 정보를 제공합니다.
  - **(Console)** ‘Dashboard’ → ‘Management’ → ‘Monitoring’ → ‘대시보드' 목록에서 기본으로 제공되는 Load Balancing, MySQL, Redis 대시보드 확인이 가능합니다.



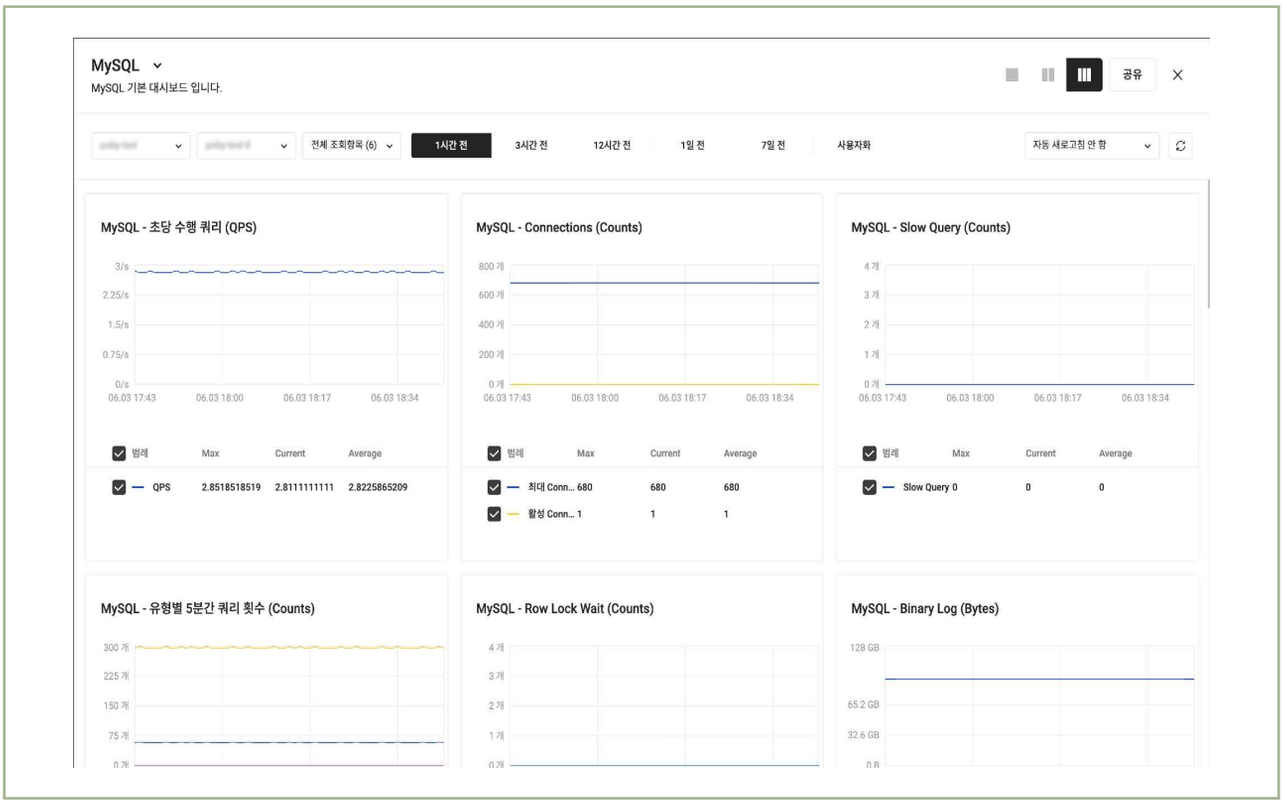
| 그림 5-3-3 | 카카오클라우드 콘솔에서 Monitoring 서비스 이동



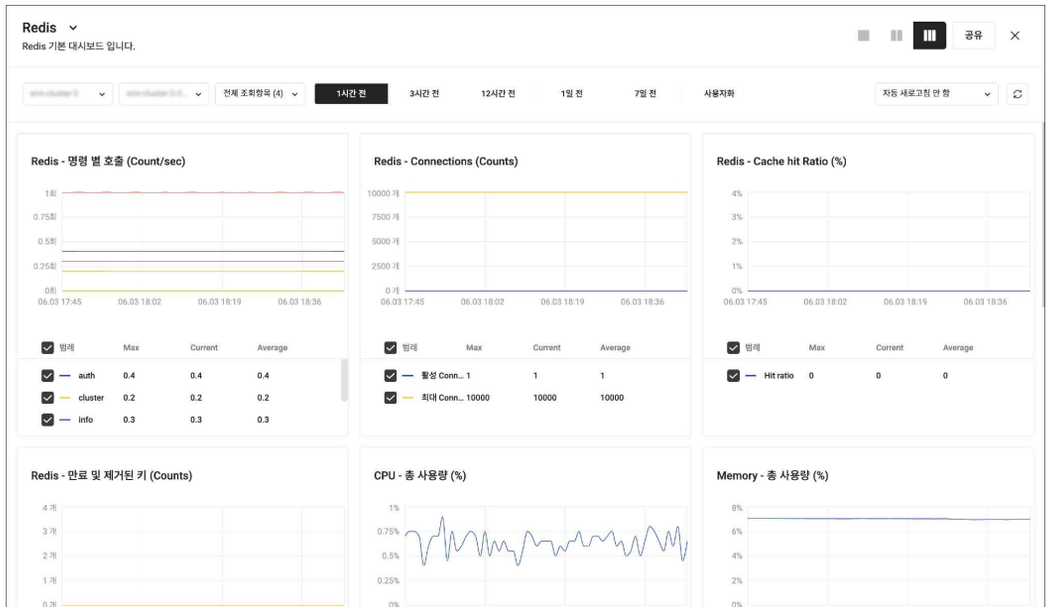
| 그림 5-3-4 | 기본 대시보드 확인



| 그림 5-3-5 | Load Balancing 기본 대시보드



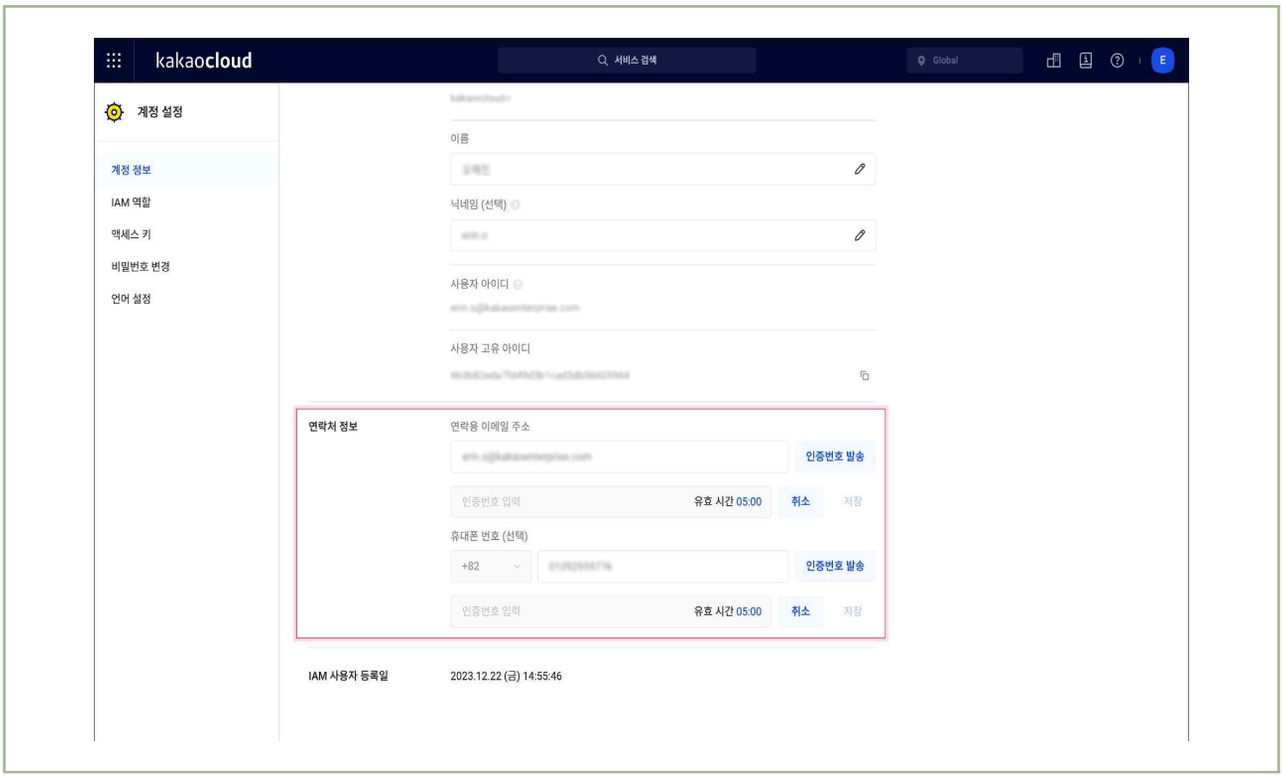
| 그림 5-3-6 | MySQL 기본 대시보드



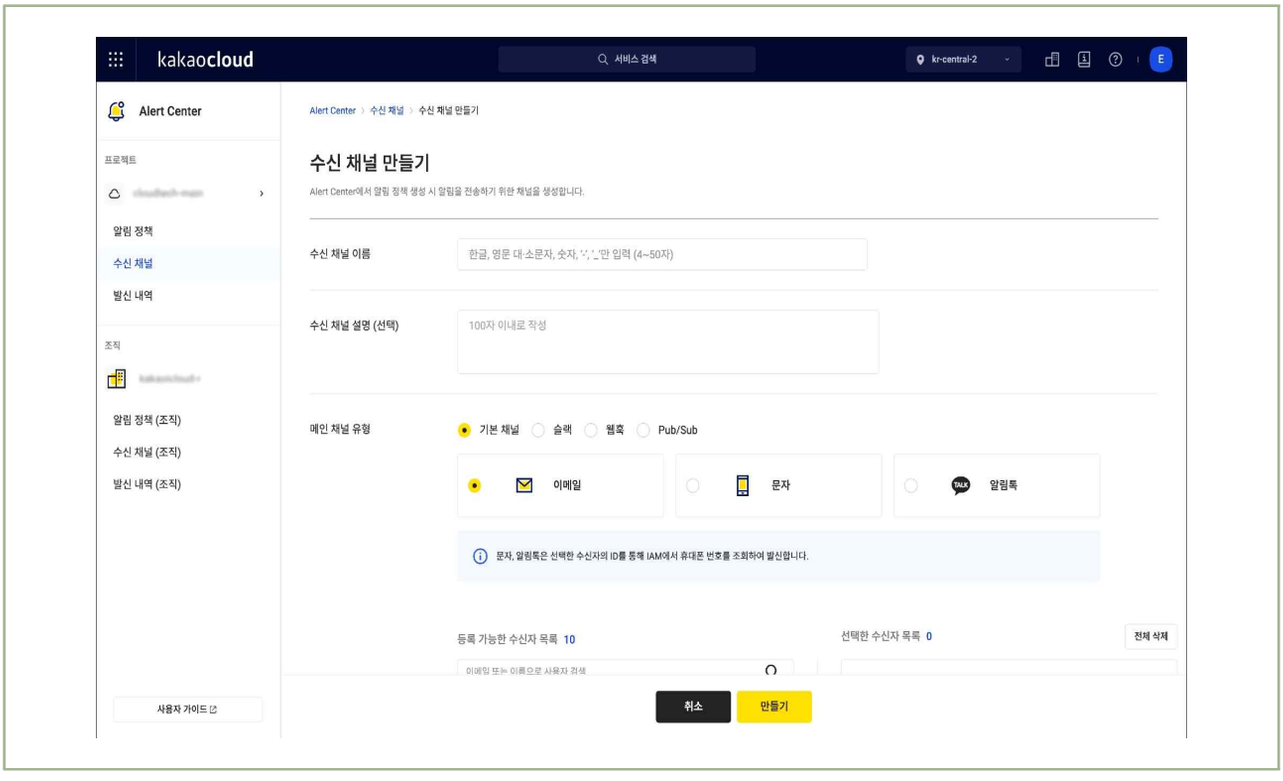
| 그림 5-3-7 | Redis 기본 대시보드

- 가상자원 장애 모니터링(장애 발생 시 담당자 공지 등)
  - 모니터링 에이전트 설치 〉 휴대폰 번호 및 이메일 인증 〉 수신 채널 설정 〉 알림 정책 설정 과정을 거쳐 서버 상태에 따라 메트릭, 로그, 이벤트를 트리거로 알림을 수신하도록 설정하여 장애 인지가 가능합니다.

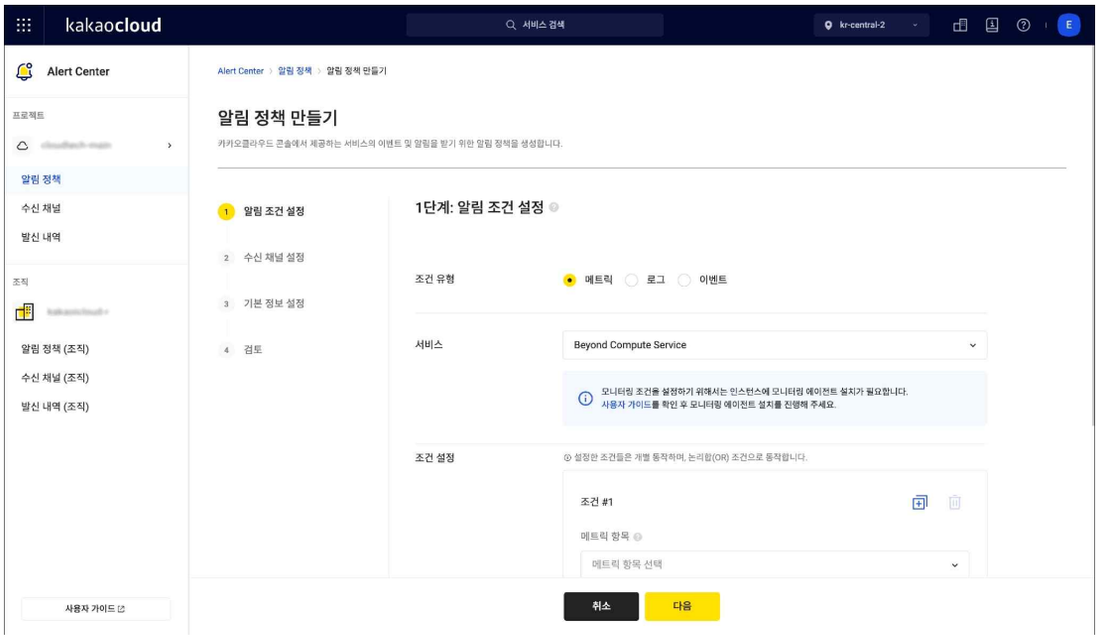
| 그림 5-3-8 | 모니터링 에이전트 설치



| 그림 5-3-9 | 사용자 계정정보에서 연락처 정보 인증 및 설정

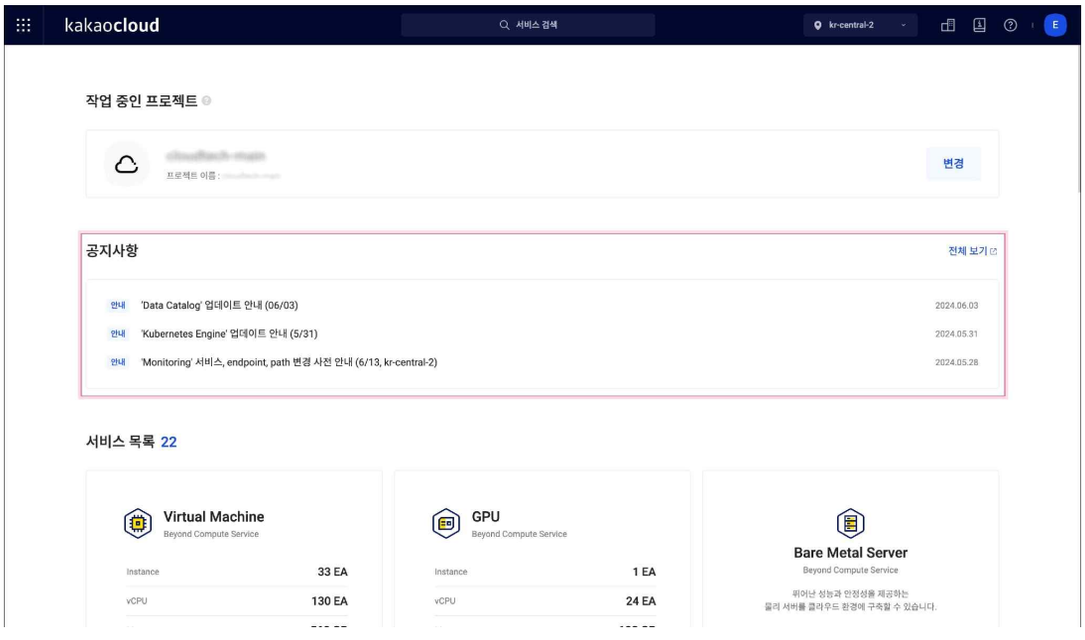


| 그림 5-3-10 | 수신 채널 생성



| 그림 5-3-11 | 메트릭, 로그, 이벤트를 트리거로 한 알림 정책 생성

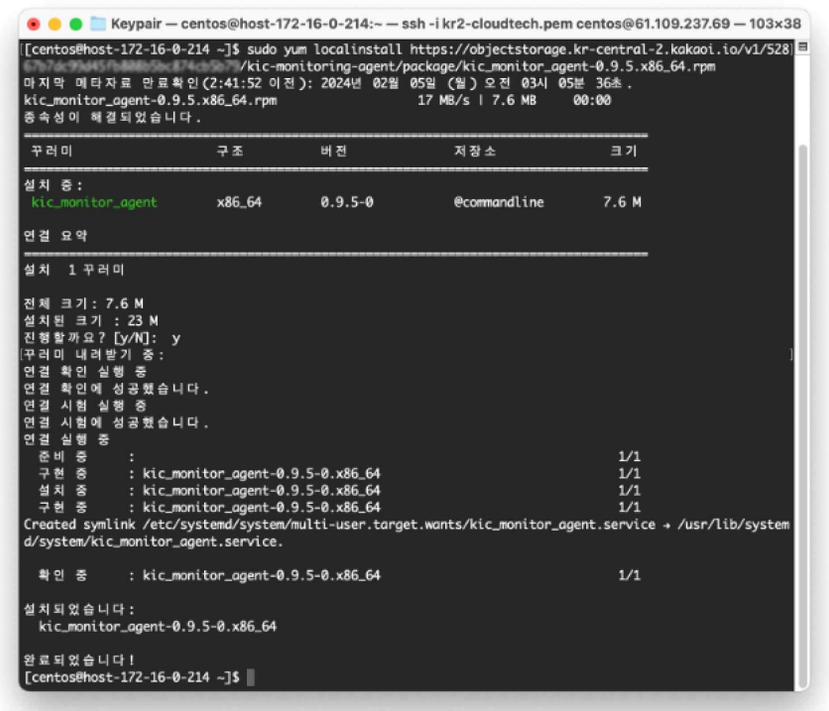
- 또한, 카카오클라우드에서는 서비스 장애 발생 시 공지사항 페이지에 공지를 등록하여 사용자에게 안내합니다.



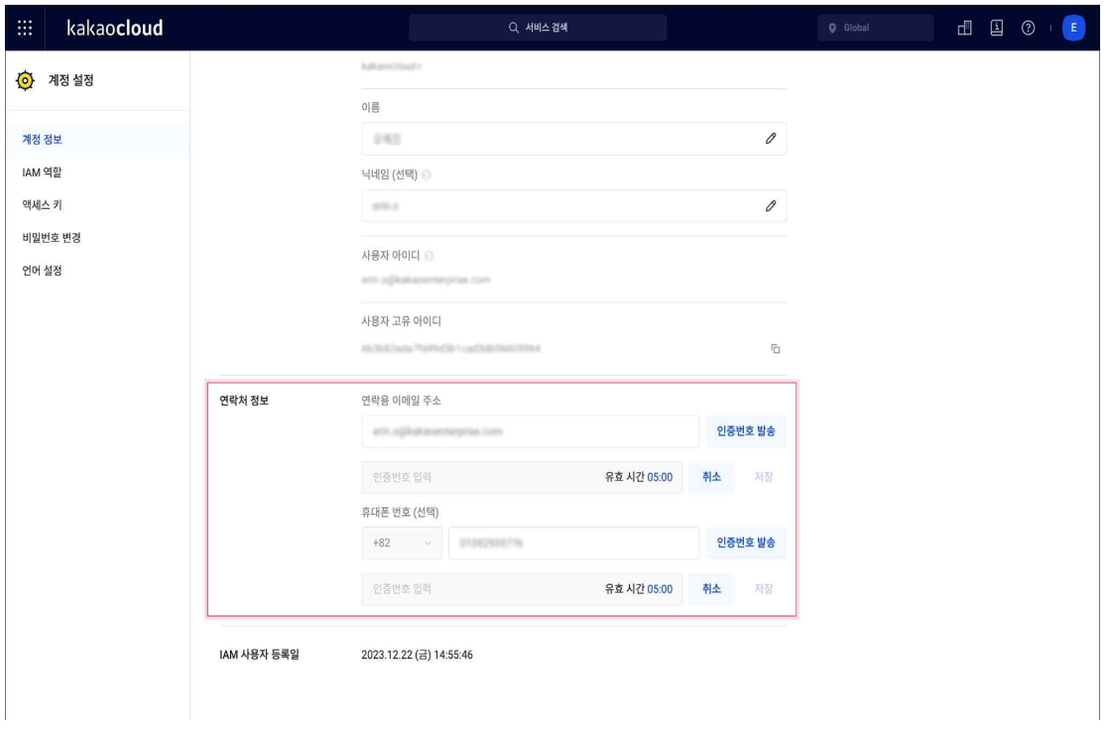
| 그림 5-3-12 | 카카오클라우드 콘솔에서 확인할 수 있는 공지사항

| 그림 5-3-13 | 카카오클라우드 포털에서 확인할 수 있는 공지사항

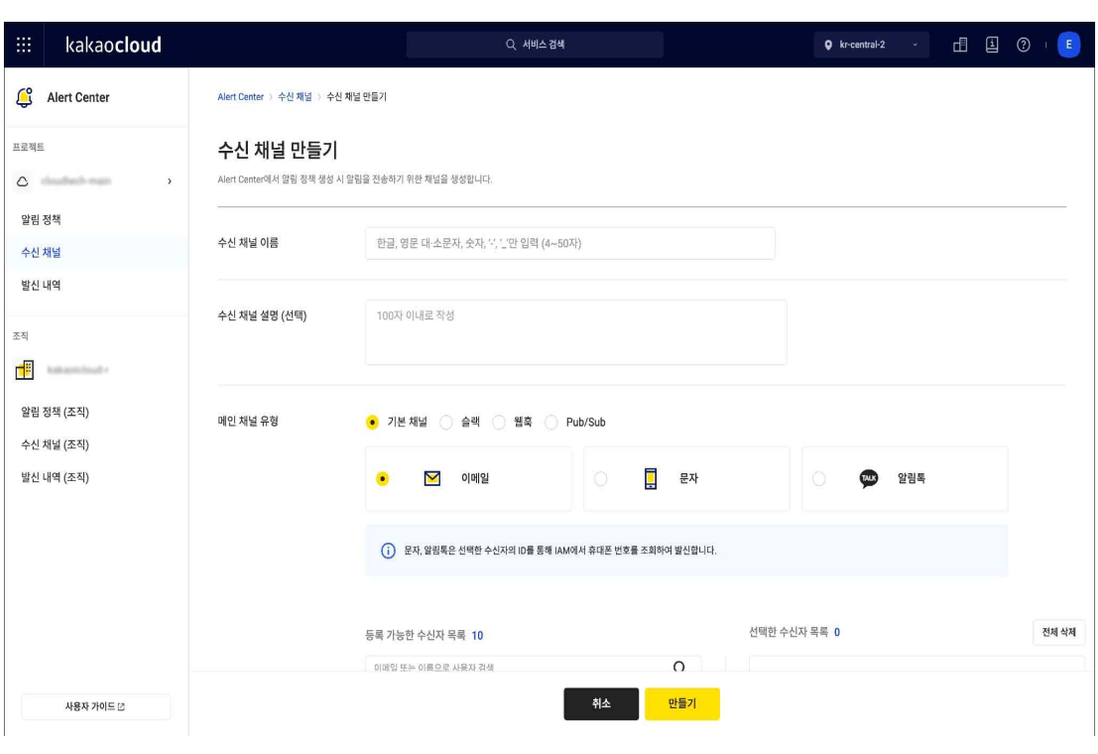
- 가상자원 장애 발생 시 장애상황기록부 작성 등
  - 모니터링 에이전트 설치 〉 휴대폰 번호 및 이메일 인증 〉 수신 채널 설정 〉 알림 정책 설정의 과정을 거쳐 서버 상태에 따라 메트릭, 로그, 이벤트를 트리거로 알림을 수신하도록 설정하여 장애 인지가 가능합니다.



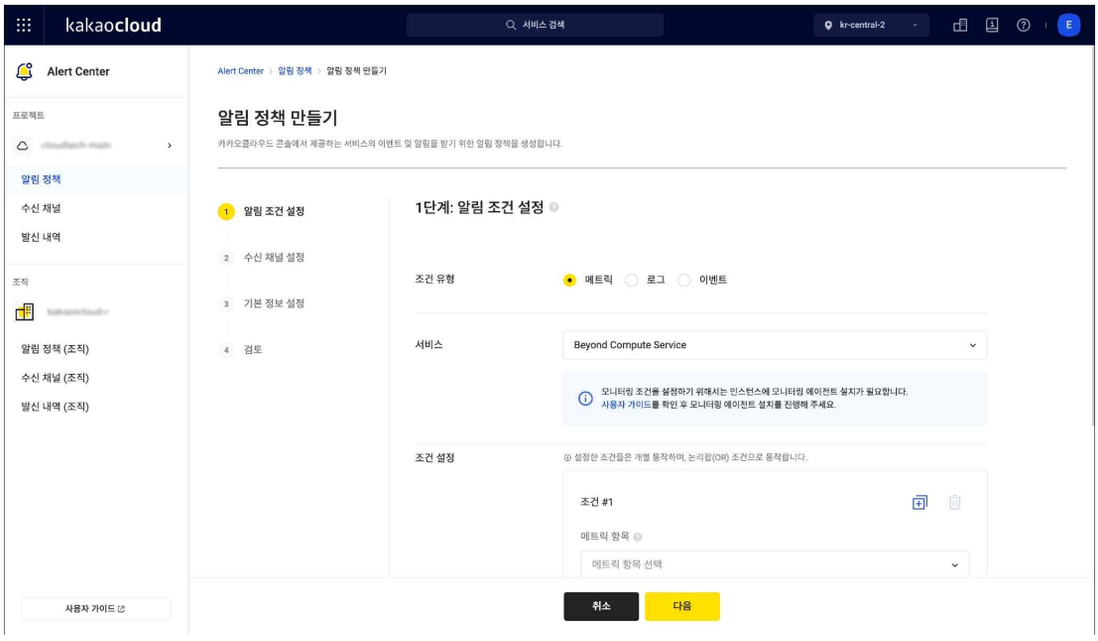
| 그림 5-3-14 | 모니터링 에이전트 설치



| 그림 5-3-15 | 사용자 계정정보에서 연락처 정보 인증 및 설정

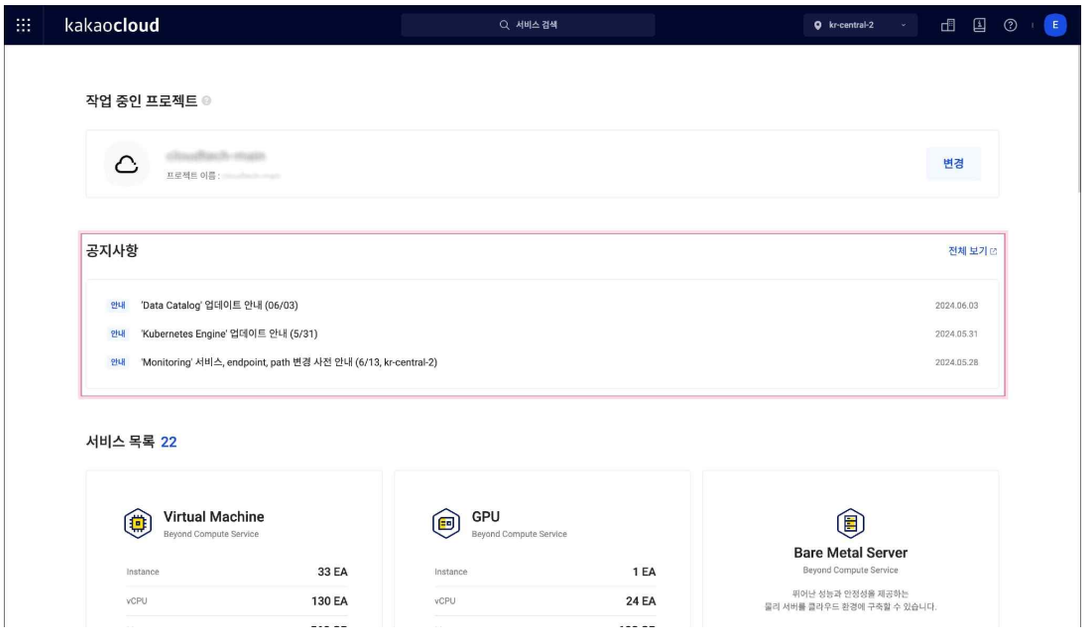


| 그림 5-3-16 | 수신 채널 생성



| 그림 5-3-17 | 메트릭, 로그, 이벤트를 트리거로 한 알림 정책 생성

- 또한, 카카오클라우드에서는 서비스 장애 발생 시 공지사항 페이지에 공지를 등록하여 사용자에게 안내합니다.

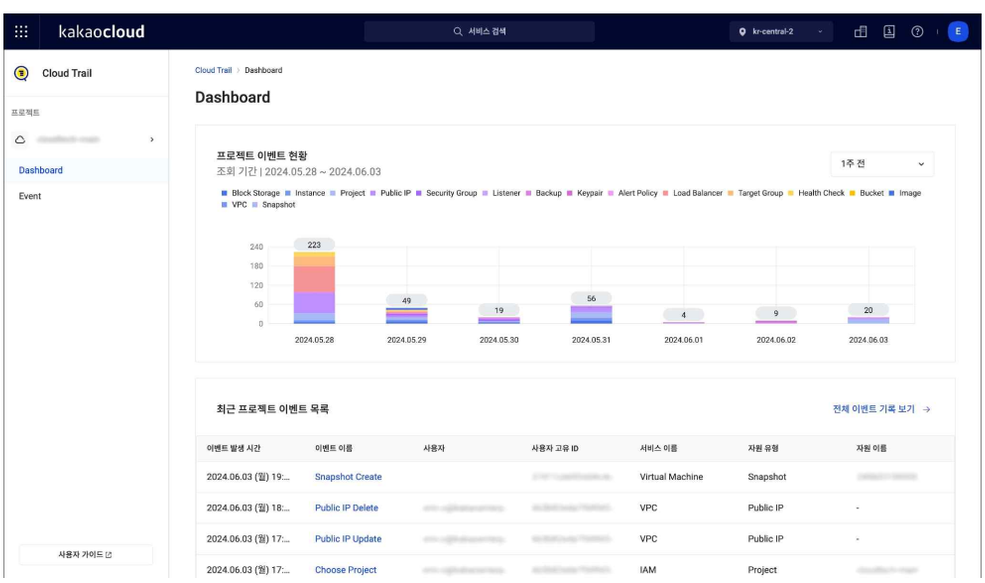


| 그림 5-3-18 | 카카오클라우드 콘솔에서 확인할 수 있는 공지사항

| 그림 5-3-19 | 카카오클라우드 포털에서 확인할 수 있는 공지사항

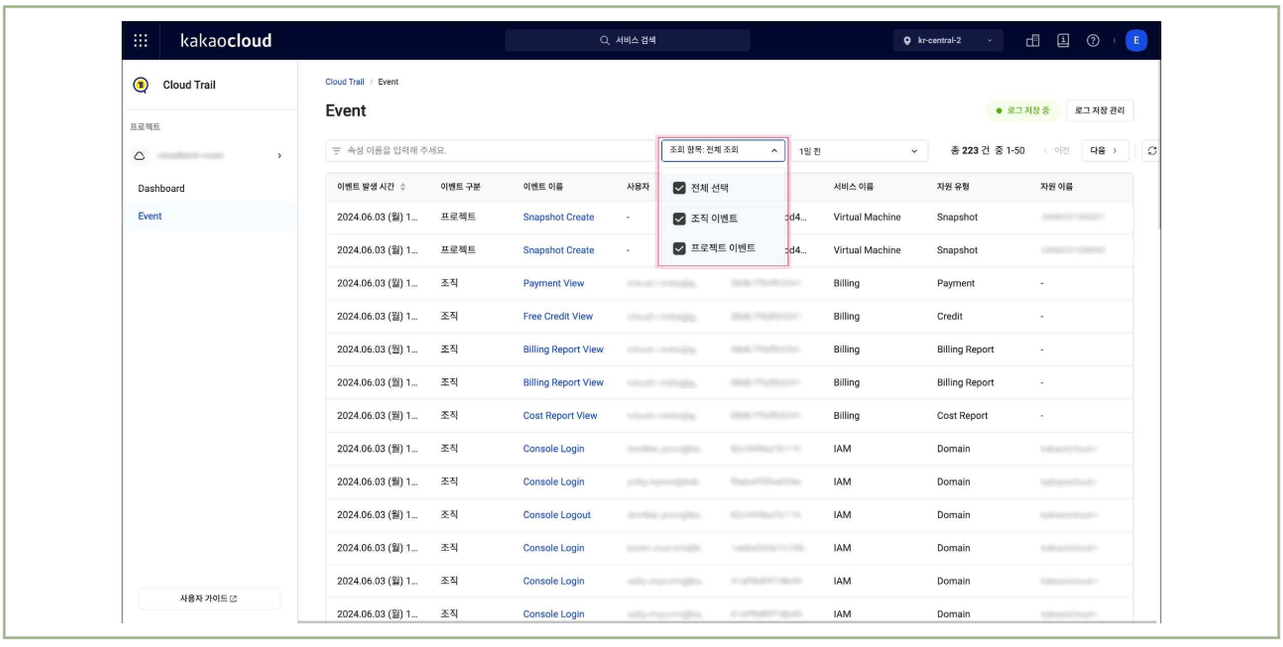
- 사용자는 알림과 공지를 참조하여 장애상황기록를 작성한다.

- 가상자원 네트워크 정책 변경(삭제 등) 모니터링
  - 카카오클라우드에서는 네트워크 서비스 사용 시 발생하는 사항에 대한 행위추적성 확보를 위해 Cloud Trail 서비스를 제공합니다.



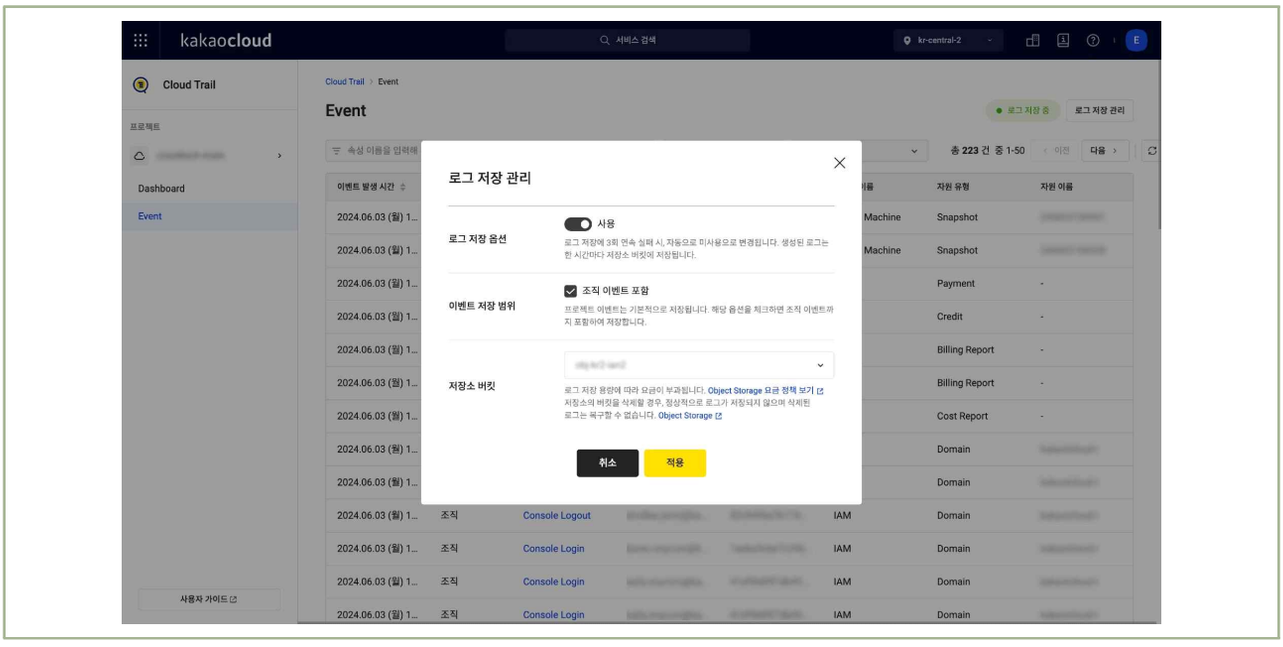
| 그림 5-3-20 | Cloud Trail 서비스의 Dashboard

- 카카오클라우드의 Cloud Trail 의 이벤트는 조직 이벤트와 프로젝트 이벤트로 구분되며, 네트워크 관련 행위 추적은 프로젝트 이벤트로 기록됩니다. 기록되는 이벤트로는 VPC, 서브넷, 라우팅 테이블, 라우트, 보안그룹, 로드밸런서 등에 대한 생성, 삭제, 변경에 대한 이벤트가 제공됩니다.



| 그림 5-3-21 | 조직 이벤트와 프로젝트 이벤트로 구분되는 Cloud Trail 이벤트

- Cloud Trail 로그는 최대 90일 이전까지의 기록만 제공하며, 추가 기능으로 로그 저장 관리 기능을 제공하여 90일보다 오래된 이벤트를 오브젝트 스토리지에 저장하여 관리할 수 있도록 합니다.



| 그림 5-3-22 | 로그 저장 관리 설정 모달

4 참고 사항

- 카카오클라우드 Monitoring 가이드
- 카카오클라우드 모니터링 에이전트 설치 가이드
- 카카오클라우드 Monitoring 〉 대시보드 활용 가이드
- 카카오클라우드 Alert Center 〉 수신 채널 생성 및 관리 가이드
- 카카오클라우드 Alert Center 〉 알림 정책 생성 및 관리 가이드
- 카카오클라우드 Cloud Trail 가이드
- 카카오클라우드 Cloud Trail 로그 저장 관리 가이드

1 기준

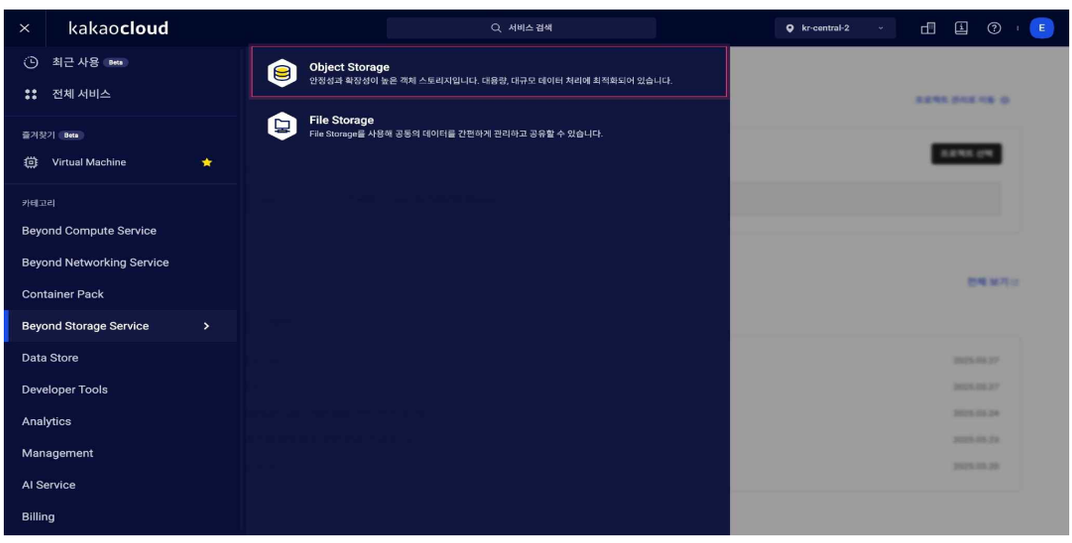
식별번호	기준	내용
5.4.	**API 사용(호출대상, 호출자, 호출일시 등)에 관한 행위추적성 확보**	**API 사용 이력에 대한 행위추적성(로그 등)을 확보하여야 한다.**

2 설명

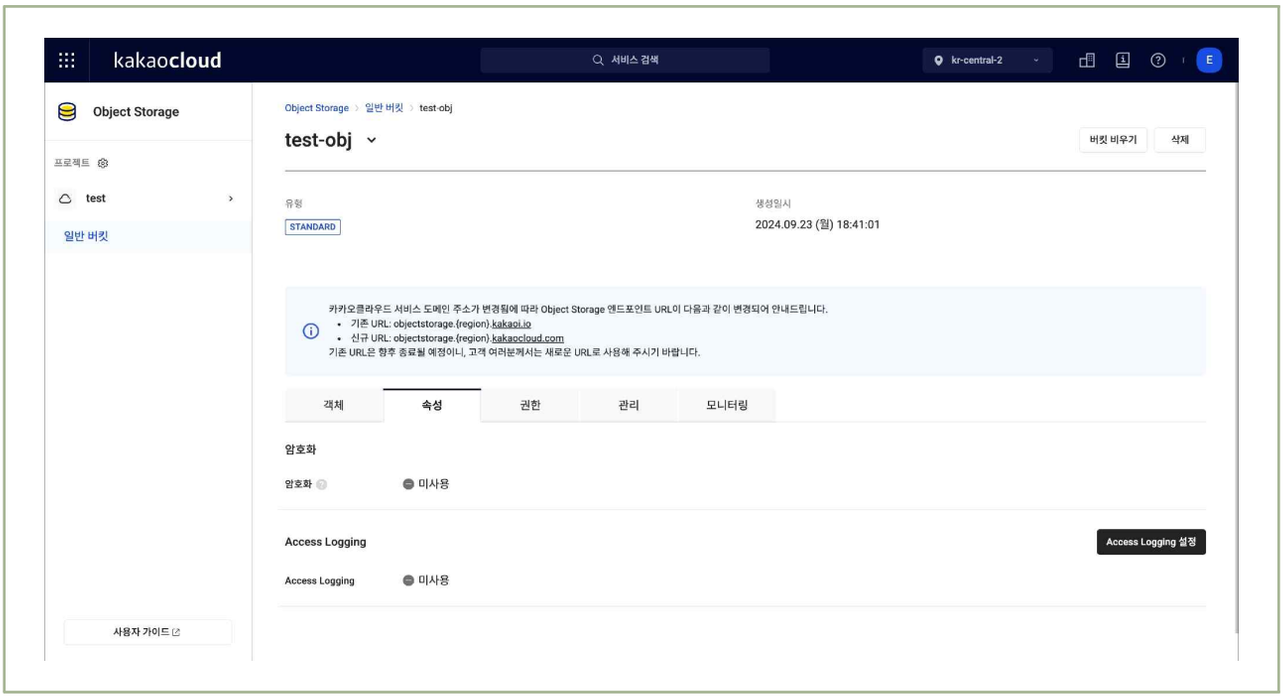
- API 사용 이력에 대한 행위추적성을 확보하여야 한다.
  - 행위 감사로그
    1) API 호출에 관한 정보(호출대상, 호출자, 호출일시 등)

3 우수 사례

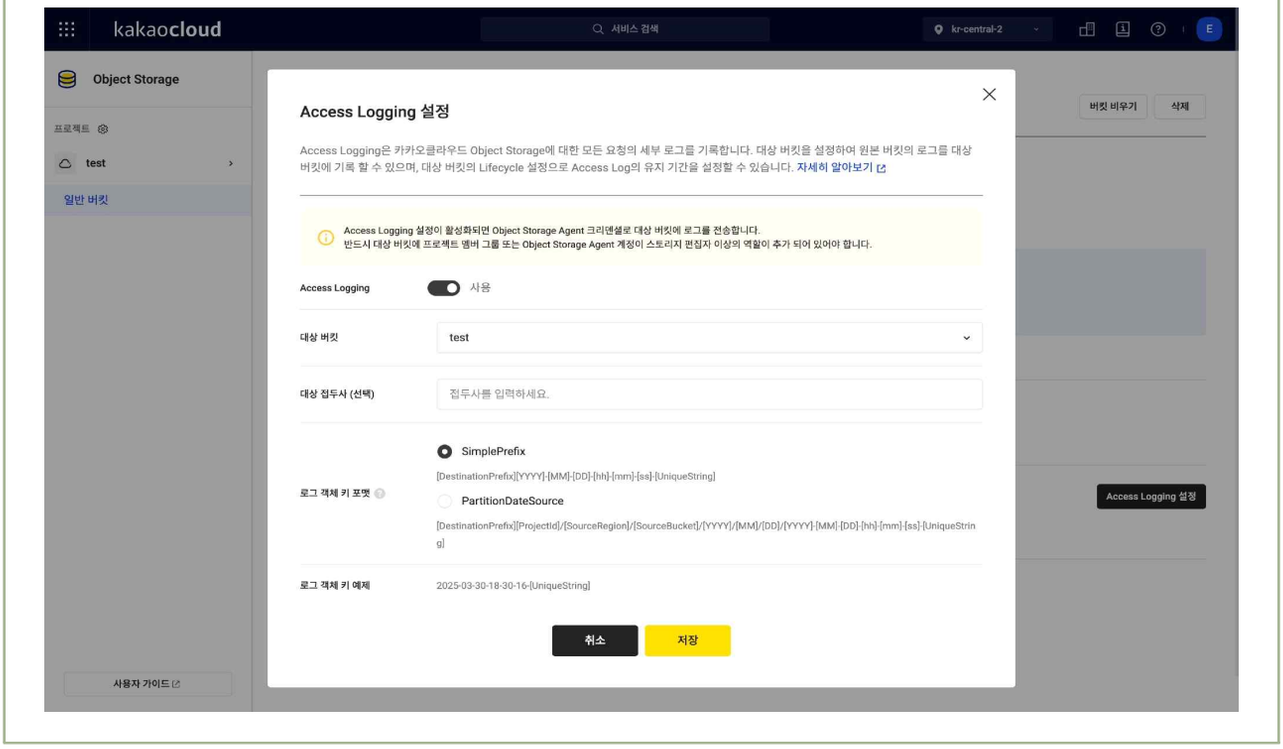
- Object Storage API를 이용할 경우, Access Logging 기능을 통해 API 사용에 대한 이력 확인이 가능합니다.
  - **(Console)** 'Dashboard' → 'Beyond Storage Service' → 'Object Storage' → 특정 버킷에서 Access Logging 설정



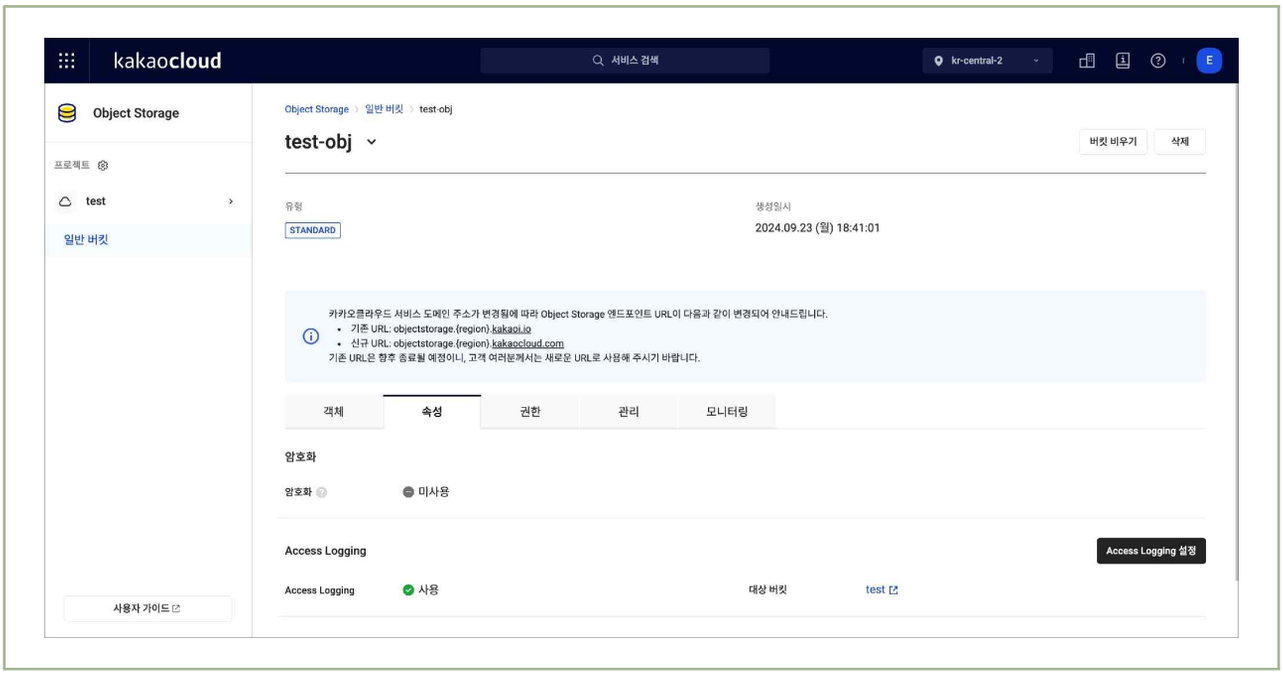
| 그림 5-4-1 | 카카오클라우드 콘솔 〉 Object Storage 서비스 이동



| 그림 5-4-2 | 버킷 상세 페이지 〉 속성 탭 〉 Access Logging 설정 버튼

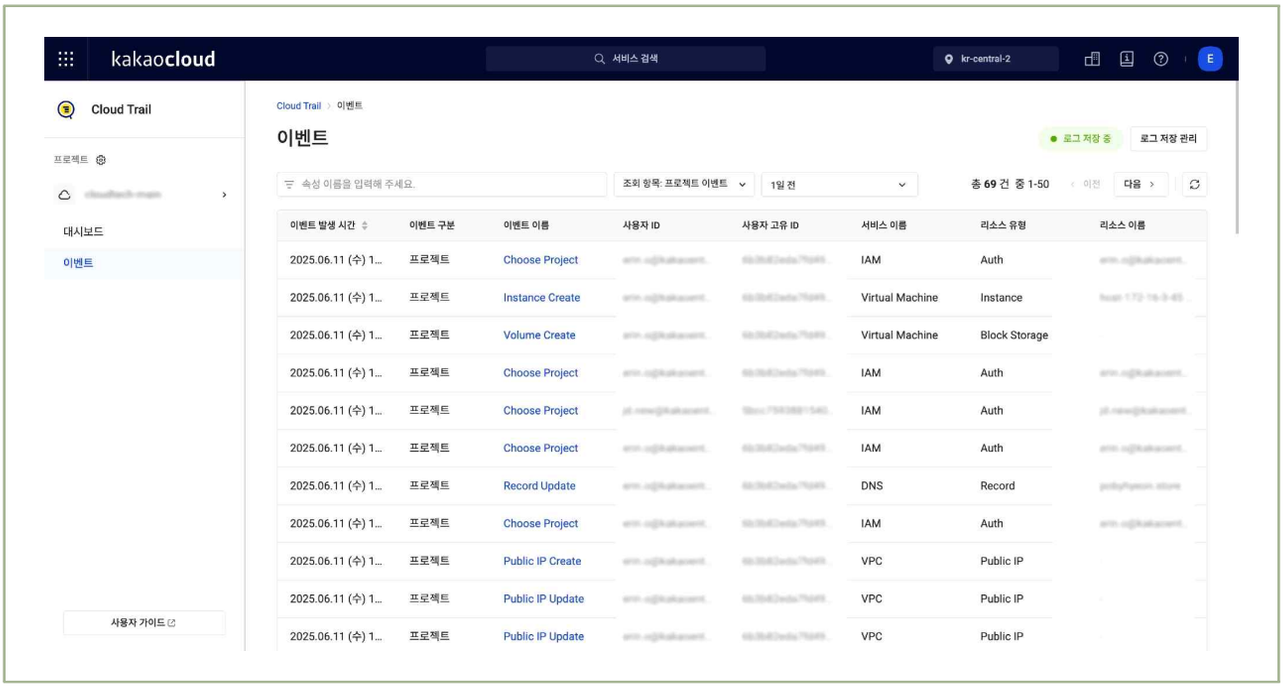


| 그림 5-4-3 | Access Logging 설정 모달

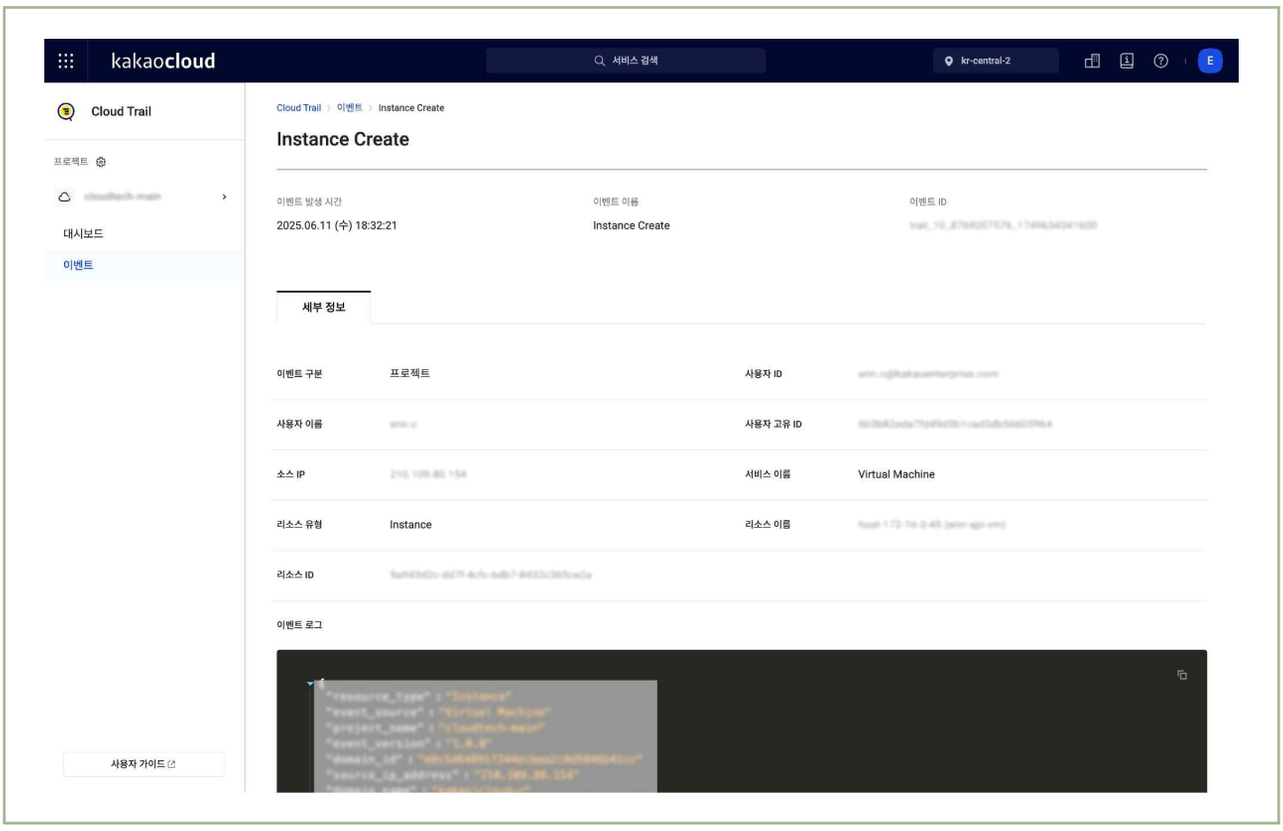


| 그림 5-4-4 | Access Logging 설정됨 확인

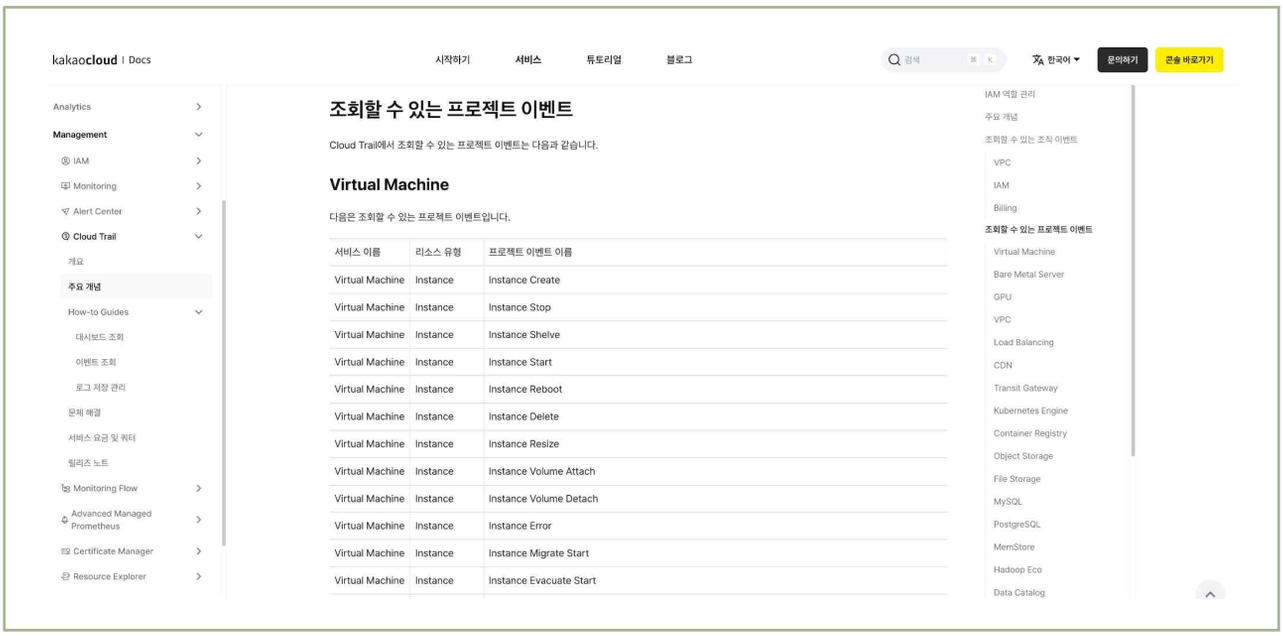
- OpenAPI사용 이력의 경우, Cloud Trail 이벤트 로그를 통해 조회가 가능합니다.
  - **(Console)** 'Dashboard' → 'Management' → 'Cloud Trail' → 이벤트 탭 → 프로젝트 이벤트 조회



| 그림 5-4-5 | 카카오클라우드 콘솔 〉 Cloud Trail 〉 프로젝트 이벤트 목록



| 그림 5-4-6 | 카카오클라우드 콘솔 〉 Cloud Trail 〉 프로젝트 이벤트 상세 내용



| 그림 5-4-7 | Cloud Trail 조회 가능한 프로젝트 이벤트 목록

- Cloud Trail에 저장된 이벤트를 로그 저장 관리 기능을 통해 Object Storage에 장기간 저장이 가능합니다. (8.1 클라우드 이용에 관한 행위추적성 증적(로그 등) 백업 참고)

4 참고 사항

- 카카오클라우드 Object Storage Access Log 가이드
- 카카오클라우드 Object Storage API 가이드
- 카카오클라우드 Cloud Trail 조회 가능한 이벤트 목록

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

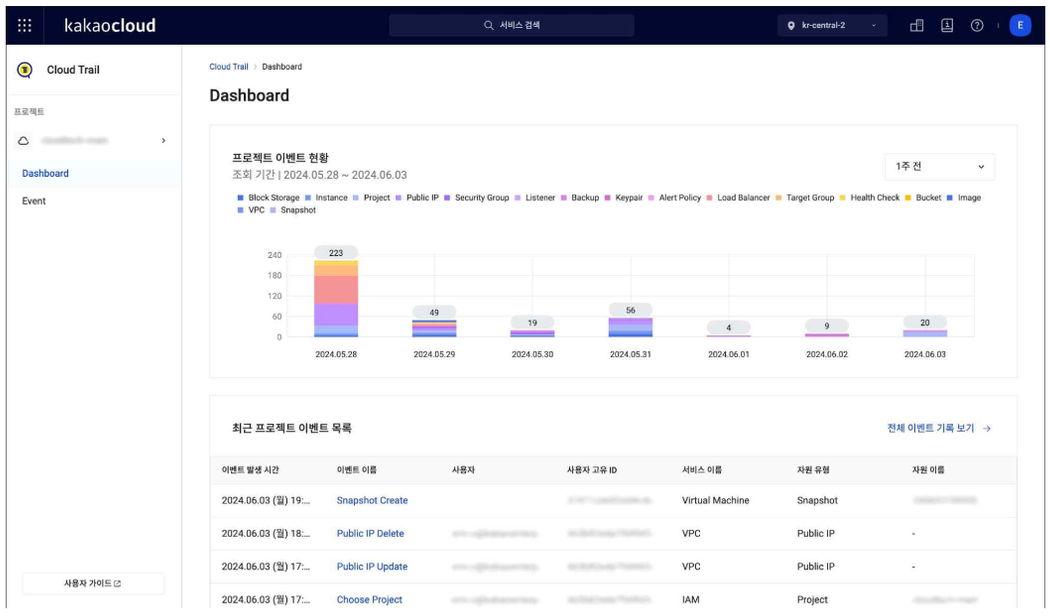
- 클라우드 환경에서 네트워크 서비스(VPC, NAT 등) 사용 시 발생하는 사항에 대한 행위추적성(로그 등)을 확보하여야 한다.

  - 행위 감사로그

    1) 네트워크 서비스 이용에 관한 사항(VPC, NAT 규칙 생성 및 변경 등) 등

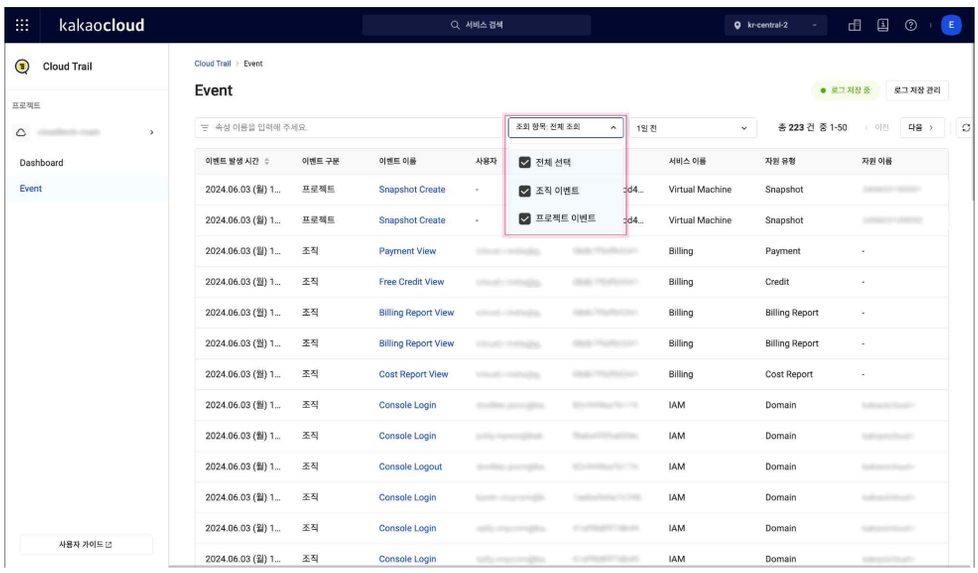
3 우수 사례

- 카카오클라우드에서는 네트워크 서비스 사용 시 발생하는 사항에 대한 행위추적성 확보를 위해 Cloud Trail 서비스를 제공합니다.



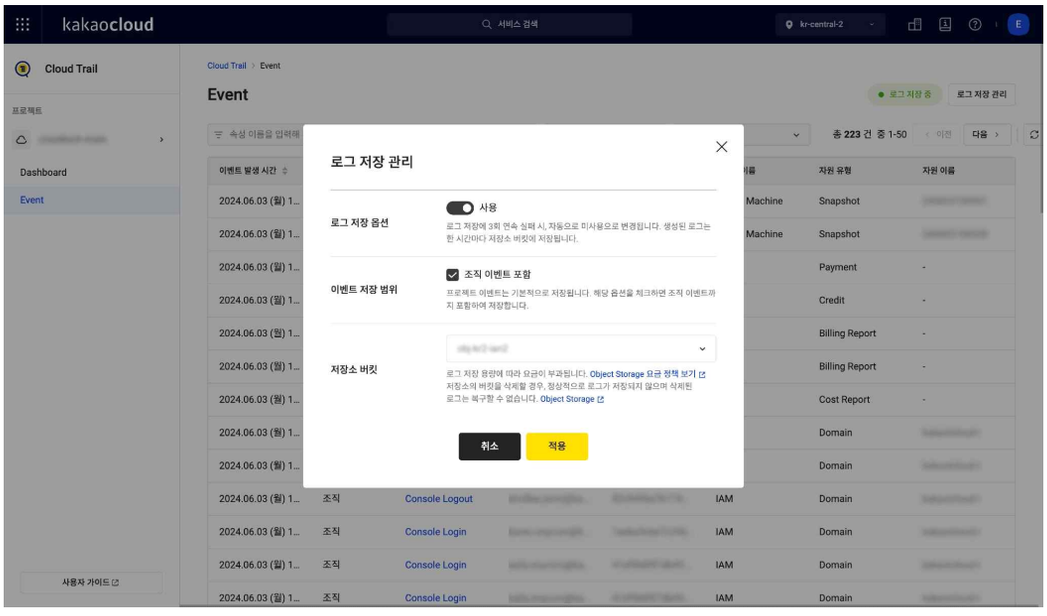
| 그림 5-5-1 | Cloud Trail 서비스의 Dashboard

- 카카오클라우드의 Cloud Trail의 이벤트는 조직 이벤트와 프로젝트 이벤트로 구분되며, 네트워크 관련 행위 추적은 프로젝트 이벤트로 기록됩니다. 기록되는 이벤트로는 VPC, 서브넷, 라우팅 테이블, 라우트, 보안그룹, 로드밸런서 등에 대한 생성, 삭제, 변경에 대한 이벤트가 제공됩니다.



| 그림 5-5-2 | 조직 이벤트와 프로젝트 이벤트로 구분되는 Cloud Trail 이벤트

- Cloud Trail 로그는 최대 90일 이전까지의 기록만 제공하며, 추가 기능으로 로그 저장 관리 기능을 제공하여 90일보다 오래된 이벤트를 오브젝트 스토리지에 저장하여 관리할 수 있도록 합니다.



| 그림 5-5-3 | 로그 저장 관리 설정 모달

4 참고 사항

- 카카오클라우드 Cloud Trail 가이드
- 카카오클라우드 Cloud Trail 로그 저장 관리 가이드

1 기준

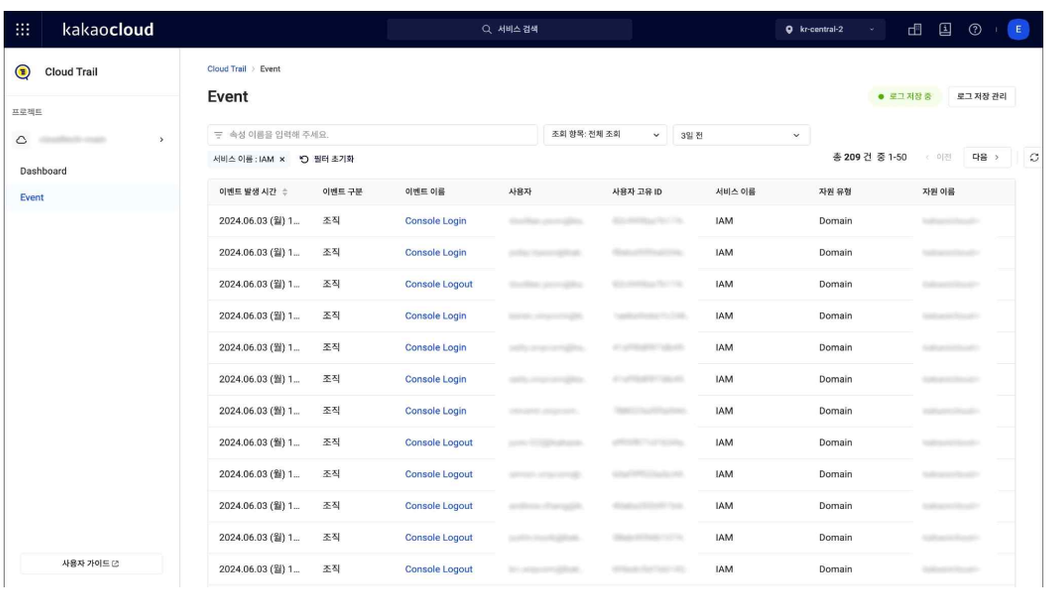
식별번호	기준	내용
5.6.	**계정 변동사항에 대한 행위 추적성 확보**	**클라우드 계정 변동사항에 대한 행위추적성(로그 등)을 확보하여야 한다.**

2 설명

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

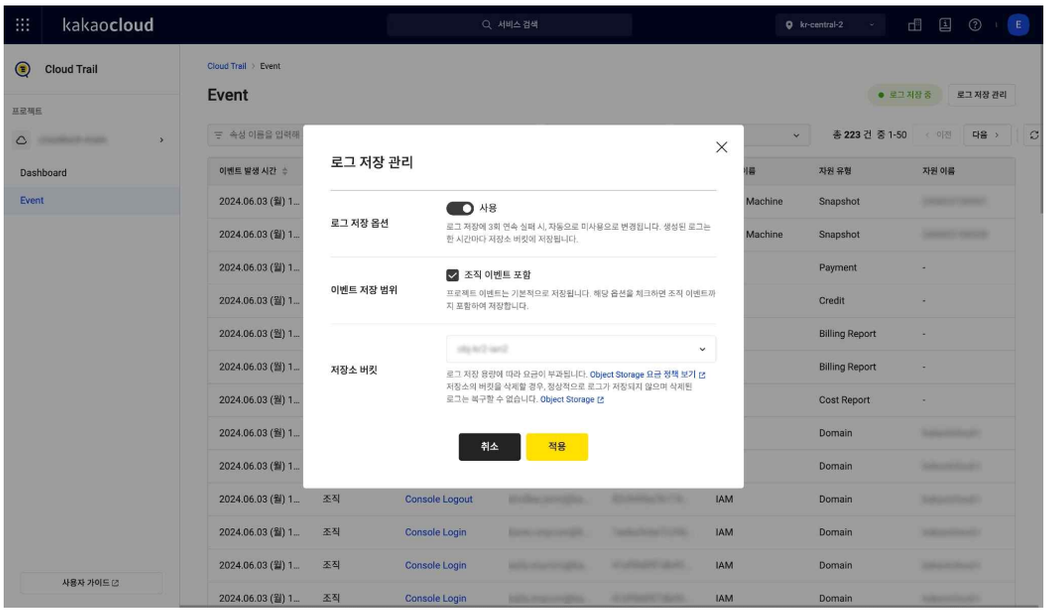
3 우수 사례

- 클라우드 가상자원 관리시스템 접속 계정 생성, 변경, 삭제에 관한 사항
  - 카카오클라우드에서는 Cloud Trail의 조직 이벤트에서 User Add, Delete, Group Assign 등 계정 변경사항에 대한 이벤트 기록을 제공합니다.



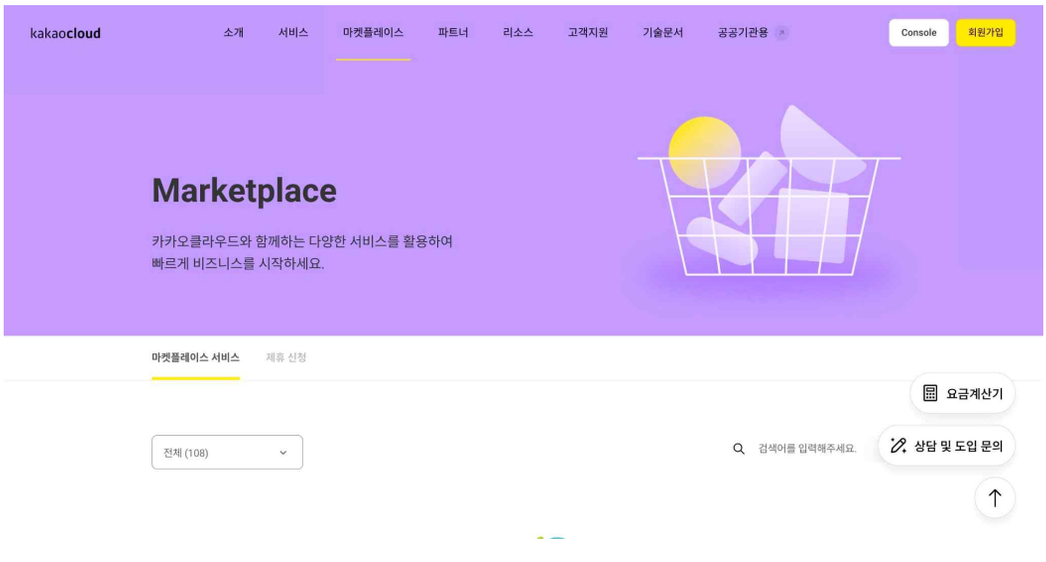
| 그림 5-6-1 | 계정 관련 Cloud Trail Event

- Cloud Trail 로그는 최대 90일 이전까지의 기록만 제공하며, 추가 기능으로 로그 저장 관리 기능을 제공하여 90일보다 오래된 이벤트를 오브젝트 스토리지에 저장하여 관리할 수 있도록 합니다.



| 그림 5-6-2 | 로그 저장 관리 설정 모달

- 클라우드 가상자원(서버, 데이터베이스 등) 접속 계정 생성, 변경, 삭제에 관한 사항
  - 가상자원에 대한 접속 계정 생성, 변경, 삭제에 관한 사항은 마켓플레이스 상품(접근제어 솔루션)을 통해 기록 및 저장할 수 있습니다



| 그림 5-6-3 | 카카오클라우드 콘솔의 마켓플레이스

4 참고 사항

- 카카오클라우드 Cloud Trail 가이드
- 카카오클라우드 Cloud Trail 로그 저장 관리 가이드
- 카카오클라우드 마켓플레이스 상품 소개

1 기준

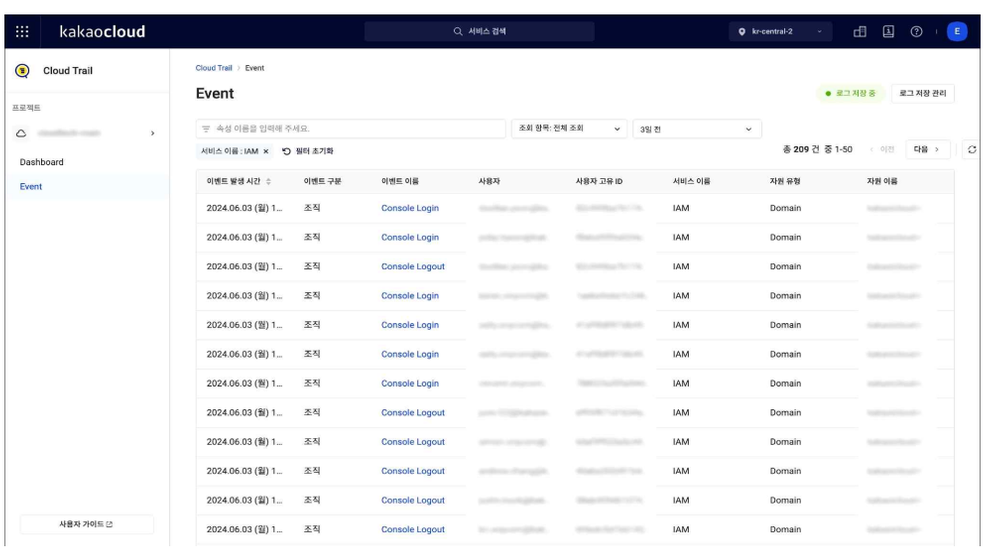
식별번호	기준	내용
5.7.	**계정 변경사항에 관한 모니터링 수행**	**클라우드 서비스 이용 계정 변경사항(생성, 삭제 등)에 관한 로깅 및 모니터링을 수행하여야 한다.**

2 설명

- 클라우드 서비스 이용 계정 변경사항에 관한 모니터링을 수행하여야 한다.
  - 예시
    1) 계정 변경사항에 관한 상시 모니터링 수행
    2) 전자금융감독규정 및 금융회사 내부규정 등에 수립된 주기에 맞추어 주기적 검토 수행
    3) 관리자 계정에 대해서는 이중확인 수행 등

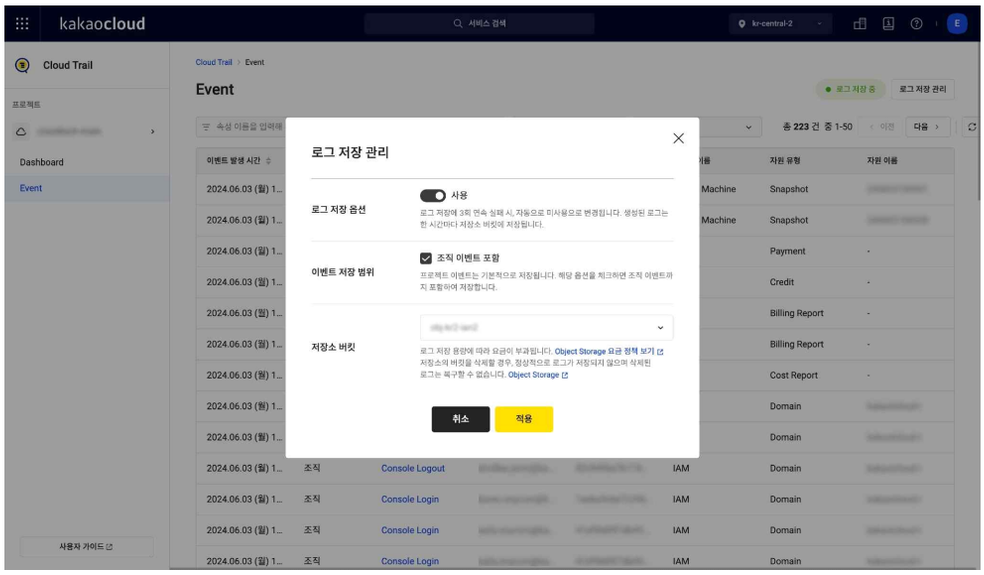
3 우수 사례

- 계정 변경사항에 관한 상시 모니터링 수행
  - 카카오클라우드에서는 Cloud Trail의 조직 이벤트에서 User Add, Delete, Group Assign 등 계정 변경사항에 대한 이벤트 기록을 제공합니다.



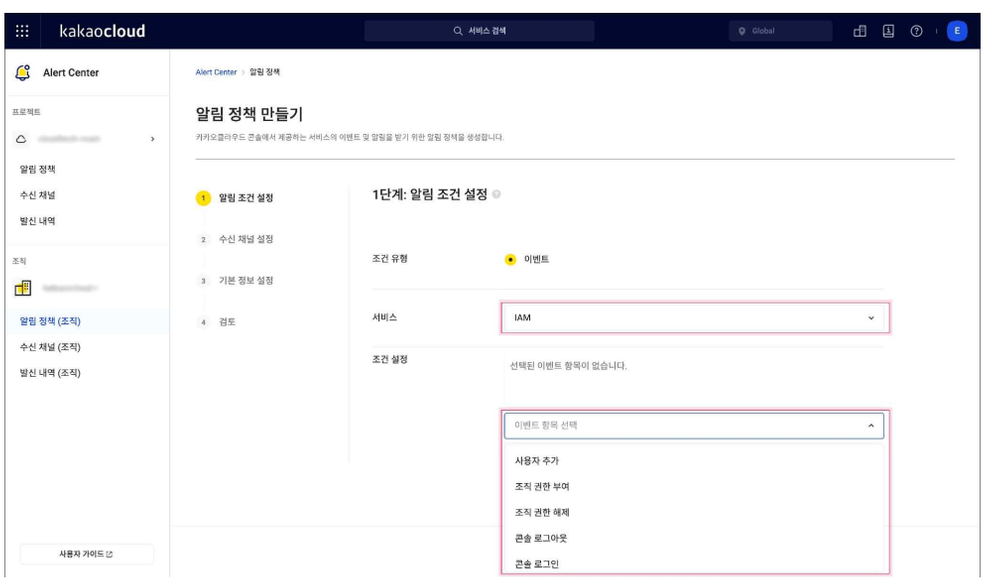
| 그림 5-7-1 | 계정 관련 Cloud Trail Event

- Cloud Trail 로그는 최대 90일 이전까지의 기록만 제공하며, 추가 기능으로 로그 저장 관리 기능을 제공하여 90일보다 오래된 이벤트를 오브젝트 스토리지에 저장하여 관리할 수 있도록 합니다.



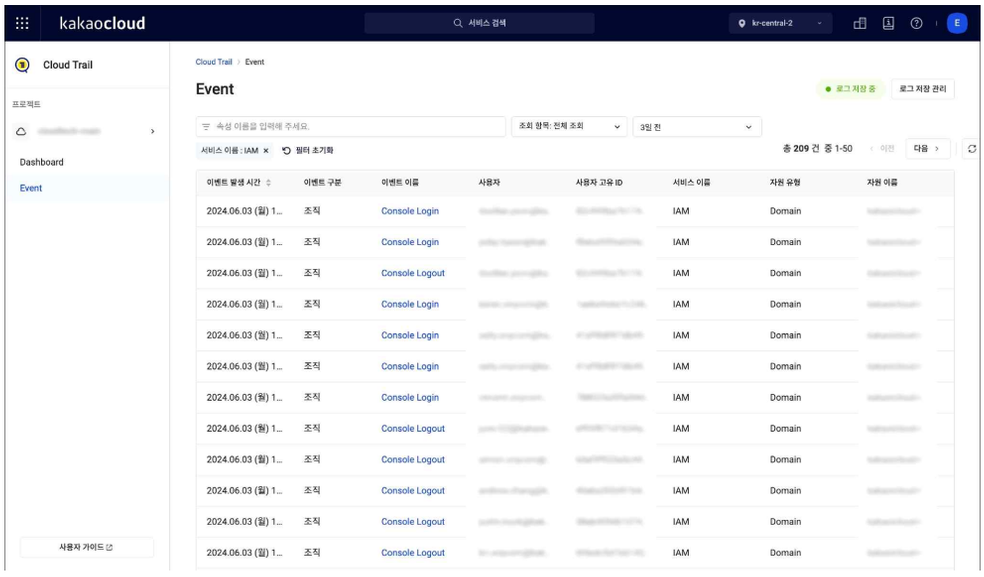
| 그림 5-7-2 | 로그 저장 관리 설정 모달

- Alert Center의 조직 레벨의 알림 정책을 통해 사용자 추가/삭제, 콘솔 로그인/로그아웃 등의 이벤트 발생 시 알림을 받도록 설정이 가능합니다. 관리자는 수신 채널 설정과 조직 레벨의 알림 정책을 설정하여 계정 변경사항에 대한 상시 모니터링을 수행할 수 있습니다.



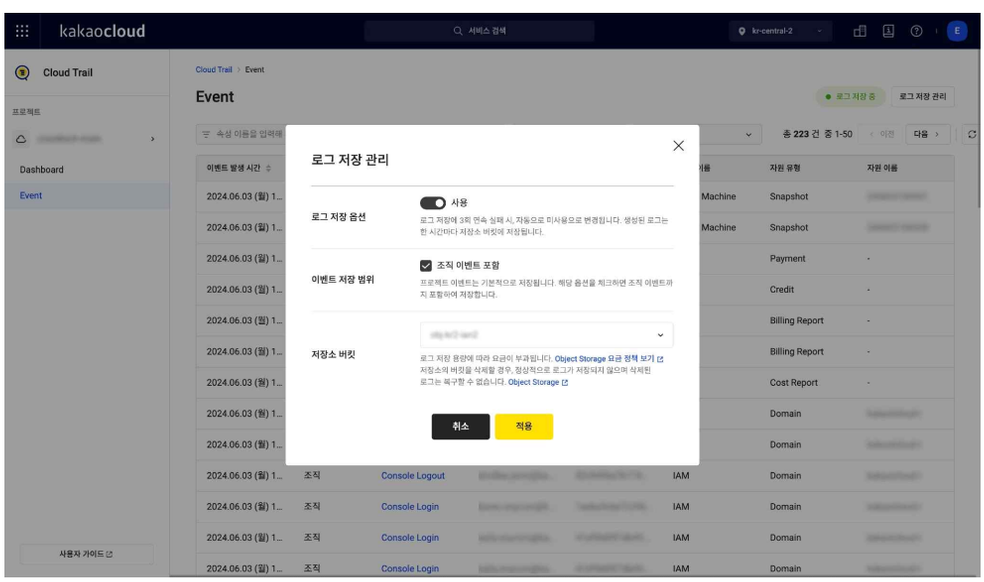
| 그림 5-7-3 | 조직 레벨의 알림 정책 생성

- 전자금융감독규정 및 금융회사 내부규정등에 수립된 주기에 맞추어 주기적 검토 수행
  - 카카오클라우드에서는 Cloud Trail의 조직 이벤트에서 User Add, Delete, Group Assign 등 계정 변경사항에 대한 이벤트 기록을 제공합니다.



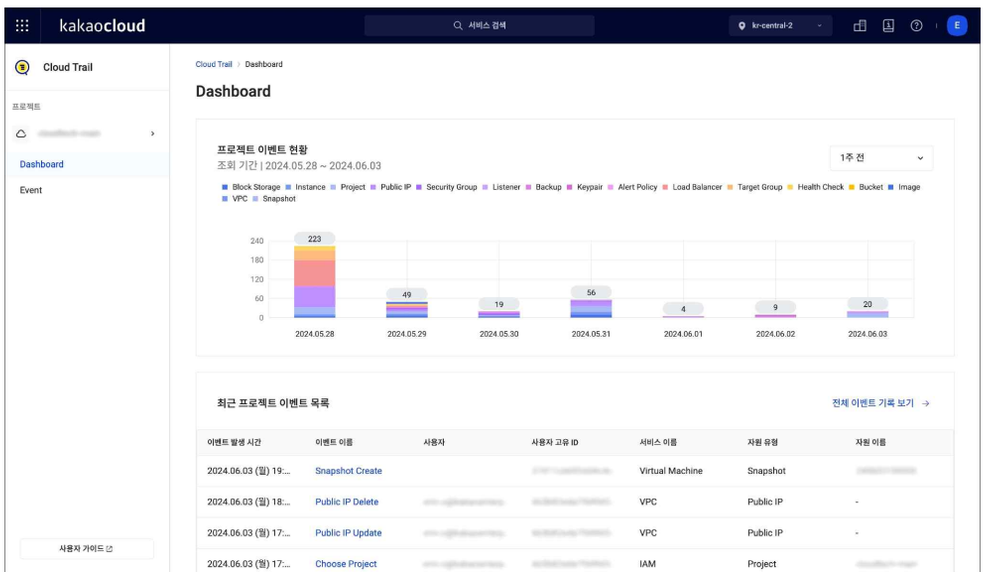
| 그림 5-7-4 | 계정 관련 Cloud Trail Event

  - Cloud Trail 로그는 최대 90일 이전까지의 기록만 제공하며, 추가 기능으로 로그 저장 관리 기능을 제공하여 90일보다 오래된 이벤트를 오브젝트 스토리지에 저장하여 관리할 수 있도록 합니다.



| 그림 5-7-5 | 로그 저장 관리 설정 모달

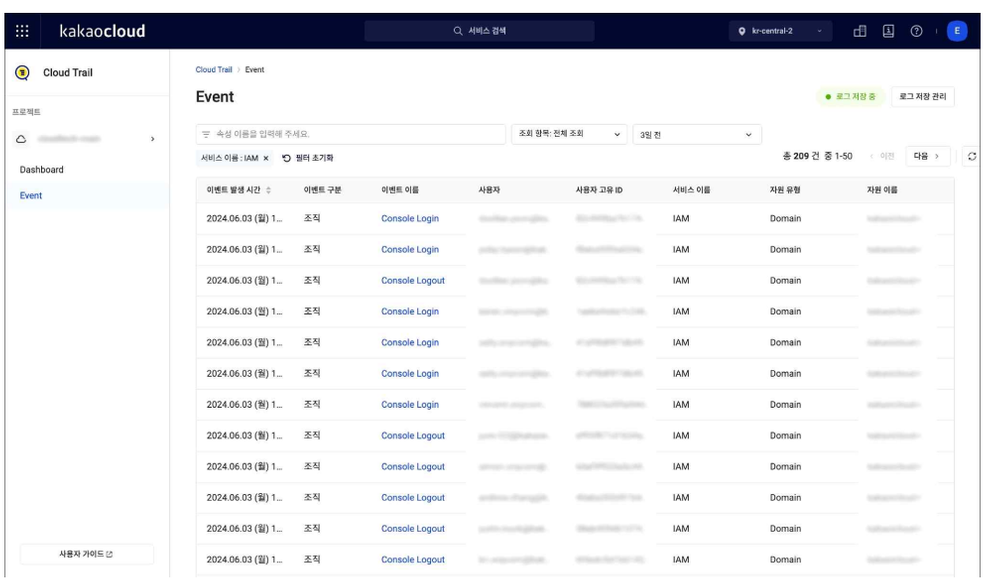
- 관리자는 전자금융감독규정 및 금융회사 내부규정등에 수립된 주기에 맞추어 주기적으로 Cloud Trail 서비스를 확인합니다.



| 그림 5-7-6 | Cloud Trail 서비스의 Dashboard

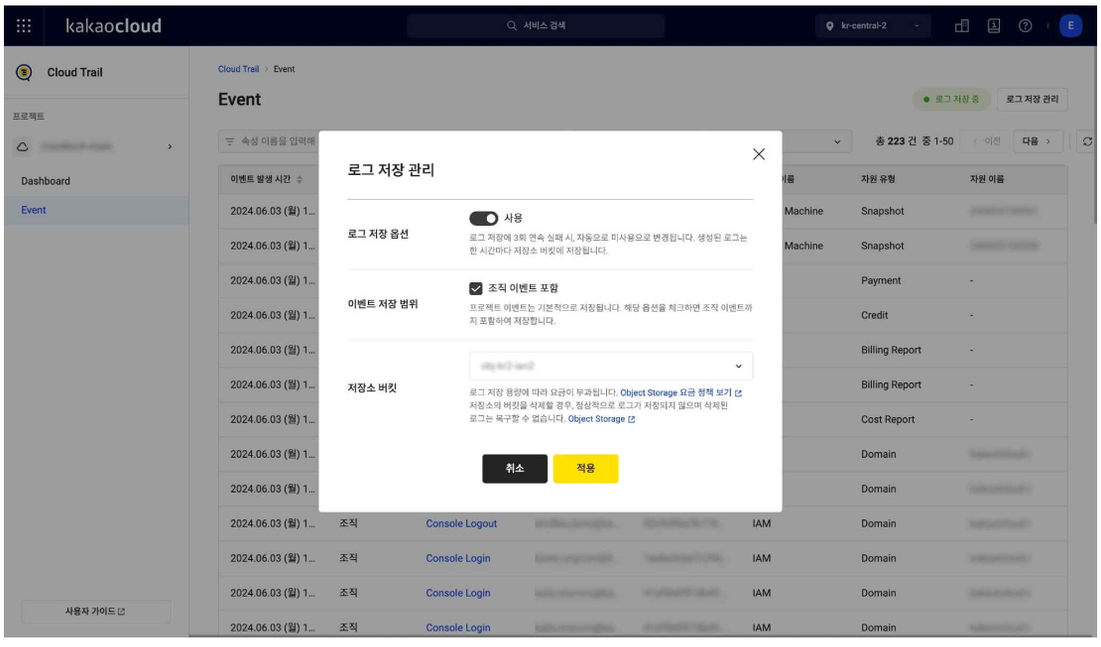
- 관리자 계정에 대해서는 이중확인 수행 등

- 카카오클라우드에서는 Cloud Trail의 조직 이벤트에서 User Add, Delete, Group Assign 등 계정 변경사항에 대한 이벤트 기록을 제공합니다.



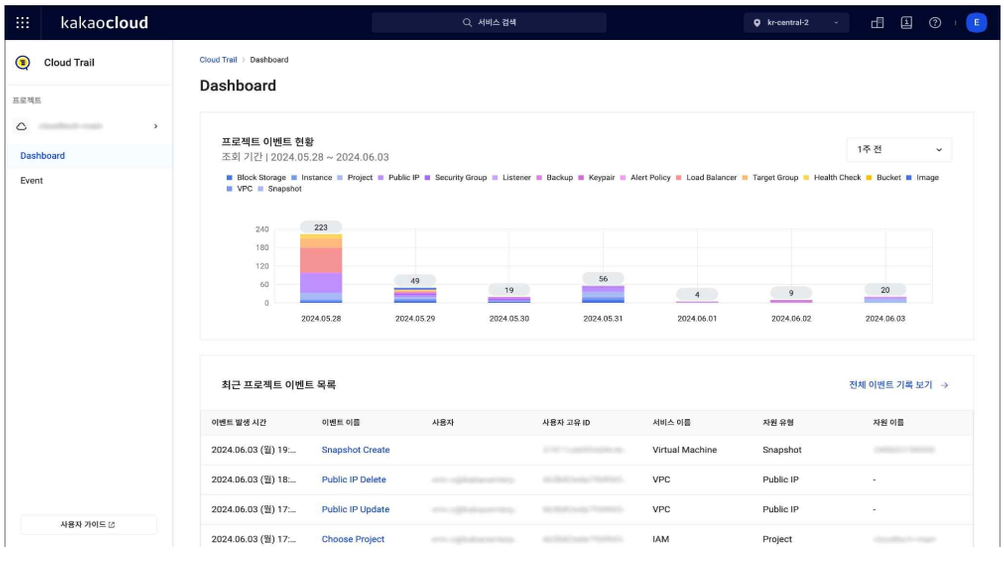
| 그림 5-7-7 | 계정 관련 Cloud Trail Event

- Cloud Trail 로그는 최대 90일 이전까지의 기록만 제공하며, 추가 기능으로 로그 저장 관리 기능을 제공하여 90일보다 오래된 이벤트를 오브젝트 스토리지에 저장하여 관리할 수 있도록 합니다.



| 그림 5-7-8 | 로그 저장 관리 설정 모달

- 관리자는 관리자 권한을 가진 계정에 대해서는 Cloud Trail 로그를 이중으로 확인합니다.



| 그림 5-7-9 | Cloud Trail 서비스의 Dashboard

4 참고 사항

- 카카오클라우드 Cloud Trail 가이드
- 카카오클라우드 Cloud Trail 로그 저장 관리 가이드
- 카카오클라우드 Alert Center 〉 수신 채널 생성 및 관리 가이드
- 카카오클라우드 Alert Center 〉 알림 정책 생성 및 관리 가이드

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 세션 및 서명 유효기간 적용
6.5. API 호출 구간 암호화 적용

6 API 관리

1 기준

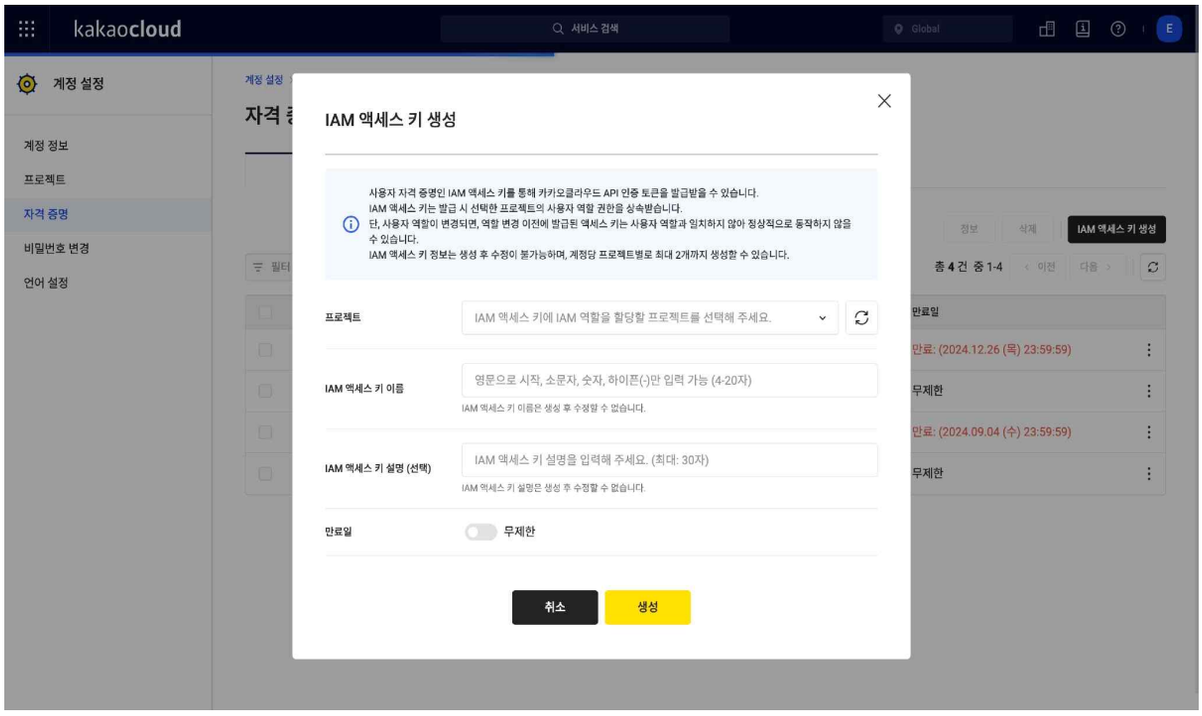
식별번호	기준	내용
6.1.	API 호출 시 인증 수단 적용	**클라우드 가상자원 관리를 위한 API 호출 시, 안전한 인증수단을 적용하여 보안성을 강화하여야 한다.**

2 설명

- API 호출 시 이용자를 인증할 수 있는 수단을 적용하여야 한다.
  - 예시
    1) API 호출이 가능한 IP 지정
    2) IAM 기능과 연동하여 API를 호출할 수 있는 권한 제어 등

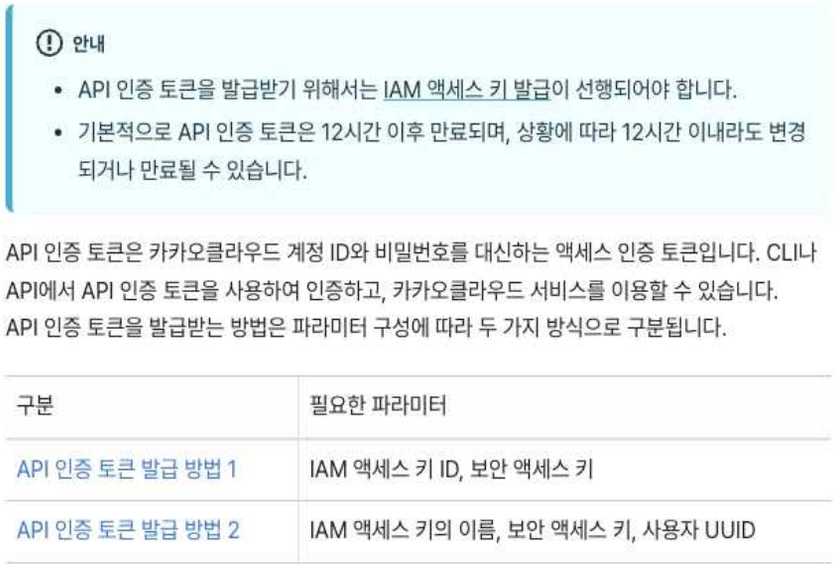
3 우수 사례

- API 인증 토큰을 사용하여 API를 호출할 때, 해당 토큰이 발급된 액세스 키 ID와 보안 액세스 키에 할당된 IAM 역할에 따라 호출할 수 있는 API가 달라집니다.
  - IAM 액세스 키는 발급 시 발급받은 사용자의 IAM 역할에 따라 호출할 수 있는 API가 달라집니다.
  - **(예시)** Billing 관리자, 빌링 매니저, 빌링 뷰어 역할을 가지고 있지 않은 사용자의 경우, Billing 조회 API 불가능
  - **(Console)** 우측 상단 프로필 아이콘 〉 '자격 증명' 〉 IAM 액세스 키 생성



| 그림 6-1-1 | 액세스 키 생성 시, 사용자 역할 권한 관련 문구 노출

- API 인증 토큰은 12시간 이후 만료되며, 상황에 따라 12시간 이내라도 변경되거나 만료될 수 있습니다.



안내

- API 인증 토큰을 발급받기 위해서는 IAM 액세스 키 발급이 선행되어야 합니다.
- 기본적으로 API 인증 토큰은 12시간 이후 만료되며, 상황에 따라 12시간 이내라도 변경되거나 만료될 수 있습니다.

API 인증 토큰은 카카오클라우드 계정 ID와 비밀번호를 대신하는 액세스 인증 토큰입니다. CLI나 API에서 API 인증 토큰을 사용하여 인증하고, 카카오클라우드 서비스를 이용할 수 있습니다.
API 인증 토큰을 발급받는 방법은 파라미터 구성에 따라 두 가지 방식으로 구분됩니다.

구분	필요한 파라미터
API 인증 토큰 발급 방법 1	IAM 액세스 키 ID, 보안 액세스 키
API 인증 토큰 발급 방법 2	IAM 액세스 키의 이름, 보안 액세스 키, 사용자 UUID

| 그림 6-1-2 | API 인증 토큰 발급 시, 주의사항

- IdP 연동 기능을 사용하여 외부 IdP 계정으로 카카오클라우드에 로그인할 수 있습니다.
  - 카카오클라우드는 현재 외부 IdP 중 Azure AD의 계정 자격 증명을 지원하고 있습니다.
  - 외부 IdP 계정으로 카카오클라우드를 이용하는 경우, 카카오클라우드의 일부 계정 기능이 제한될 수 있습니다.

4 참고 사항

- 카카오클라우드 API 인증 토큰 발급 가이드
- 카카오클라우드 IdP OAuth 연동

1 기준

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

2 설명

- API 호출 시 호출 메시지의 무결성을 보장하기 위한 방안을 확보하여야 한다.

  - 예시

    1) API 보안 키와 서명을 통한 변조방지 대책 마련 등

3 우수 사례

- 카카오클라우드에서는 현재 API 호출 시 서명 등에 대한 기능이 제공되지 않습니다.

4 참고 사항

1 기준

식별번호	기준	내용
6.3.	**API 호출 시 인증키 보호대책 수립**	**API 호출 시 인증 키를 안전하게 보관하고 관리할 수 있는 방안을 마련해야 한다.**

2 설명

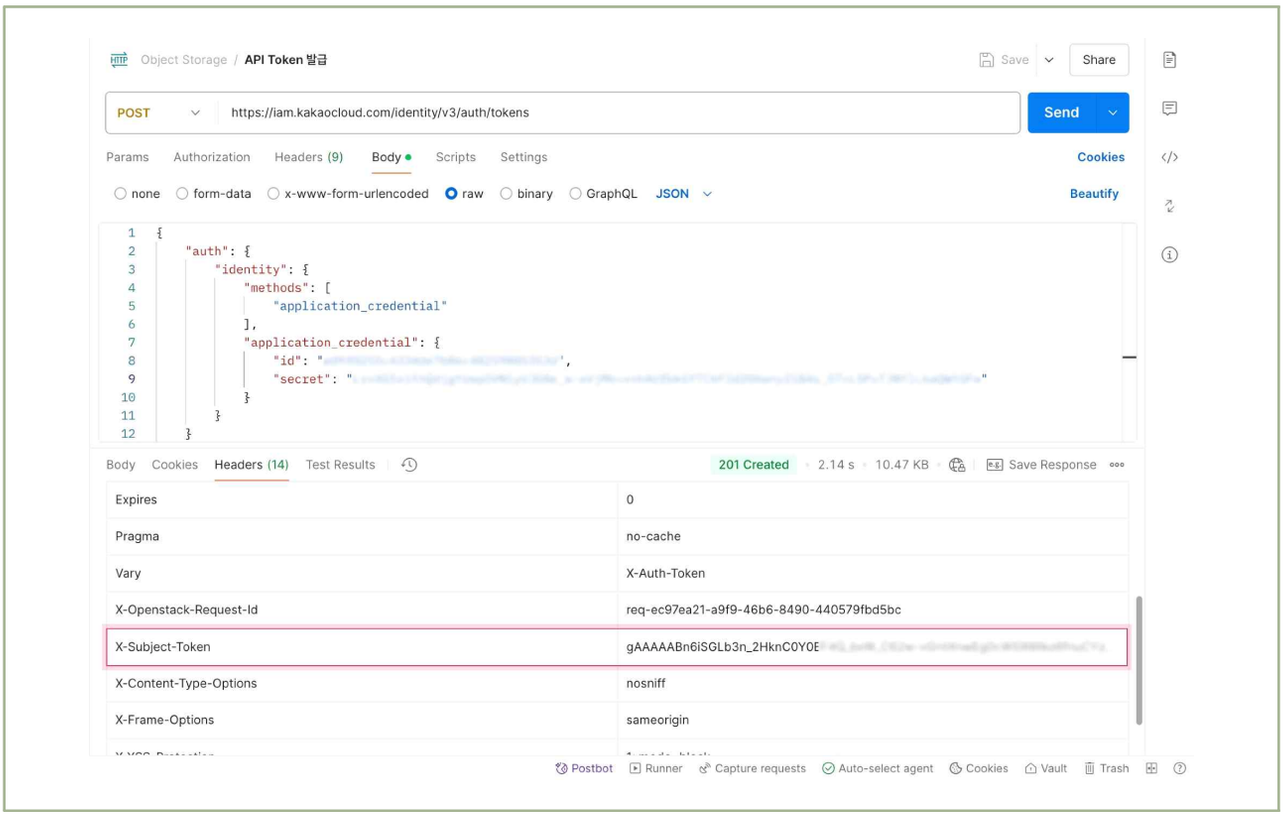
- API 호출 시 인용되는 유니크 값(ex. 보안키 등)은 안전하게 보관 및 관리하여야 한다.
  - 예시
    1) API 보안키 생성 시 이용자에게 1회만 노출 등 〉 API

3 우수 사례

- API 인증 토큰 발급을 위한 보안 액세스 키는 생성 당시 이용자에게 1회만 노출됩니다.
  - **(Console)** 우측 상단 프로필 아이콘 〉 '자격 증명' 〉 IAM 액세스 키 생성 시, 보안 액세스 키는 생성 당시 1회만 노출

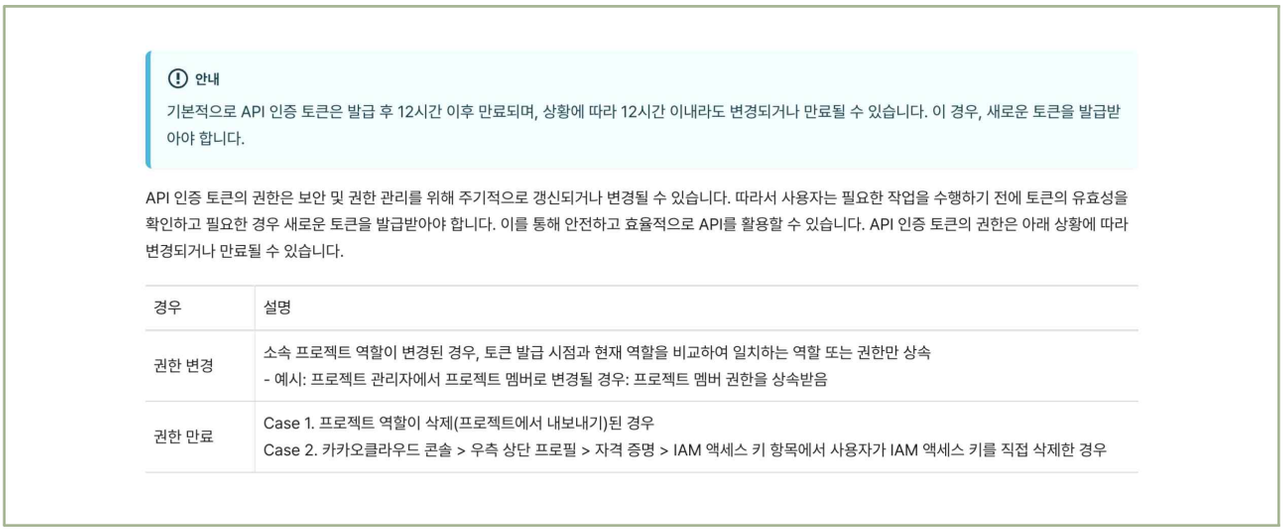
| 그림 6-3-1 | IAM 액세스 키 생성 시, 정보 확인 모달

- API 인증 토큰은 생성 요청 시, 이용자에게 1회만 노출됩니다.



| 그림 6-3-2 | API 인증 토큰 발급 방법

- API 인증 토큰은 12시간 이후 만료되며, 상황에 따라 12시간 이내라도 변경되거나 만료될 수 있습니다.



안내

기본적으로 API 인증 토큰은 발급 후 12시간 이후 만료되며, 상황에 따라 12시간 이내라도 변경되거나 만료될 수 있습니다. 이 경우, 새로운 토큰을 발급받아야 합니다.

API 인증 토큰의 권한은 보안 및 권한 관리를 위해 주기적으로 갱신되거나 변경될 수 있습니다. 따라서 사용자는 필요한 작업을 수행하기 전에 토큰의 유효성을 확인하고 필요한 경우 새로운 토큰을 발급받아야 합니다. 이를 통해 안전하고 효율적으로 API를 활용할 수 있습니다. API 인증 토큰의 권한은 아래 상황에 따라 변경되거나 만료될 수 있습니다.

경우	설명
권한 변경	소속 프로젝트 역할이 변경된 경우, 토큰 발급 시점과 현재 역할을 비교하여 일치하는 역할 또는 권한만 상속 - 예시: 프로젝트 관리자에서 프로젝트 멤버로 변경될 경우: 프로젝트 멤버 권한을 상속받음
권한 만료	Case 1. 프로젝트 역할이 삭제(프로젝트에서 내보내기)된 경우 Case 2. 카카오클라우드 콘솔 > 우측 상단 프로필 > 자격 증명 > IAM 액세스 키 항목에서 사용자가 IAM 액세스 키를 직접 삭제한 경우

| 그림 6-3-3 | API 인증 토큰 만료 관련 내용

- 카카오클라우드의 KMS와 인증키를 연동하는 기능은 하반기 출시 예정입니다.

4 참고 사항

- 카카오클라우드 API 인증 토큰 발급 가이드
- 카카오클라우드 IAM 액세스 키 발급 가이드

1 기준

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

2 설명

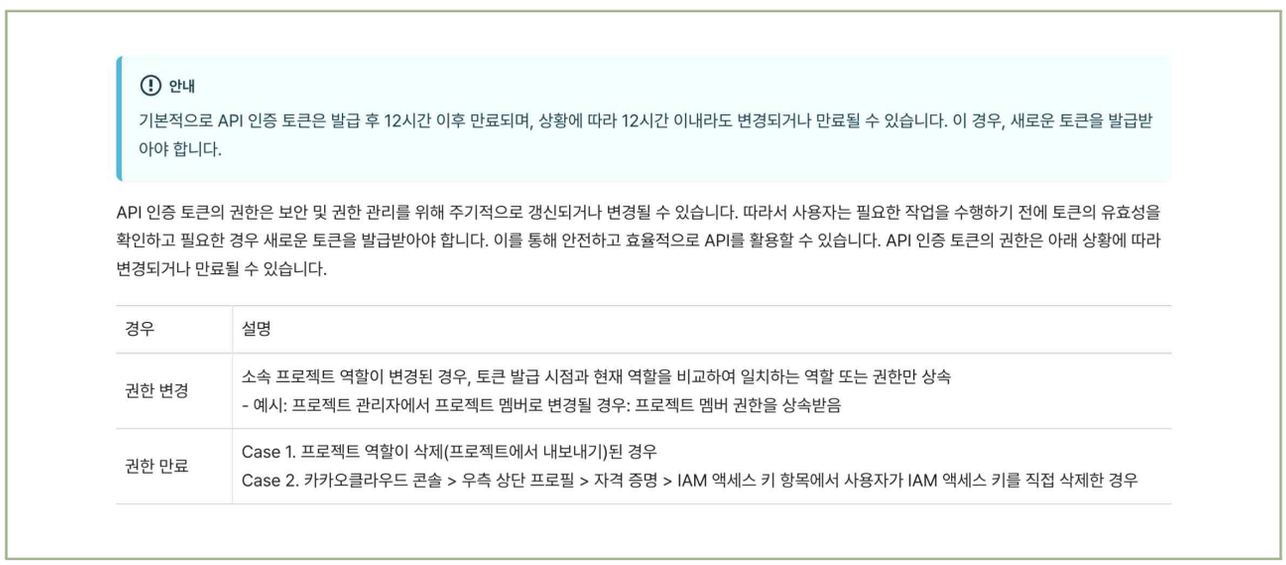
- API 세션 및 서명값에 대한 유효기간 설정하고, 유니크값(보안키 등) 유출 방지대책으로 만료기간을 적용하여야 한다.

  - 예시

    1) API 호출 세션의 유효기간 설정
    2) 서명의 유효기간 확인
    3) API 보안키 만료기간 설정
    4) 유니크값(보안키 등) 폐기 및 재발급 기능으로 만료기간 준수 등

3 우수 사례

- 기본적으로 API 인증 토큰은 12시간 이후 만료되며, 상황에 따라 12시간 이내라도 변경되거나 만료될 수 있습니다.



안내

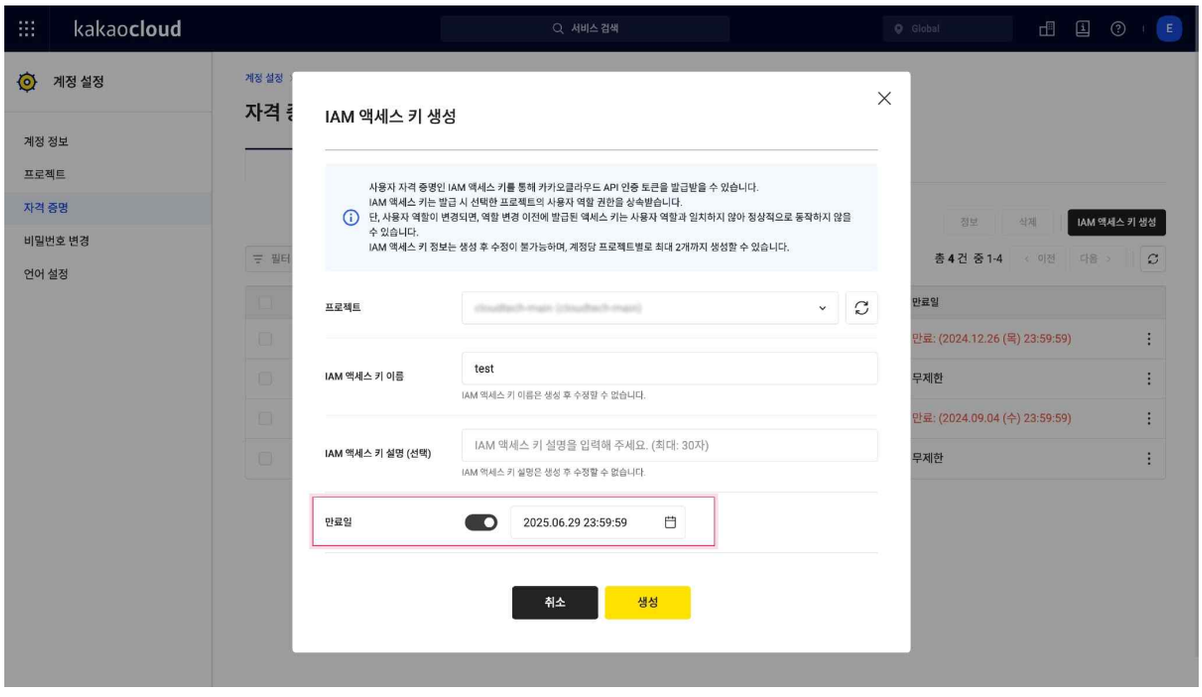
기본적으로 API 인증 토큰은 발급 후 12시간 이후 만료되며, 상황에 따라 12시간 이내라도 변경되거나 만료될 수 있습니다. 이 경우, 새로운 토큰을 발급받아야 합니다.

API 인증 토큰의 권한은 보안 및 권한 관리를 위해 주기적으로 갱신되거나 변경될 수 있습니다. 따라서 사용자는 필요한 작업을 수행하기 전에 토큰의 유효성을 확인하고 필요한 경우 새로운 토큰을 발급받아야 합니다. 이를 통해 안전하고 효율적으로 API를 활용할 수 있습니다. API 인증 토큰의 권한은 아래 상황에 따라 변경되거나 만료될 수 있습니다.

경우	설명
권한 변경	소속 프로젝트 역할이 변경된 경우, 토큰 발급 시점과 현재 역할을 비교하여 일치하는 역할 또는 권한만 상속 - 예시: 프로젝트 관리자에서 프로젝트 멤버로 변경될 경우: 프로젝트 멤버 권한을 상속받음
권한 만료	Case 1. 프로젝트 역할이 삭제(프로젝트에서 내보내기)된 경우 Case 2. 카카오클라우드 콘솔 > 우측 상단 프로필 > 자격 증명 > IAM 액세스 키 항목에서 사용자가 IAM 액세스 키를 직접 삭제한 경우

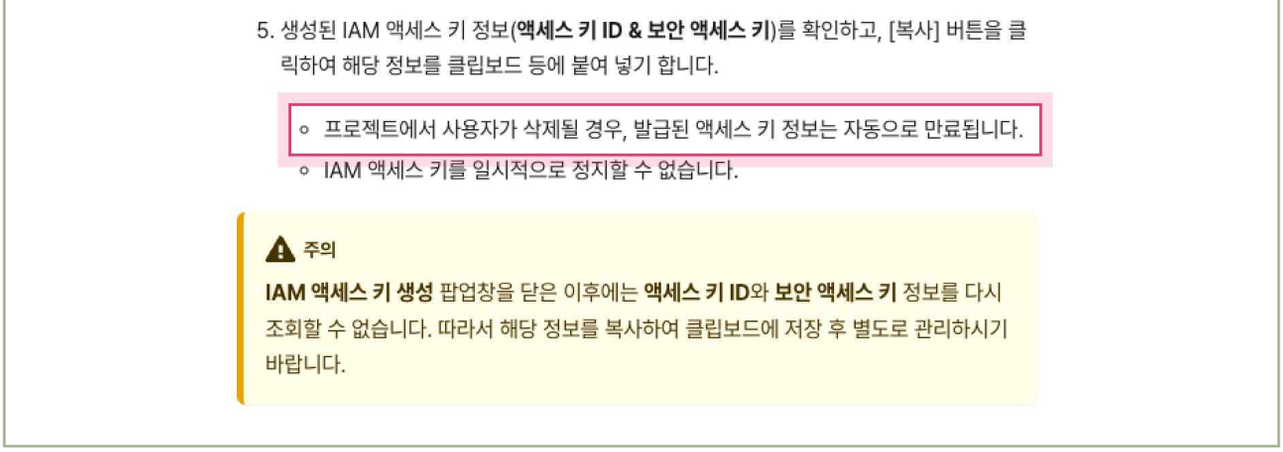
| 그림 6-4-1 | API 인증 토큰 만료 관련 내용

- 2. API 인증 토큰 발급을 위한 액세스 키 ID와 보안 액세스 키의 만료 기간을 설정할 수 있습니다.
  - **(Console)** 우측 상단 프로필 아이콘 〉 '자격 증명' 〉 IAM 액세스 키 생성 시 만료 기간 설정



| 그림 6-4-2 | IAM 액세스 키 생성 시, 만료일 설정

- 프로젝트에서 사용자가 삭제될 경우, 발급된 액세스 키 정보는 자동으로 만료됩니다.



5. 생성된 IAM 액세스 키 정보(**액세스 키 ID & 보안 액세스 키**)를 확인하고, [복사] 버튼을 클릭하여 해당 정보를 클립보드 등에 붙여 넣기 합니다.

- 프로젝트에서 사용자가 삭제될 경우, 발급된 액세스 키 정보는 자동으로 만료됩니다.
- IAM 액세스 키를 일시적으로 정지할 수 없습니다.

주의

IAM 액세스 키 생성 팝업창을 닫은 이후에는 **액세스 키 ID**와 **보안 액세스 키** 정보를 다시 조회할 수 없습니다. 따라서 해당 정보를 복사하여 클립보드에 저장 후 별도로 관리하시기 바랍니다.

| 그림 6-4-3 | 카카오클라우드 가이드 〉 자격증명 〉 IAM 액세스 키 발급

4 참고 사항

- 카카오클라우드 API 인증 토큰 발급 가이드
- 카카오클라우드 IAM 액세스 키 발급 가이드

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.

  - 예시

    1) SSL 적용 등

3 우수 사례

- API 서버와 클라이언트 간 통신을 HTTPS로만 허용하여 데이터가 암호화된 상태로 전송되도록 하며, TLS 1.3을 지원합니다.

API 인증 토큰 발급 URL

```
https://iam.kakaocloud.com/identity/v3/auth/tokens
```

| 그림 6-5-1 | API 인증 토큰 발급 URL

4 참고 사항

- 카카오클라우드 API 준비 가이드
- 카카오클라우드 Object Storage API 가이드
- 카카오클라우드 MemStore API 가이드
- 카카오클라우드 Hadoop Eco API 가이드
- 카카오클라우드 Data Query API 가이드
- 카카오클라우드 Pub/Sub API 가이드

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 접근 관리**	**스토리지 접근 시 적절한 통제방안을 적용하여야 한다.**

2 설명

- 스토리지 목적에 따라 외부 공개 차단 등 적절한 접근통제를 수행 하여야 한다.

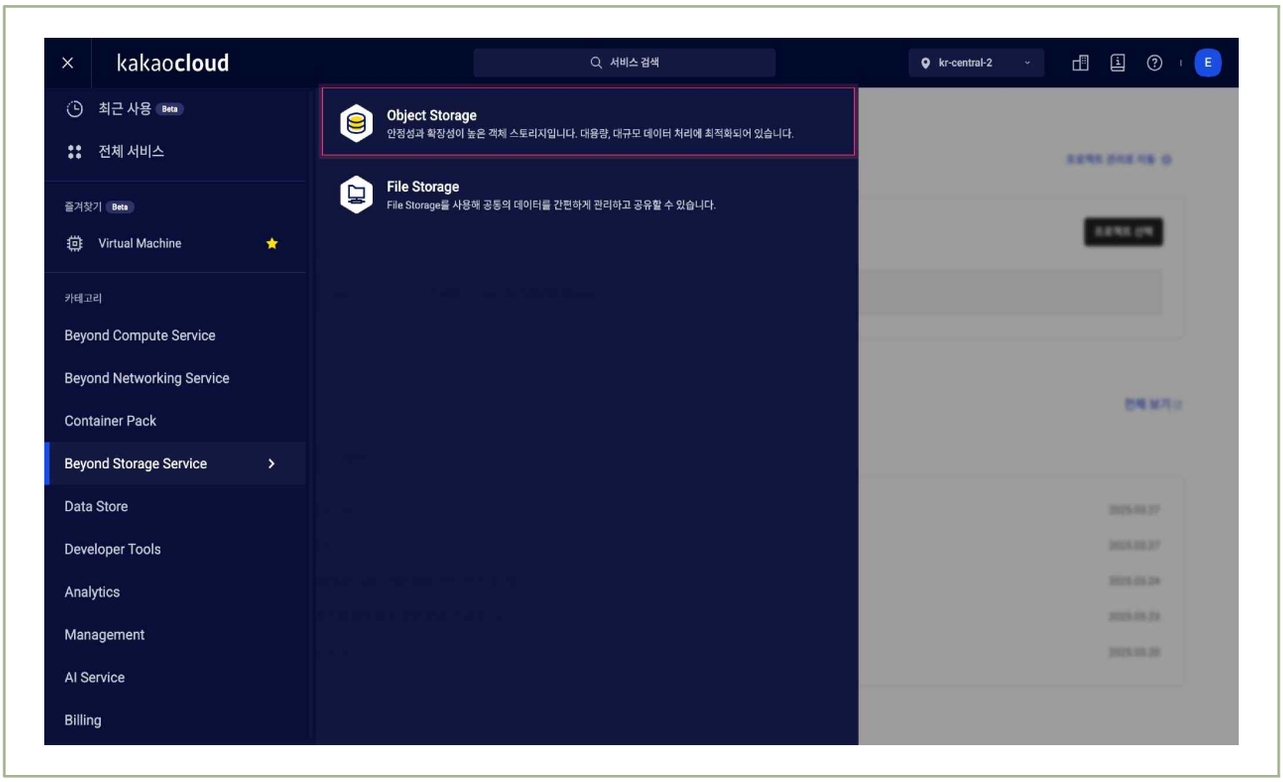
  - 예시

    1) 외부 공개가 불필요한 경우, 스토리지 퍼블릭 액세스 차단
    2) 스토리지에 접근 가능한 계정(IAM) 적용
    3) URL로 접근 시 접근 가능한 시간, 별도 IP 지정 등

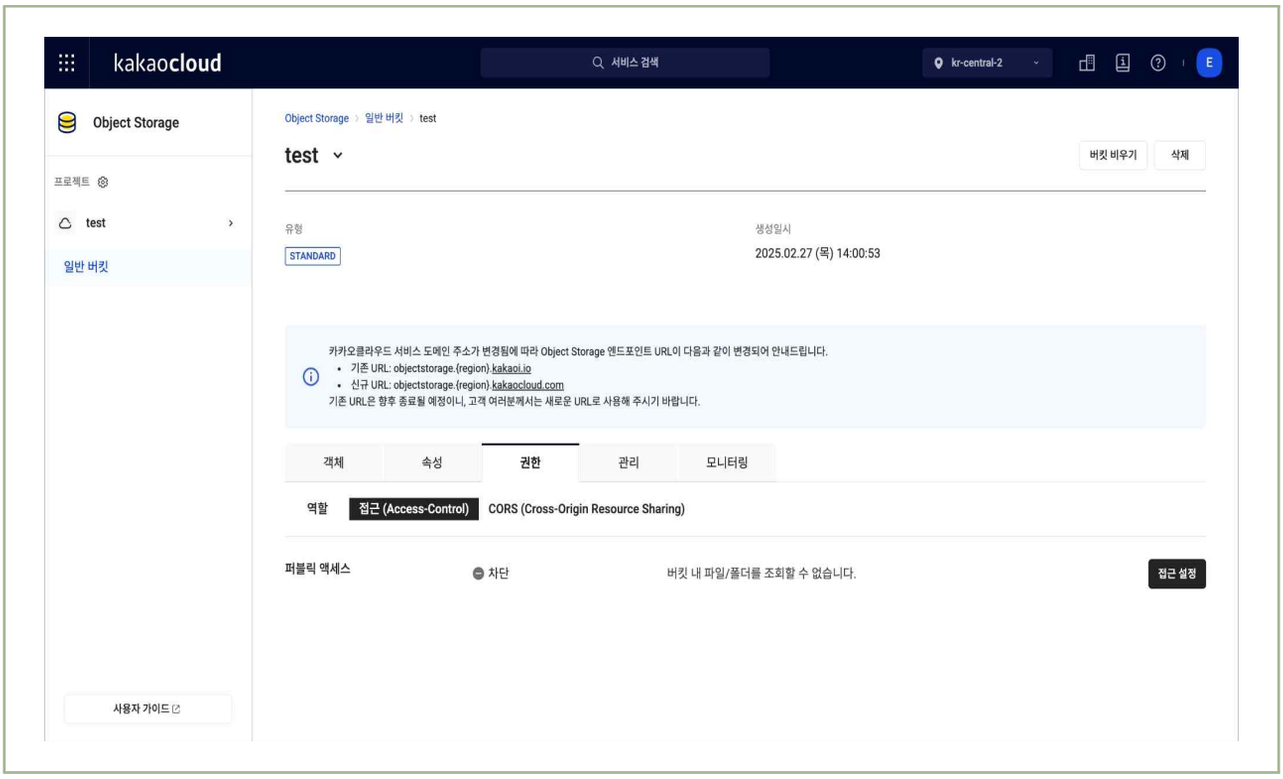
3 우수 사례

- 외부 공개가 불필요한 경우, 스토리지의 퍼블릭 액세스 차단이 가능합니다.

  - **(Console)** ‘Dashboard’ → ‘Beyond Storage Service’ → ‘Object Storage’ → 특정 버킷의 ‘권한’ 탭에서 퍼블릭 액세스 차단을 설정

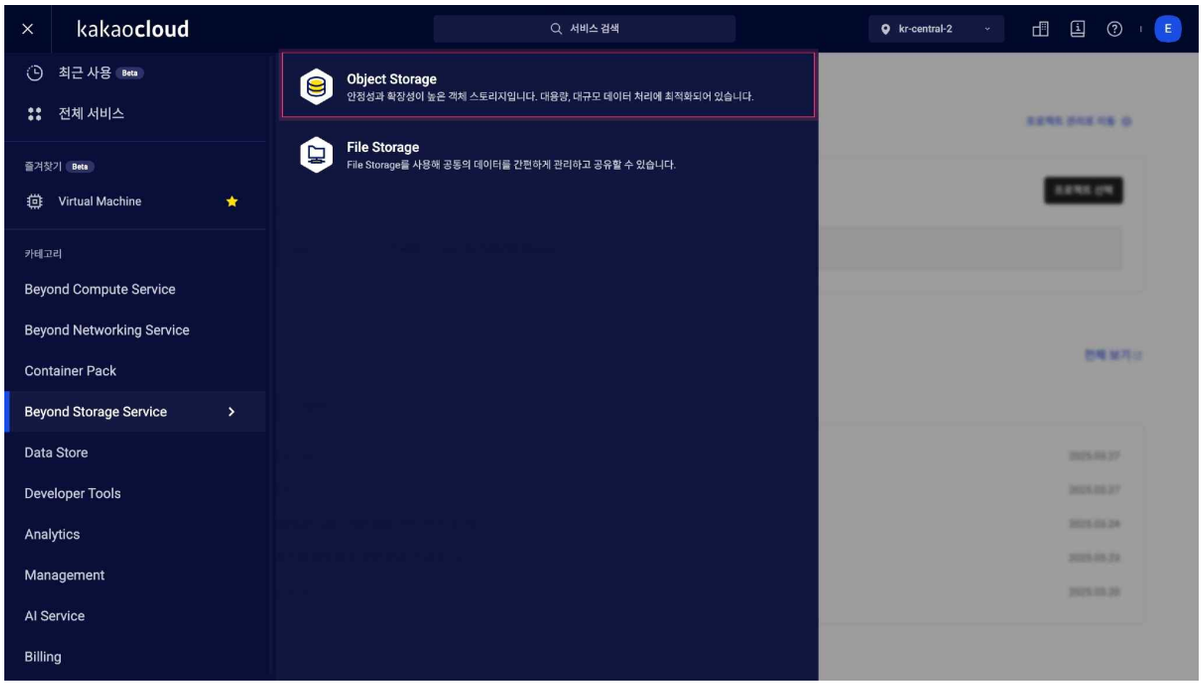


| 그림 7-1-1 | 카카오클라우드 콘솔 〉 Object Storage 서비스 이동

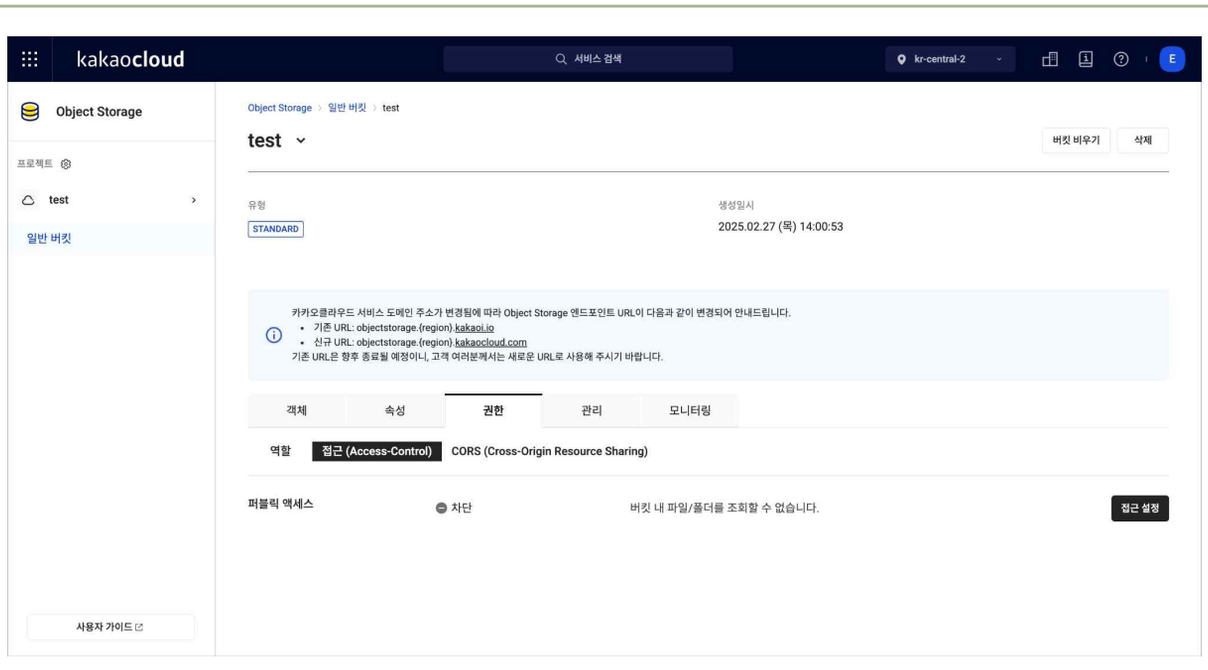


| 그림 7-1-2 | 특정 Bucket의 권한 탭에서 접근 설정 기능을 통해 퍼블릭 액세스 차단

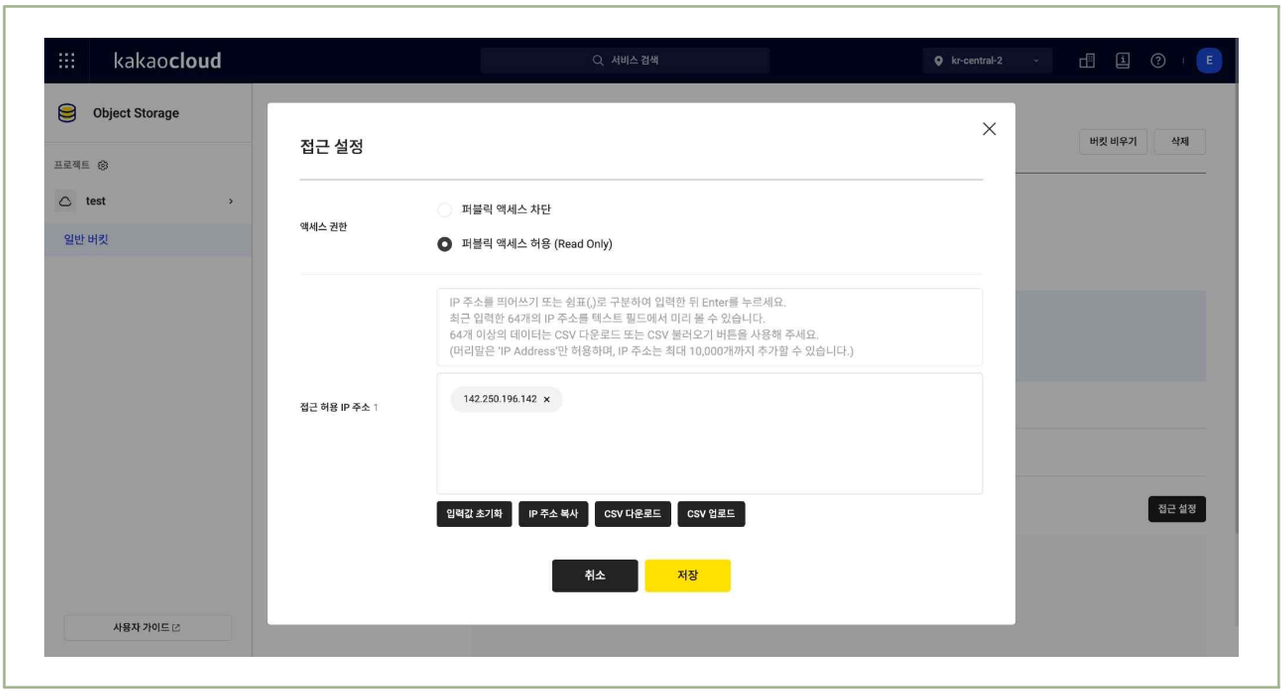
- 접근 허용 IP 주소를 지정하여 설정한 IP만 접근이 가능하도록 합니다.
  - **(Console)** ‘Dashboard’ → ‘Beyond Storage Service’ → ‘Object Storage’ → 특정 버킷의 ‘권한’ 탭에서 접근 설정을 통해 특정 접근 허용 IP 주소를 입력



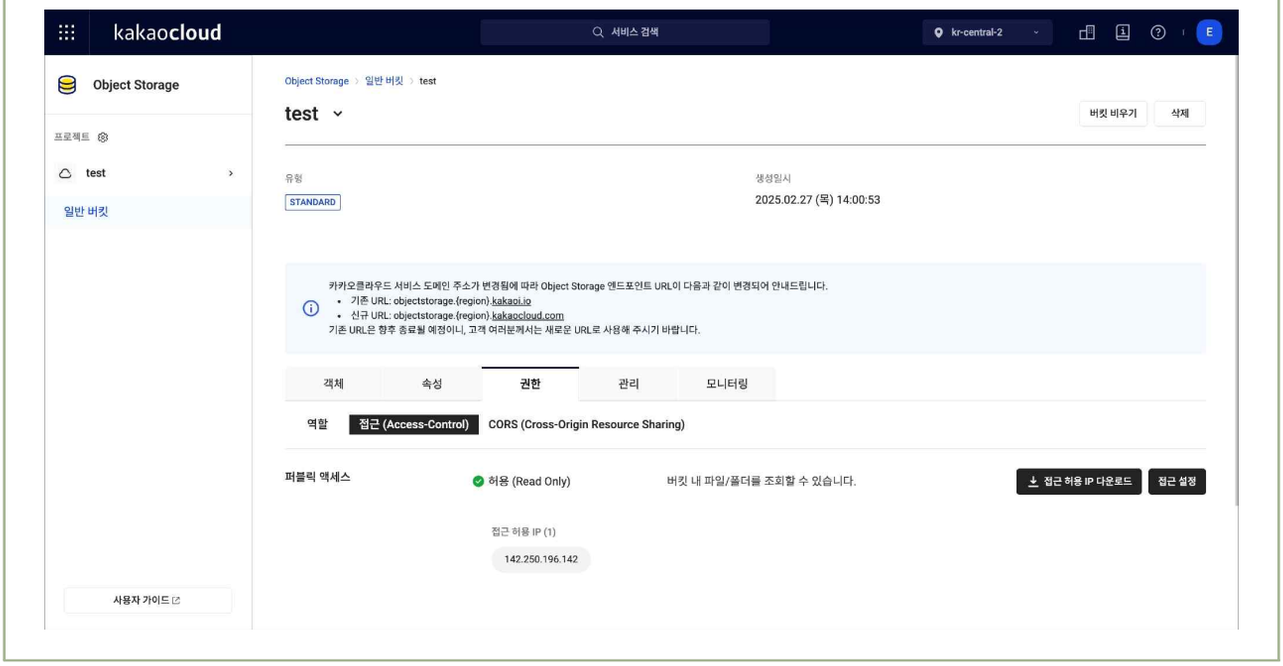
| 그림 7-1-3 | 카카오클라우드 콘솔 〉 Object Storage 서비스 이동



| 그림 7-1-4 | 버킷 상세 페이지 〉 권한 탭 〉 접근 설정 버튼

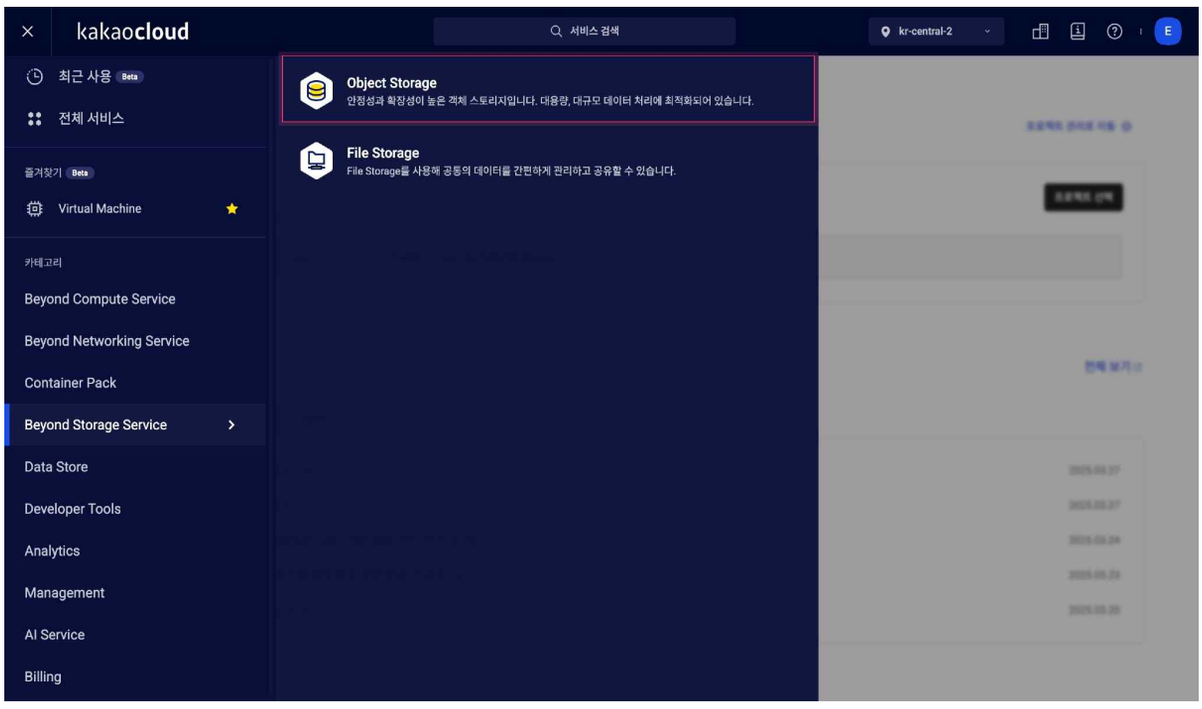


| 그림 7-1-5 | 퍼블릭 액세스 허용할 특정 IP만 입력

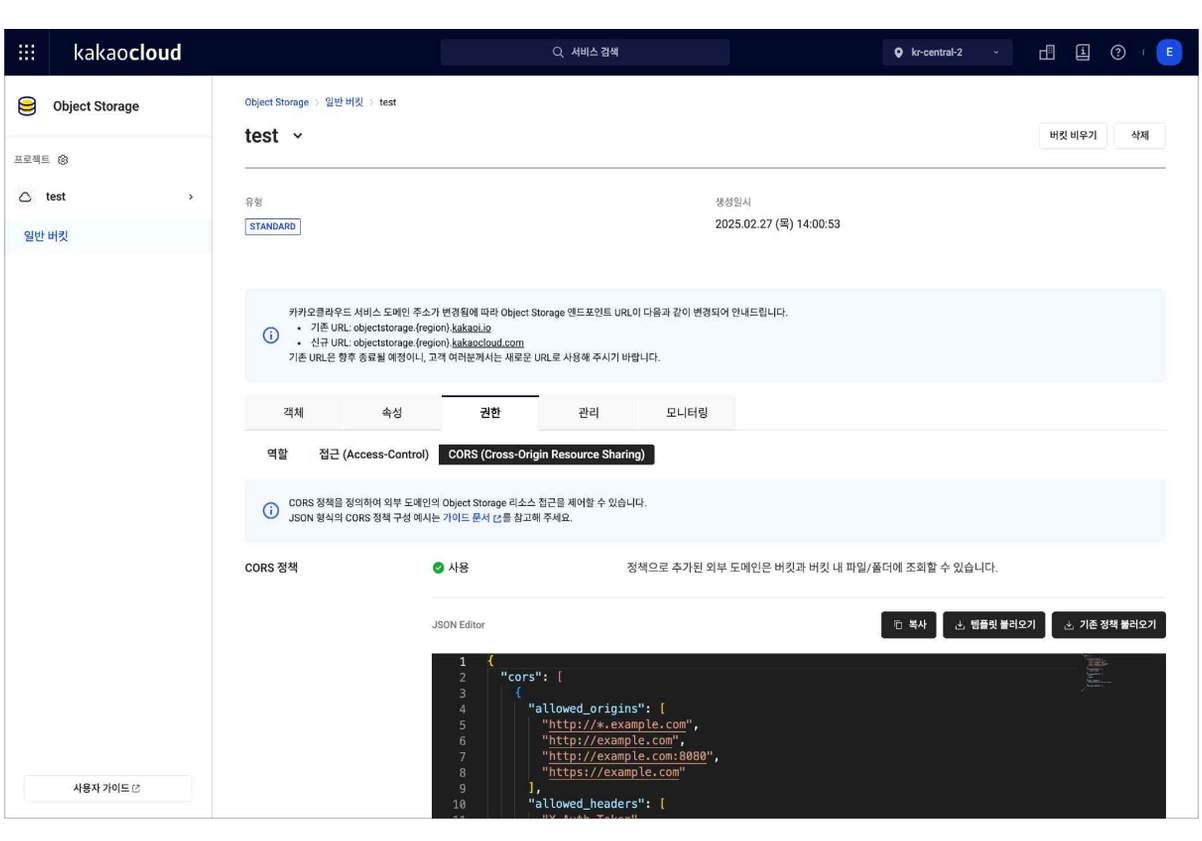


| 그림 7-1-6 | 특정 IP에 대해서만 퍼블릭 액세스 허용됨 확인

- 스토리지 CORS 정책 구성을 통해 특정 도메인에만 응답할 수 있도록 옵션 설정이 가능합니다.
  - **(Console)** 'Dashboard' → 'Beyond Storage Service' → 'Object Storage' → 특정 버킷의 '권한' 탭에서 CORS 정책을 구성하여 외부 도메인의 Object Storage 리소스 접근을 제어



| 그림 7-1-7 | 카카오클라우드 콘솔 〉 Object Storage 서비스 이동



| 그림 7-1-8 | 버킷 상세 페이지 〉 권한 탭 〉 CORS 탭에서 CORS 정책 적용

4 참고 사항

- 카카오클라우드 Object Storage 버킷 접근 설정 가이드
- 카카오클라우드 Object Storage 버킷 CORS 정책 가이드

1 기준

식별번호	기준	내용
7.2.	**스토리지 권한 관리**	**스토리지 목적에 따라 권한을 적용하고 관리를 하여야 한다.**

2 설명

- 스토리지 목적에 따라 읽기, 쓰기 등 권한을 세분화하여 적용하고 관리하여야 한다.
  - 예시
    1) 스토리지 객체 권한(읽기, 쓰기 등)을 목적에 따라 적용
    2) 스토리지 권한 부여 현황에 대해 주기적인 검토 수행 등

3 우수 사례

- 같은 프로젝트에 속한 구성원을 대상으로 스토리지 객체 접근 권한 및 역할을 개별적으로 부여할 수 있습니다.
  - 역할에 따라 버킷에 대한 임의의 동작(버킷 생성, 객체 조회, 권한 부여 등)이 제한

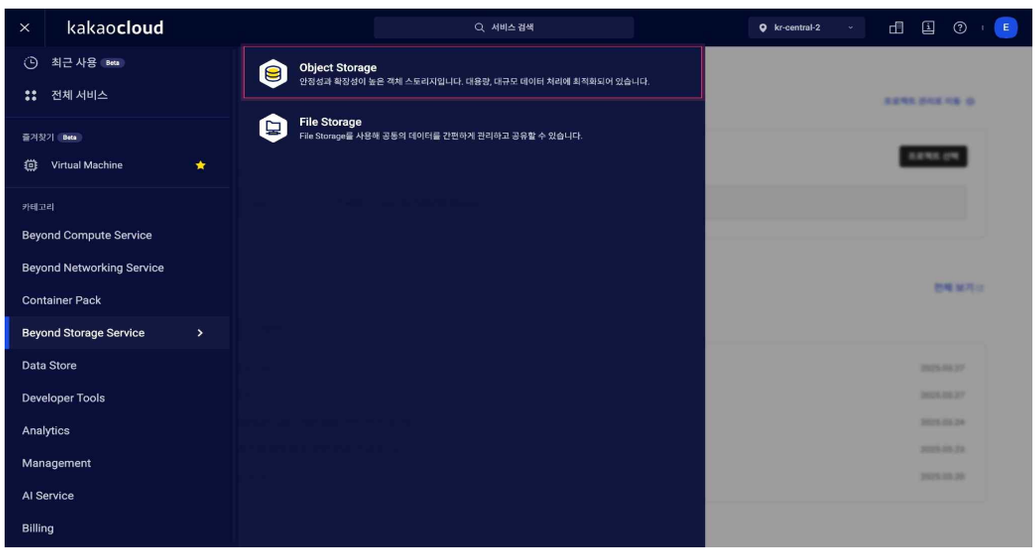
권한 범위	역할(Role)	권한(Permissions)	S3 Bucket ACL
버킷	스토리지 관리자 (storage.admin)	버킷과 객체를 관리할 수 있는 전체 권한을 부여 - storage.buckets.delete - storage.buckets.get - storage.buckets.update - storage.buckets.getIamPolicy - storage.buckets.setIamPolicy - storage.objects.create - storage.objects.delete - storage.objects.list - storage.objects.get - storage.objects.update	FULL_CONTROL
	스토리지 편집자 (storage.editor)	버킷의 권한 정책을 제외한 버킷과 객체를 관리할 수 있는 권한을 부여 - storage.buckets.get - storage.buckets.update - storage.objects.create - storage.objects.delete - storage.objects.list - storage.objects.get - storage.objects.update	READ + WRITE
	스토리지 뷰어 (storage.Viewer)	버킷의 메타데이터 정보와 객체 메타 데이터를 볼 수 있는 권한을 부여 - storage.buckets.get - storage.objects.list - storage.objects.get	READ

| 그림 7-2-1 | Object Storage 역할별 버킷 권한 내용 일부

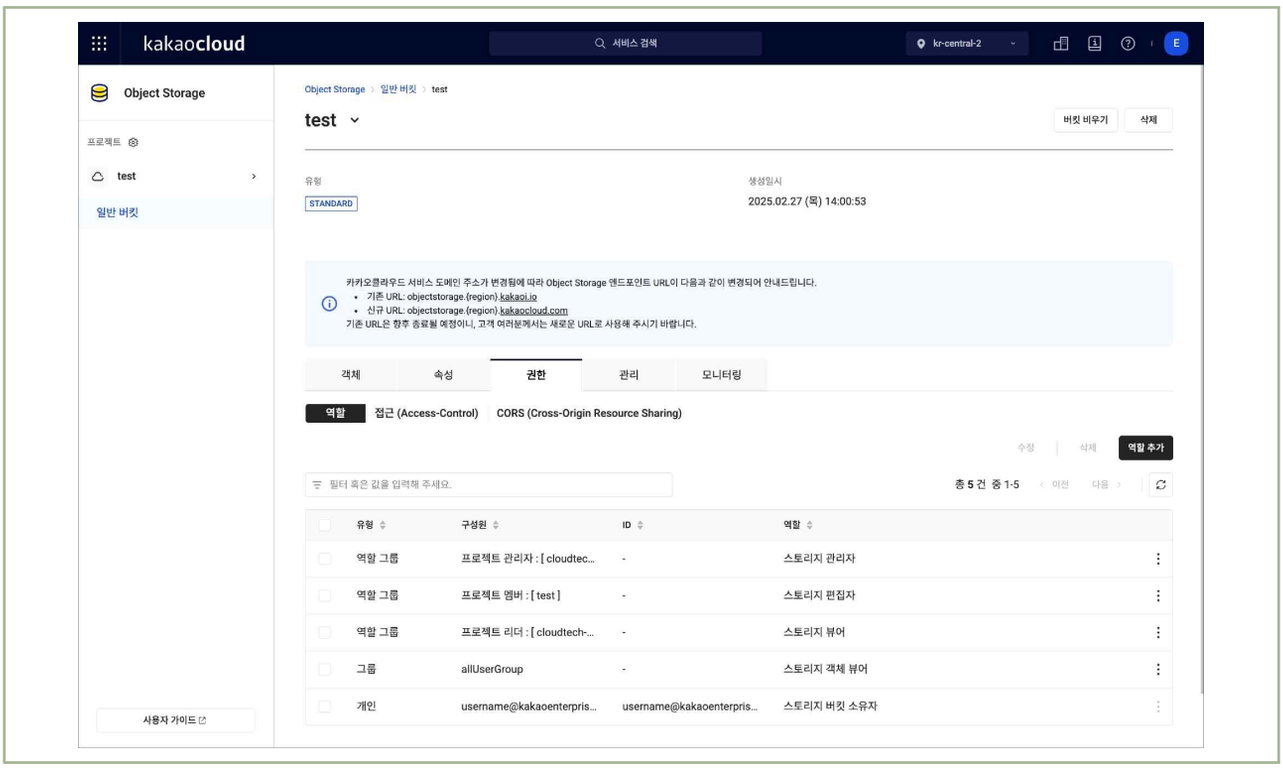
범위	권한(Permission)	기능
버킷	storage.buckets.create	버킷 생성하기
	storage.buckets.delete	버킷 삭제하기
	storage.buckets.list	버킷 목록 조회하기, 버킷의 메타 데이터 조회하기
	storage.buckets.get	버킷의 상세 정보, 메타 데이터 조회하기
	storage.buckets.update	버킷 수정하기 - 예시: 메타 데이터 수정
	storage.buckets.getIamPolicy	버킷 권한 정책 조회하기, Lifecycle 조회
	storage.buckets.setIamPolicy	버킷 권한 정책 등록, 수정, 삭제하기, Lifecycle 설정
객체	storage.objects.create	객체 등록하기 - 예시: 파일 업로드, 폴더 만들기
	storage.objects.delete	객체 삭제하기
	storage.objects.list	객체 조회하기 - 예시: 객체 목록 조회 및 객체의 메타 데이터 조회
	storage.objects.get	객체 상세 정보 조회하기 - 예시: 객체의 메타 데이터 조회, 객체 태그 조회, 파일 정보 조회, 파일 다운로드
	storage.objects.update	객체 수정하기 - 예시: 객체의 메타 데이터 추가/수정, 객체 태그 추가/삭제, 이름 바꾸기
	- storage.objects.create - storage.objects.delete - storage.objects.get	파일 이동하기
	- storage.objects.create - storage.objects.get	파일 복사하기

| 그림 7-2-2 | 버킷 또는 객체에 해당하는 권한별 기능

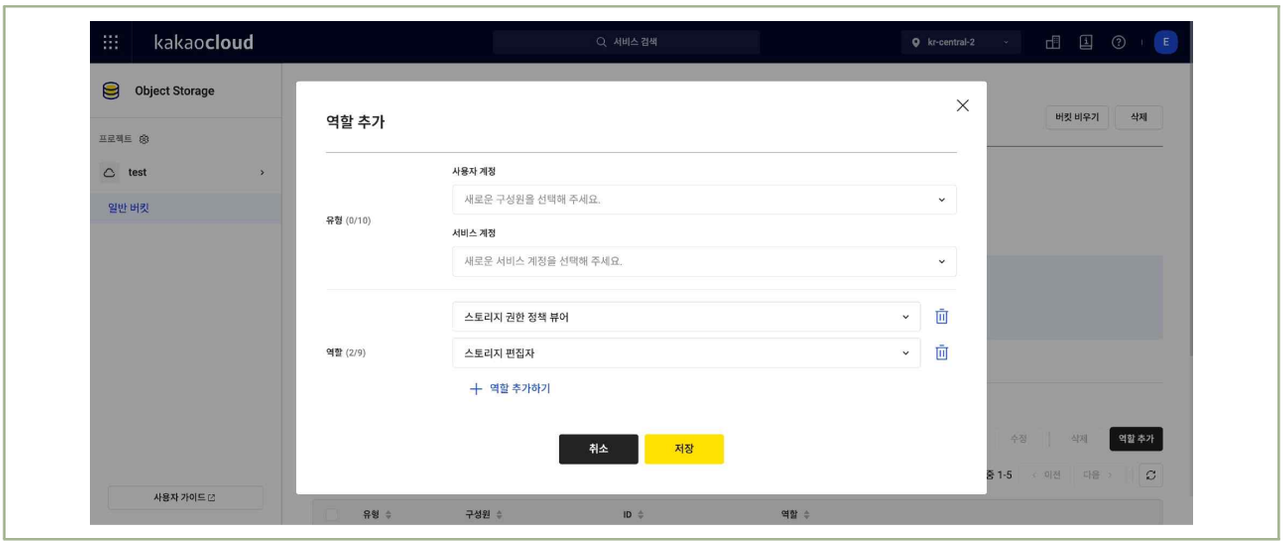
- **(Console)** ‘Dashboard’ → ‘Beyond Storage Service’ → ‘Object Storage’ → 특정 버킷의 ‘권한’ 탭에서 사용자 계정 혹은 서비스 계정에 역할 추가



| 그림 7-2-3 | 카카오클라우드 콘솔 〉 Object Storage 서비스 이동



| 그림 7-2-4 | 버킷 상세 페이지 〉 권한 탭 〉 역할 탭 〉 역할 추가 버튼



| 그림 7-2-5 | 사용자 계정 혹은 서비스 계정에 역할 추가

4 참고 사항

- 카카오클라우드 Object Storage 버킷 권한 관리 가이드
- 카카오클라우드 Object Storage 역할 및 권한 개념
- 카카오클라우드 IAM 프로젝트 역할 개념

1 기준

식별번호	기준	내용
7.3.	**스토리지 업로드 파일 제한**	**스토리지 목적에 맞는 안전한 파일만 업로드 될 수 있도록 보호대책을 마련하여야 한다.**

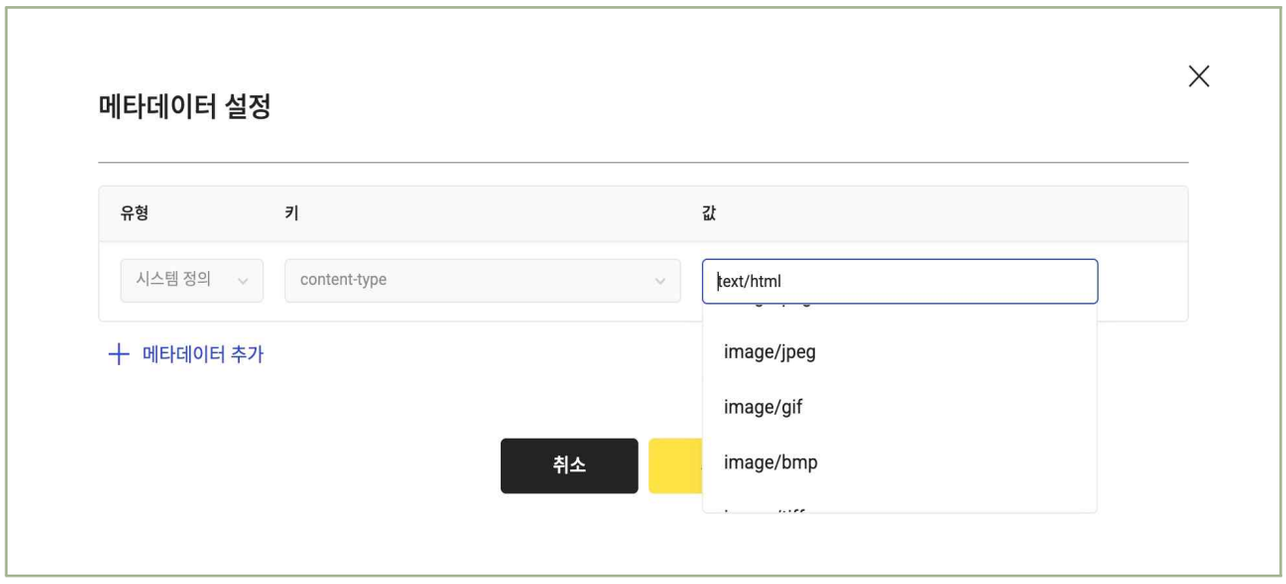
2 설명

- 스토리지 목적에 맞는 파일만 업로드 될 수 있도록 업로드 가능한 파일을 제한하여야 한다.
  - 예시
    1) 스토리지 버킷 정책 설정을 통한 업로드 파일 확장자 제한 등
    2) 금융회사에서 스토리지 내 파일 업로드 시 확장자 등을 검증할 수 있는 절차 마련

3 우수 사례

- 이용자는 카카오클라우드를 이용하여 서비스할 경유 유해한 콘텐츠가 스토리지에 업로드될 가능성을 최소화하려면 필요한 파일 유형만 업로드될 수 있도록 제한하여 구현하시기 바랍니다.
- 이용자가 스토리지 내 업로드된 파일에 대한 확장자 등은 아래 경로에서 확인 할 수 있으며, 메타데이터 설정을 통하여 파일에 대한 관리를 할 수 있습니다.
  - (Console) ‘Dashboard’ → ‘Beyond Storage Service’ → ‘Object Storage’ → ‘일반 버킷’ → ‘버킷 선택’ → ‘파일 메뉴 선택’ → ‘메타데이터 설정’

| 그림 7-3-1 | 파일 유형 및 크기 확인



| 그림 7-3-2 | 메타데이터 설정

4 참고 사항

- 카카오클라우드 Object Storage 파일/객체 관리 가이드

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 및 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 행위 추적성 증적(로그 등) 백업**	**클라우드 이용 내역을 추적할 수 있도록 관련 자료를 백업(1년이상 보관)하여야야 한다.**

2 설명

- 클라우드 이용 시 발생하는 로그에 대해 백업을 수행(1년이상 보관)하여야 한다.

  - 예시

    1) 스토리지 행위 감사로그 백업

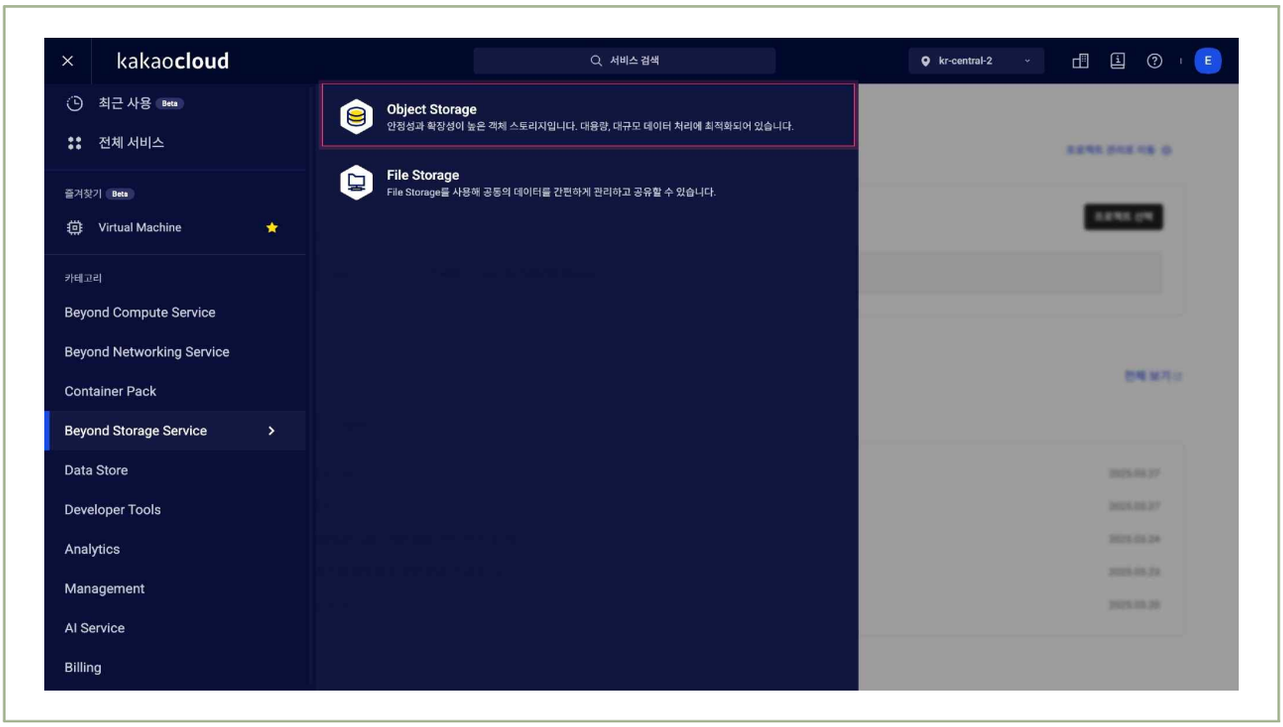
    2) 클라우드 웹 콘솔 감사로그 별도의 파일로 보관 등

       * 로그 : 가상자원, API, 스토리지 관리, 계정 및 권한관리 등

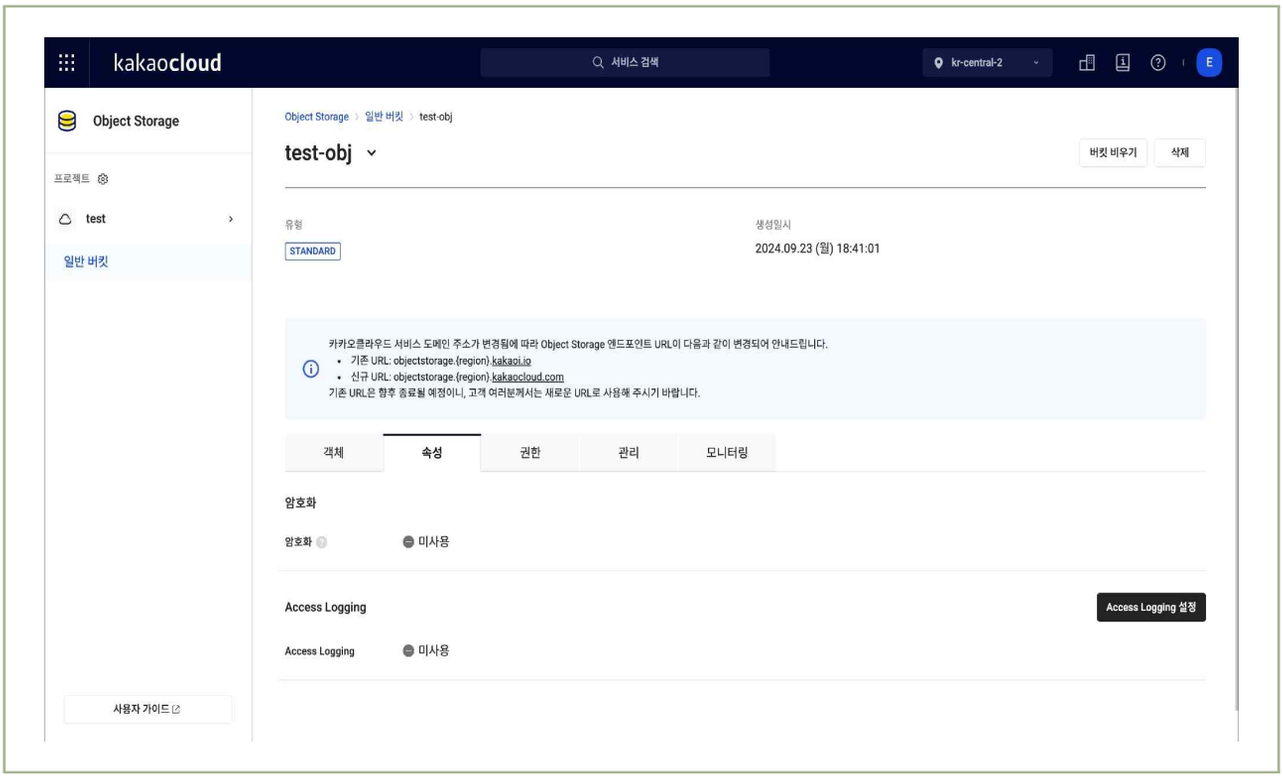
3 우수 사례

- Object Storage의 Access Logging을 통해 버킷에서 수행된 요청을 기록하여 보안 감사 및 액세스 분석에 활용 가능합니다.

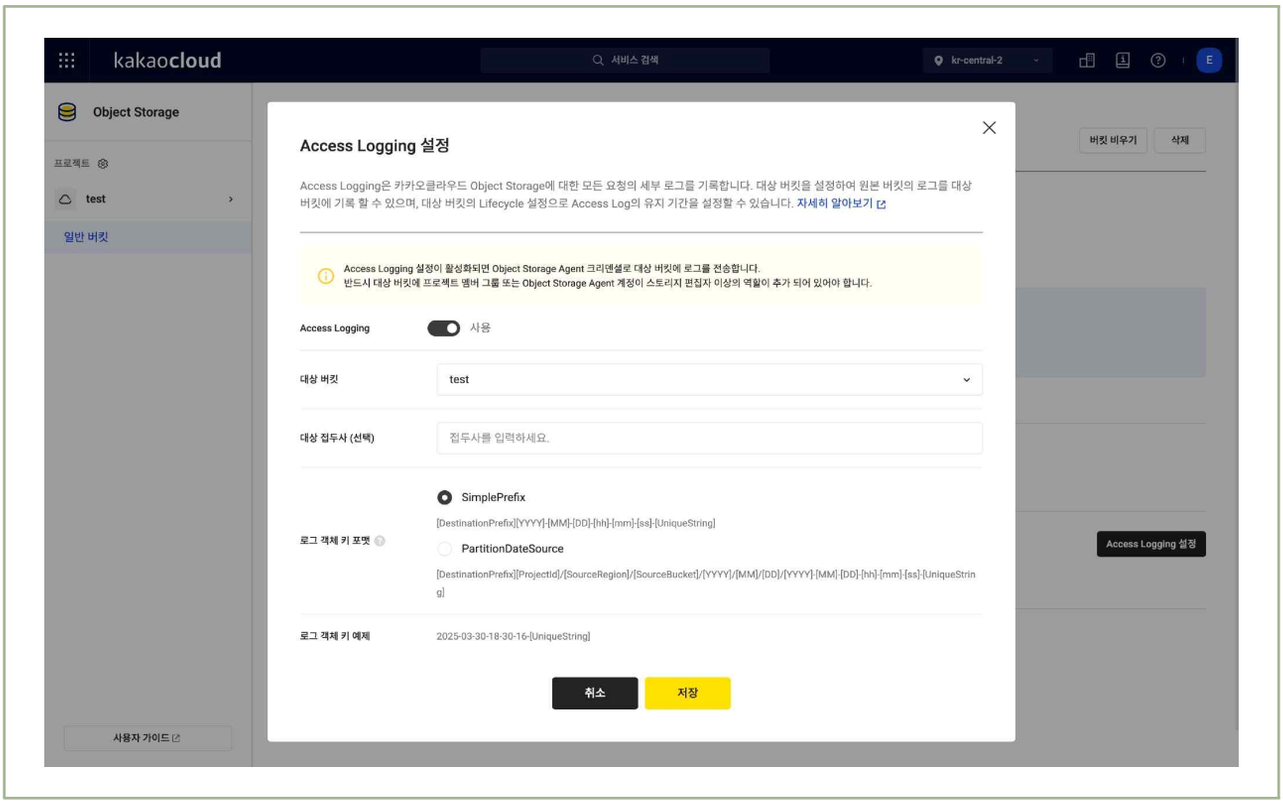
  - **(Console)** 'Dashboard' → 'Beyond Storage Service' → 'Object Storage' → 특정 버킷에서 Access Logging 설정



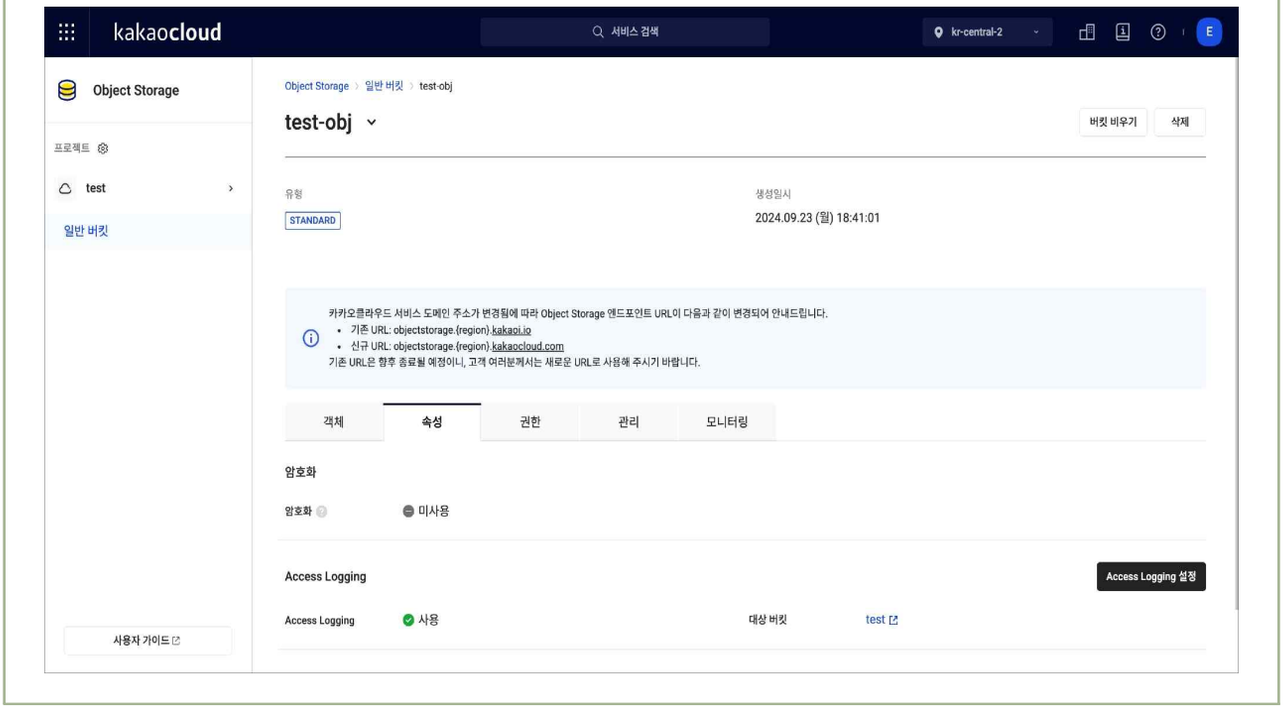
| 그림 8-1-1 | 카카오클라우드 콘솔 〉 Object Storage 서비스 이동



| 그림 8-1-2 | 버킷 상세 페이지 〉 속성 탭 〉 Access Logging 설정 버튼

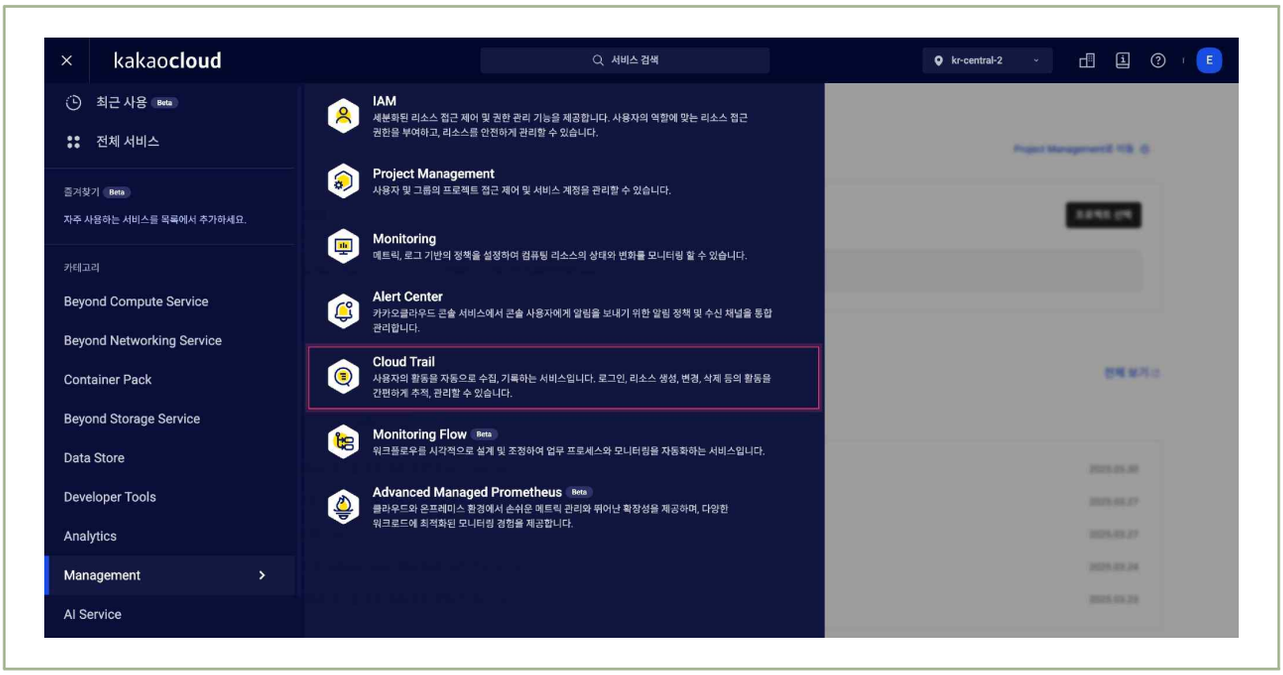


| 그림 8-1-3 | Access Logging 설정 모달

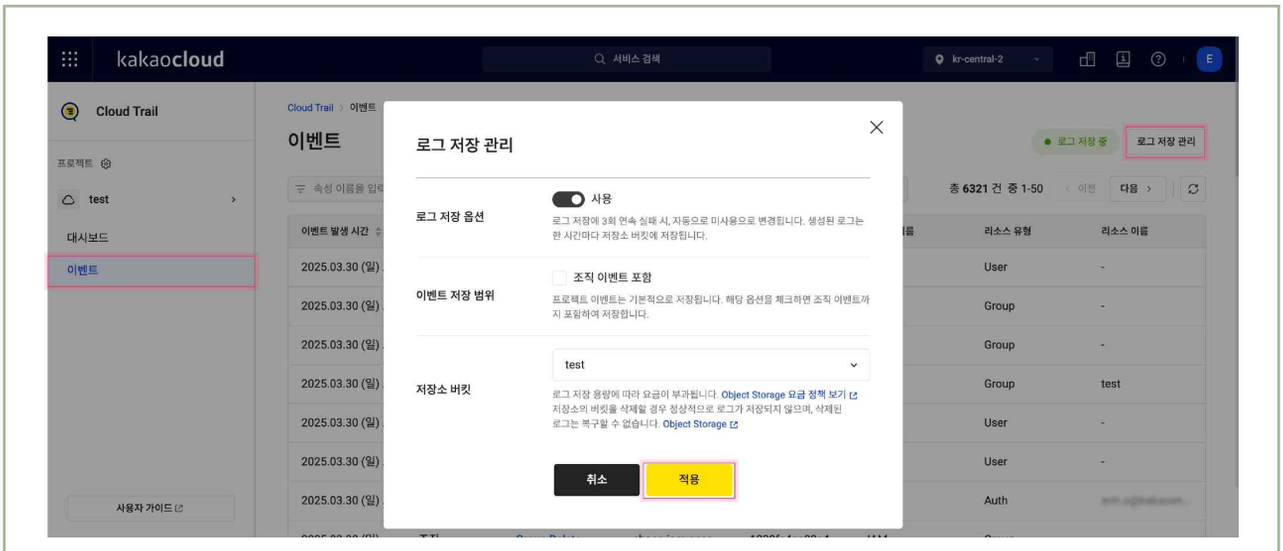


| 그림 8-1-4 | Access Logging 설정됨 확인

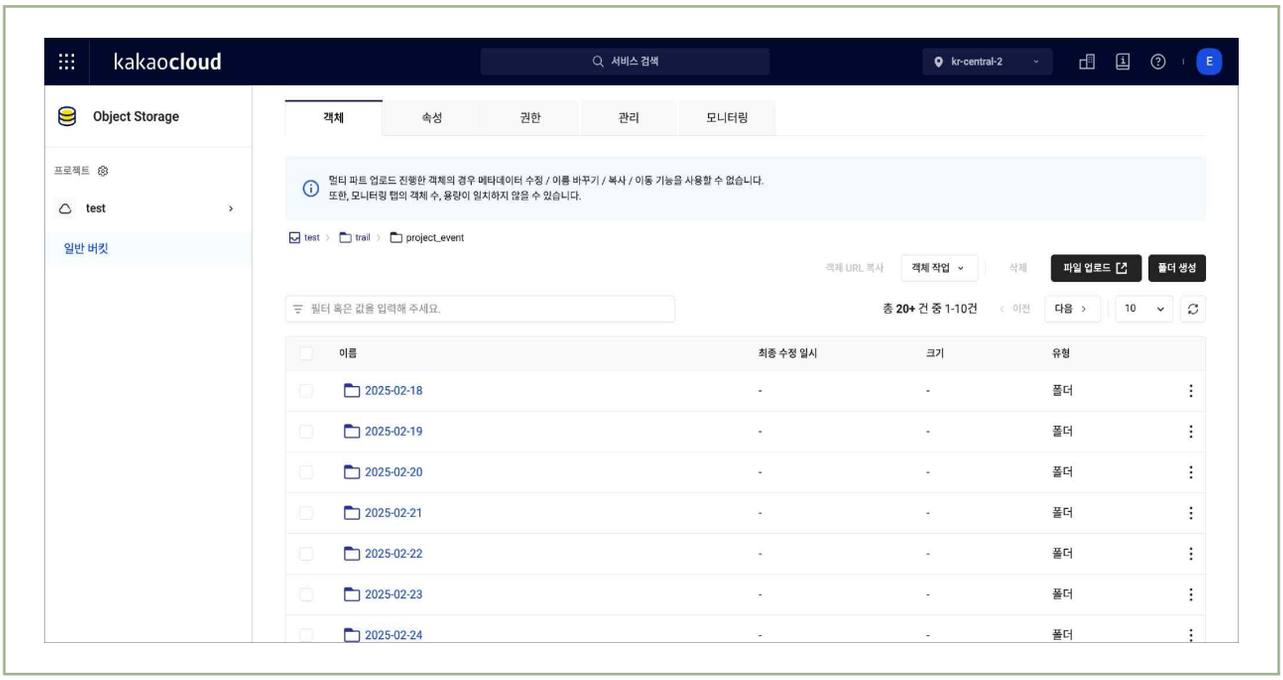
- Cloud Trail에 저장된 이벤트를 로그 저장 관리 기능을 통해 Object Storage에 장기간 저장이 가능합니다.
  - 해당 로그를 저장하는 Object Storage에 Lifecycle 정책 적용 가능: 일정 기간동안 버킷 내 로그 파일 저장 (최소 1일부터 최대 18,250일(50년)까지)
  - **(Console)** 'Dashboard' → 'Management' → 'Cloud Trail' → 이벤트 탭에서 로그 저장 기능 활성화



| 그림 8-1-5 | 카카오클라우드 콘솔 〉 Cloud Trail 서비스 이동

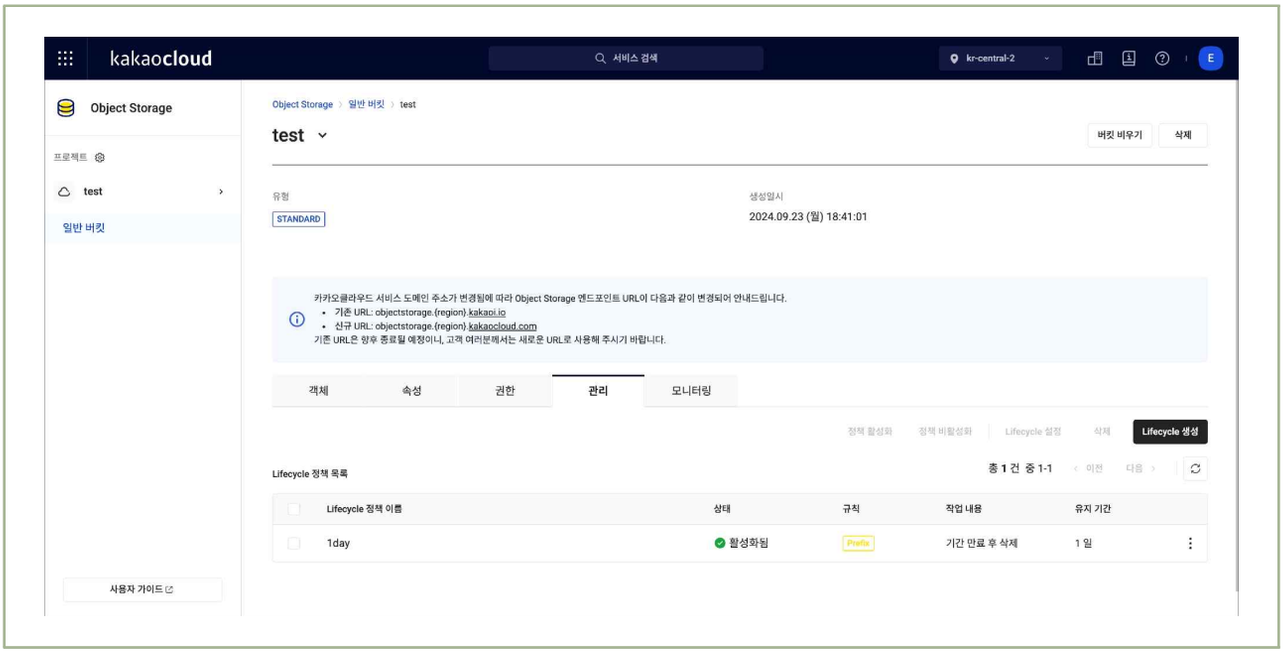


| 그림 8-1-6 | 이벤트 탭 〉 로그 저장 관리 버튼 〉 로그 저장할 버킷 선택

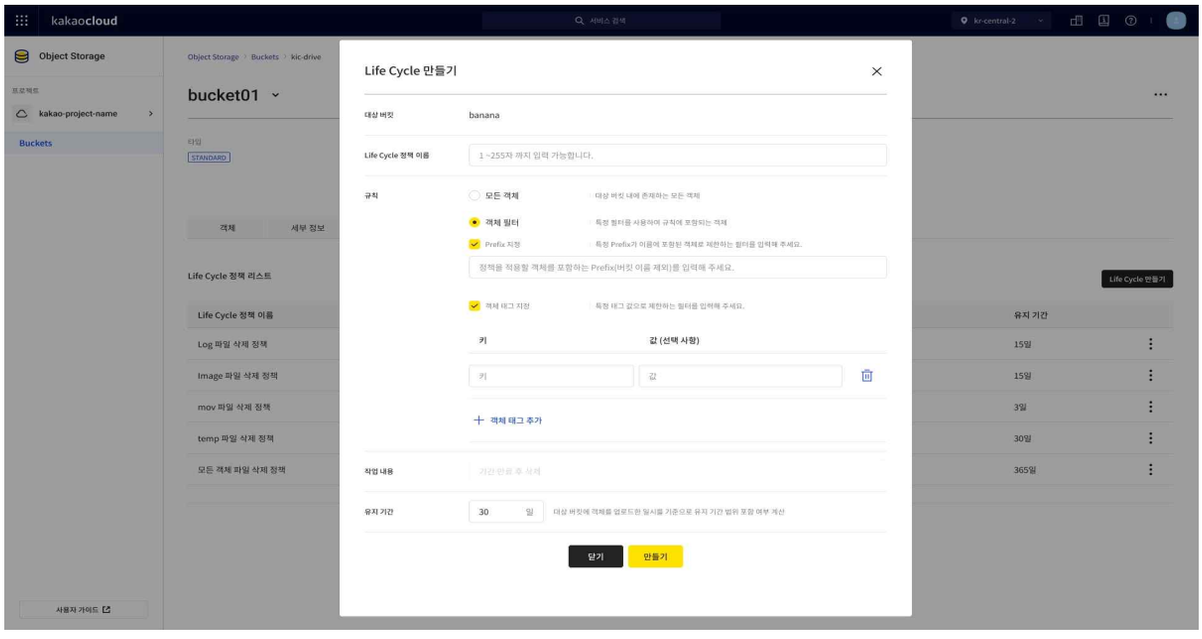


| 그림 8-1-7 | Object Storage 버킷에 쌓인 Cloud Trail 이벤트 목록

- **(Console)** Cloud Trail 로그를 저장한 Object Storage 버킷 내 Lifecycle 생성



| 그림 8-1-8 | Object Storage 버킷 내 Lifecycle 설정 화면



| 그림 8-1-9 | Lifecycle 설정 모달

4 참고 사항

- 카카오클라우드 Object Storage 버킷 Access Logging 가이드
- 카카오클라우드 Cloud Trail의 조회 가능한 이벤트 목록
- 카카오클라우드 Cloud Trail 로그 저장 관리 가이드
- 카카오클라우드 Object Storage 버킷 Lifecycle 설정 가이드

1 기준

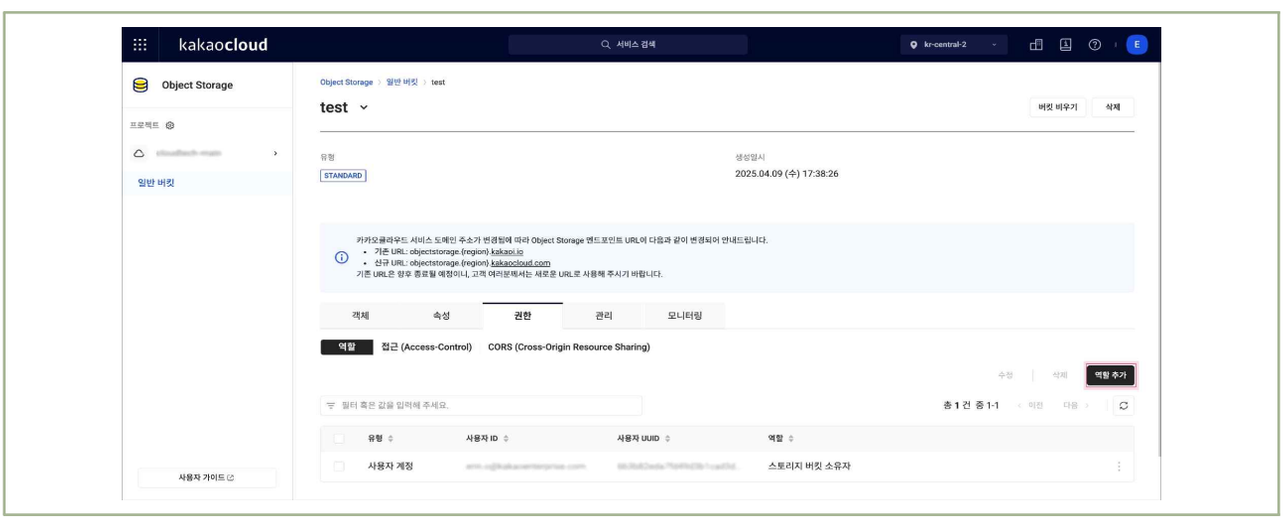
식별번호	기준	내용
8.2.	**행위추적성 증적(로그 등) 백업 파일 무결성 검증**	**백업을 통해 보관되고 있는 행위추적성 파일에 대한 무결성이 보장되어야 한다.**

2 설명

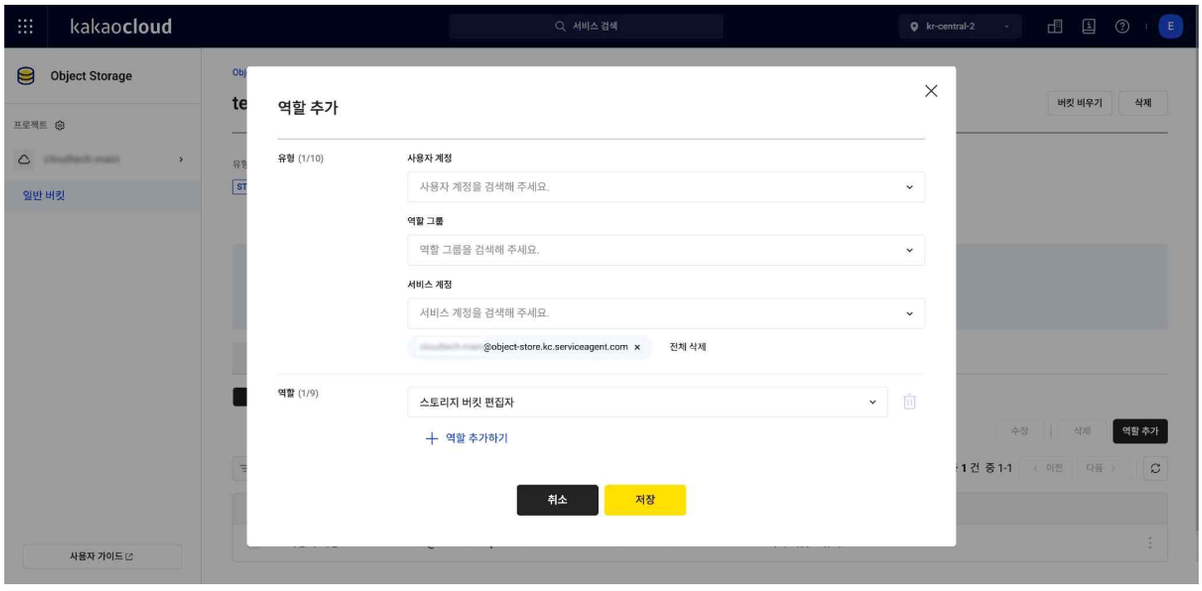
- 이용자의 행위추적성 백업 증적(로그 등)은 무결하게 보관하여야 한다.
  - 예시
    1) 감사로그 훼손 탐지에 대한 알람 설정
    2) 별도 스토리지 백업 기능(객체 잠금 등)을 통해 로그 무결성 보장 등

3 우수 사례

- Object Storage 버킷에서 수행된 요청을 Access Log를 통해 분석한다면, Access Log가 저장되는 버킷의 권한을 조정하여 무결성을 보장할 수 있습니다.
  - Object Storage Agent 계정과 스토리지 버킷 소유자를 제외한 사용자들은 버킷의 접근 및 사용을 차단
  - **(Console)** Access Log를 기록하는 Object Storage Agent 계정만 스토리지 편집자 이상의 역할로 추가 (project-name@object-store.kc.serviceagent.com)



| 그림 8-2-1 | Access Log 저장 버킷 상세 페이지 〉 권한 탭 〉 역할 추가



| 그림 8-2-2 | Object Storage 서비스 에이전트 계정 역할 추가

- 카카오클라우드 Object Storage는 자체 무결성 검증 과정이 있기 때문에 무단 변경이 불가능합니다.

4 참고 사항

- 카카오클라우드 서비스 계정 개념
- 카카오클라우드 Object Storage Access Logging 가이드

1 기준

식별번호	기준	내용
8.3.	금융회사 전산자료 백업	금융회사 중요 전산자료에 대해 백업을 수행하여야 한다.

2 설명

- 관련 법령(전자금융감독규정 등)에 따라 백업이 필요한 금융회사 전산자료는 별도 보관 및 관리하여야 한다.

  * 금융회사 중요 업무인 경우, 가상 시스템 이미지 및 설정 파일도 백업 대상에 포함(중요도에 따라 1년 이상 보관)

  - 예시

    1) 클라우드 서비스 제공자(CSP)의 백업 서비스 이용

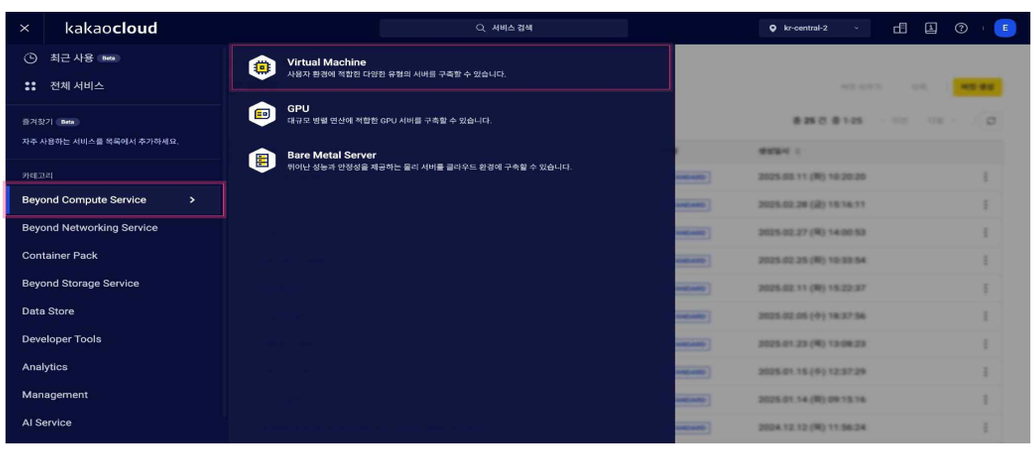
    2) 전산자료를 별도로 다운받아 금융회사가 관리하는 백업 서버내 보관 등

3 우수 사례

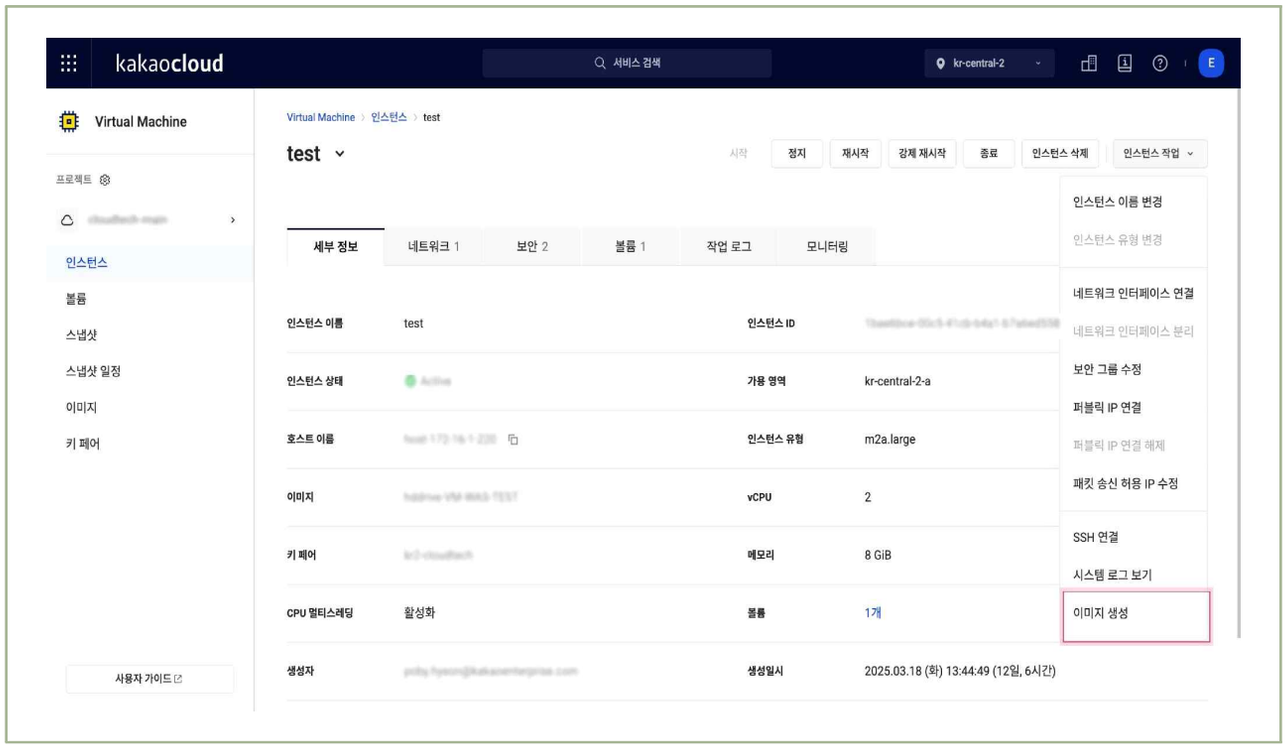
- 전산자료가 보관된 백업서버의 이미지를 생성하여 관리합니다. (백업서버의 루트 볼륨에 저장되었을 경우)

  - **(Console)** ‘Dashboard’ → ‘Beyond Compute Service’ → ‘Virtual Machine’ → 특정 서버의 이미지 생성 가능

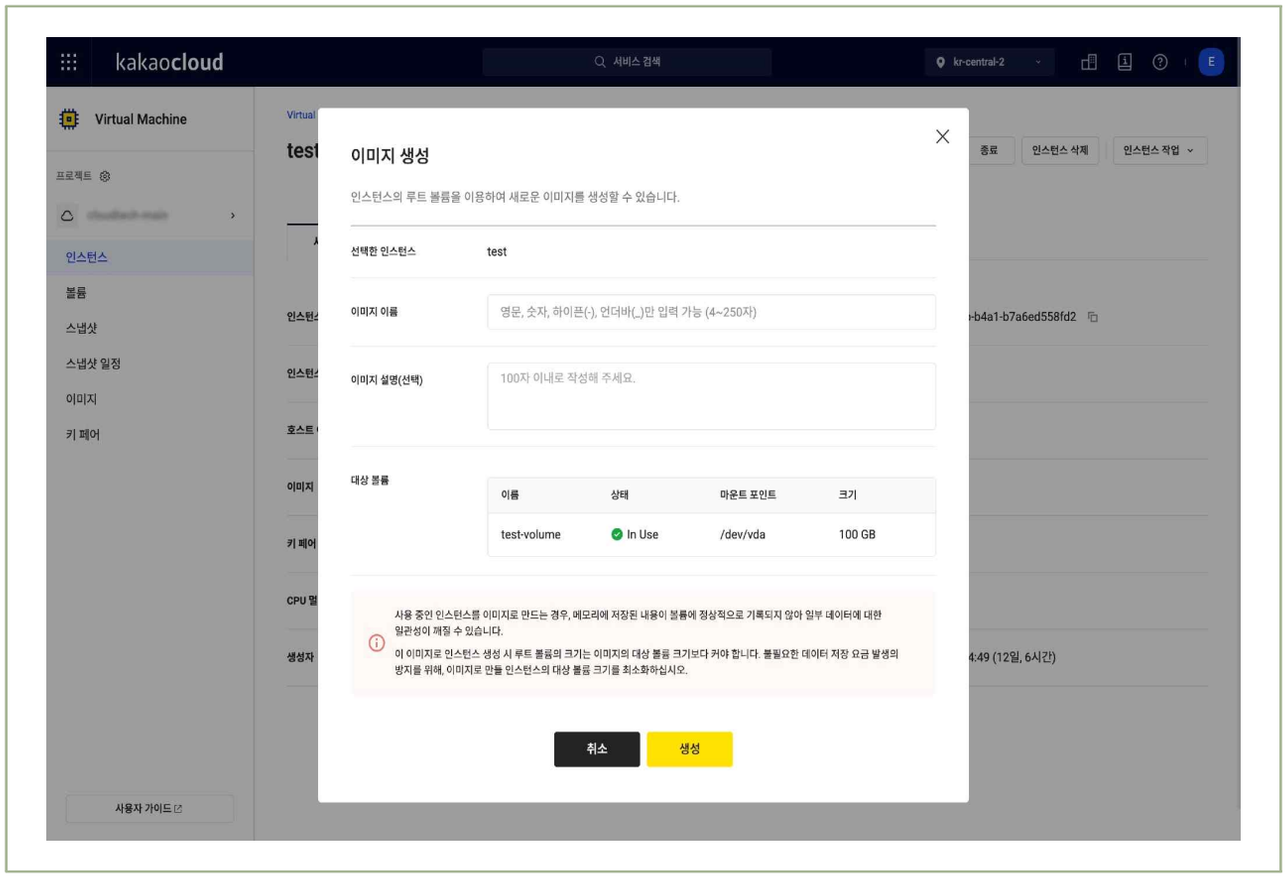
  - **(Console)** ‘Dashboard’ → ‘Beyond Compute Service’ → ‘Image’에서 생성된 이미지 확인 및 이미지를 통해 인스턴스 생성 가능



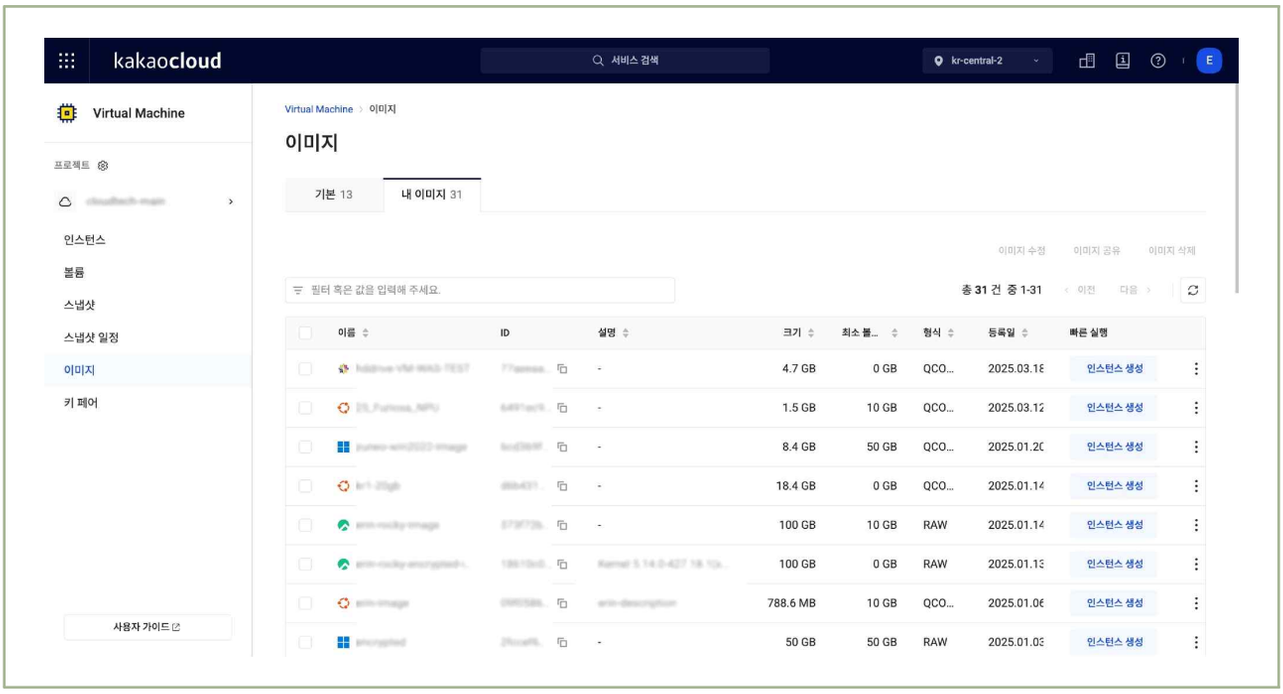
| 그림 8-3-1 | 카카오클라우드 콘솔 〉 ‘Virtual Machine’ 서비스 이동



| 그림 8-3-2 | 인스턴스 탭 〉 인스턴스 상세 페이지 〉 인스턴스 작업 버튼 〉 이미지 생성 버튼

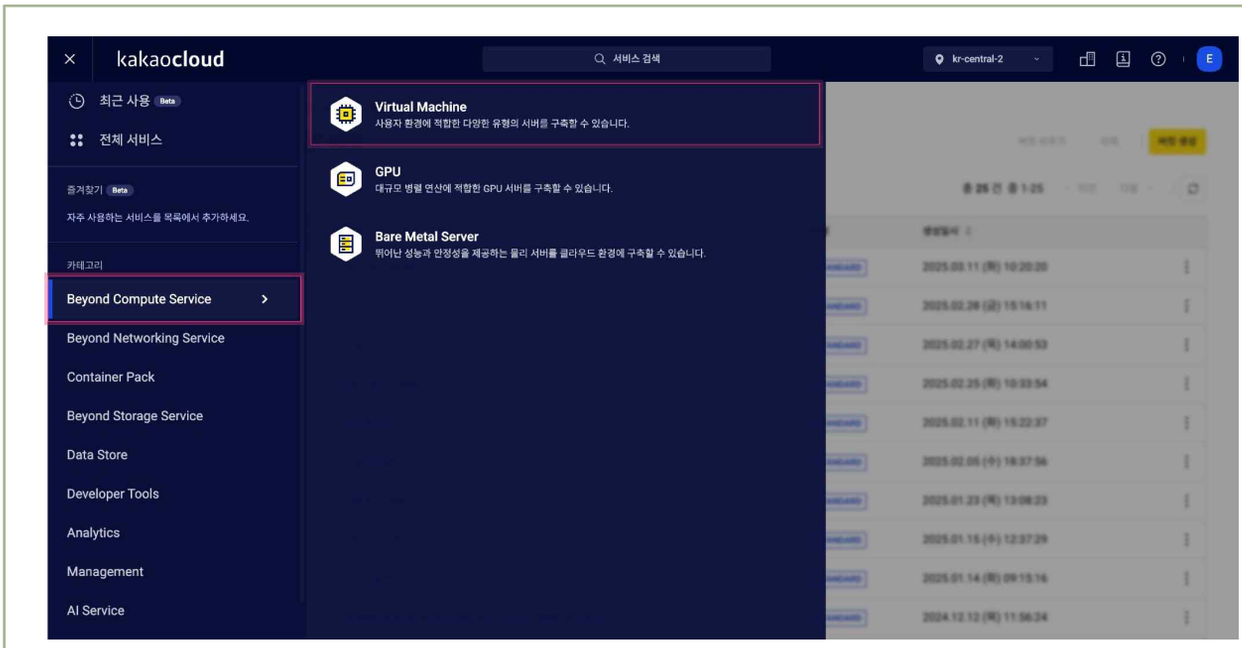


| 그림 8-3-3 | 루트 볼륨을 대상으로 하는 이미지 생성 모달

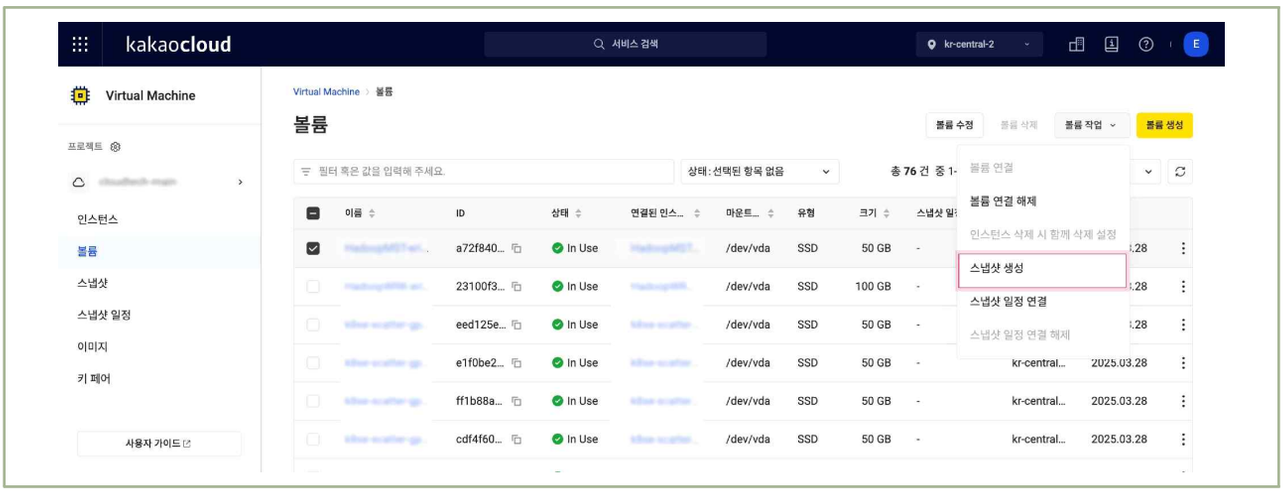


| 그림 8-3-4 | 이미지 탭 〉 내 이미지 탭 〉 생성된 이미지 확인 및 이미지 기반의 인스턴스 생성 가능

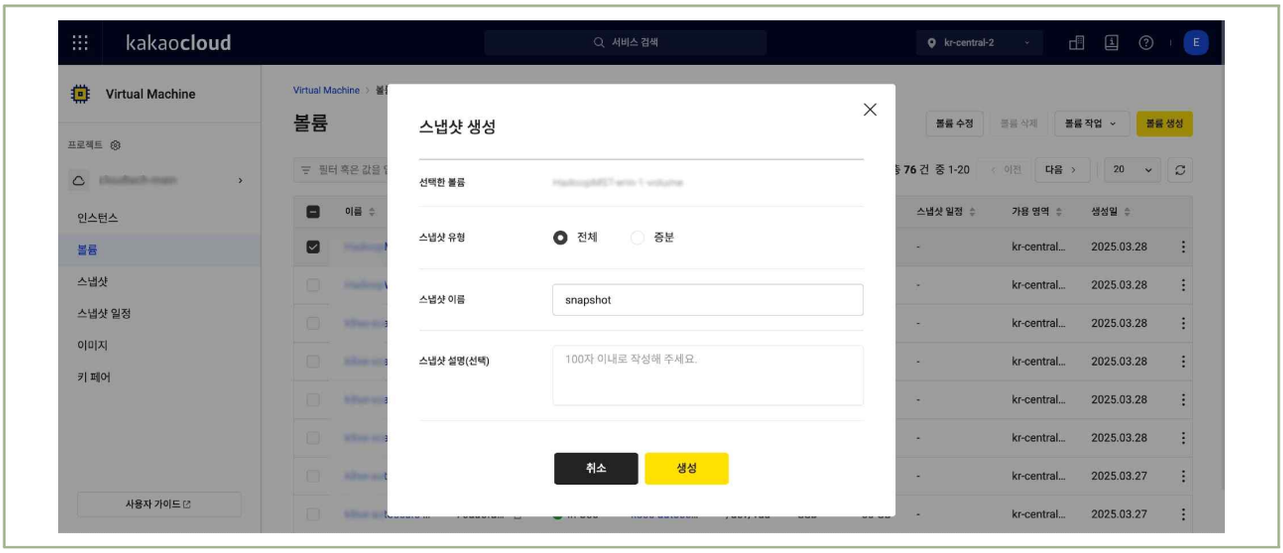
- 전산자료가 보관된 백업서버의 볼륨에 대한 스냅샷을 생성하여 관리합니다. (백업 서버의 추가 볼륨에 저장되었을 경우)
  - **(Console)** 'Dashboard' → 'Management' → 'Cloud Trail' → 이벤트 탭에서 로그 저장 기능 활성화



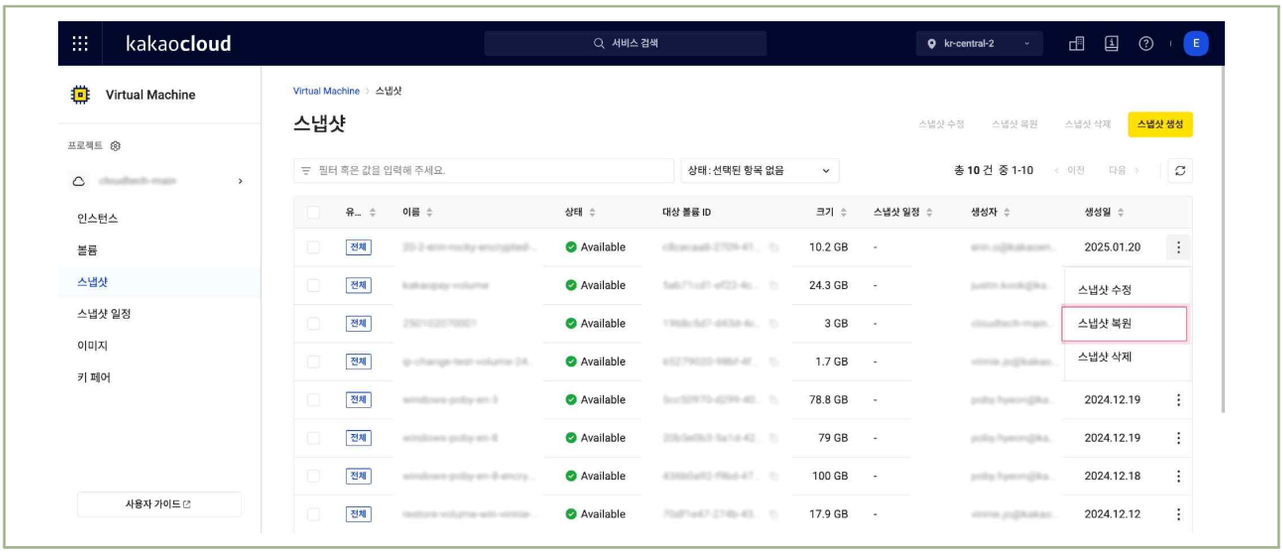
| 그림 8-3-5 | 카카오클라우드 콘솔 〉 'Virtual Machine' 서비스 이동



| 그림 8-3-6 | 볼륨 탭 〉 특정 볼륨 선택 〉 볼륨 작업 버튼 〉 스냅샷 생성 버튼

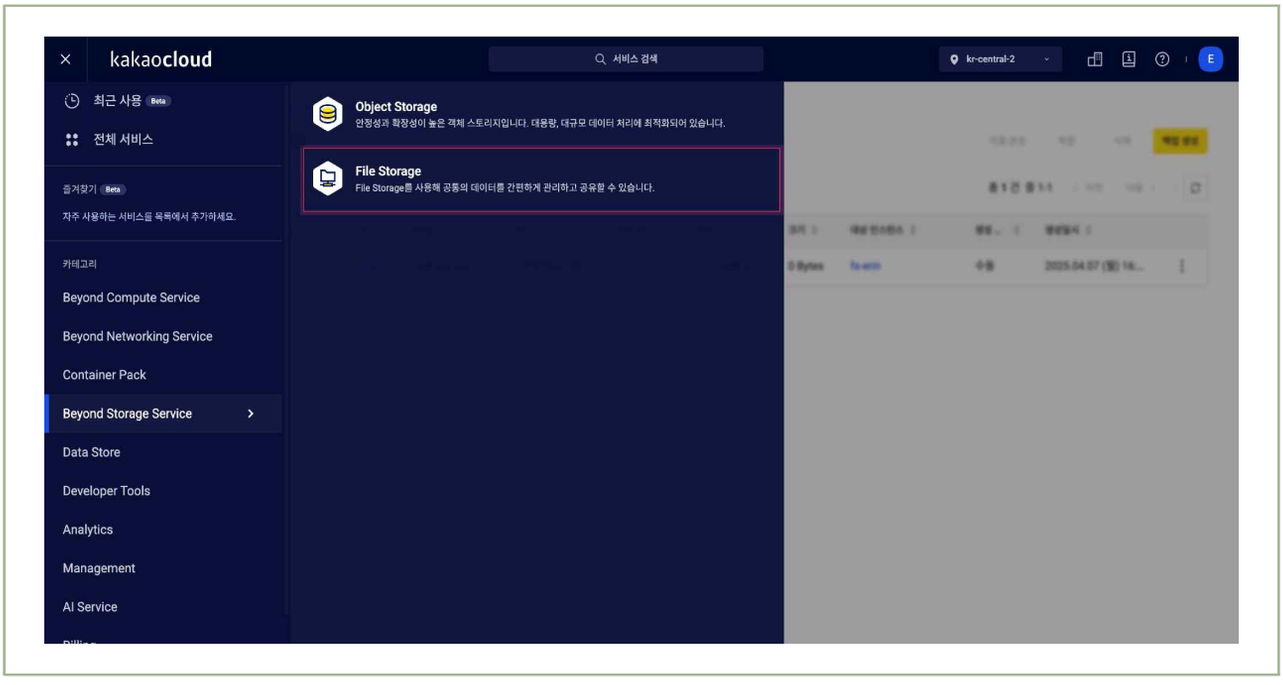


| 그림 8-3-7 | 스냅샷 생성 모달

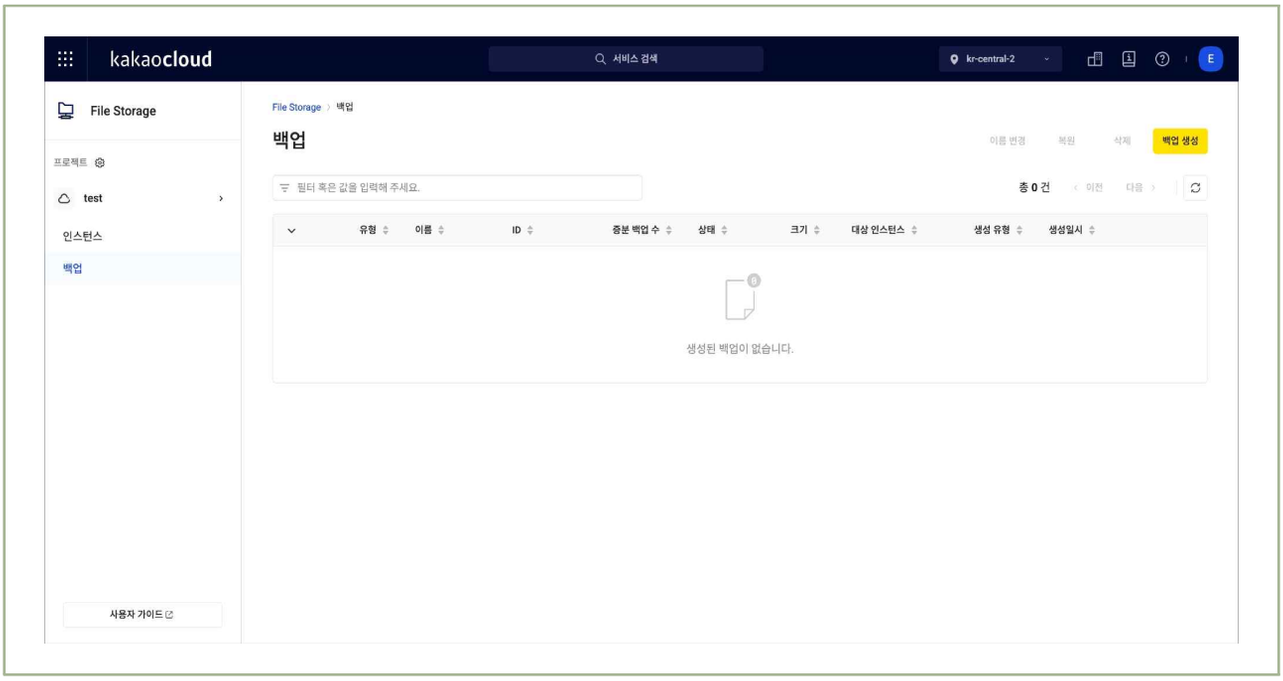


| 그림 8-3-8 | 스냅샷 탭 이동 〉 생성된 스냅샷의 더보기 버튼 〉 스냅샷 복원 선택을 통해 복원 가능

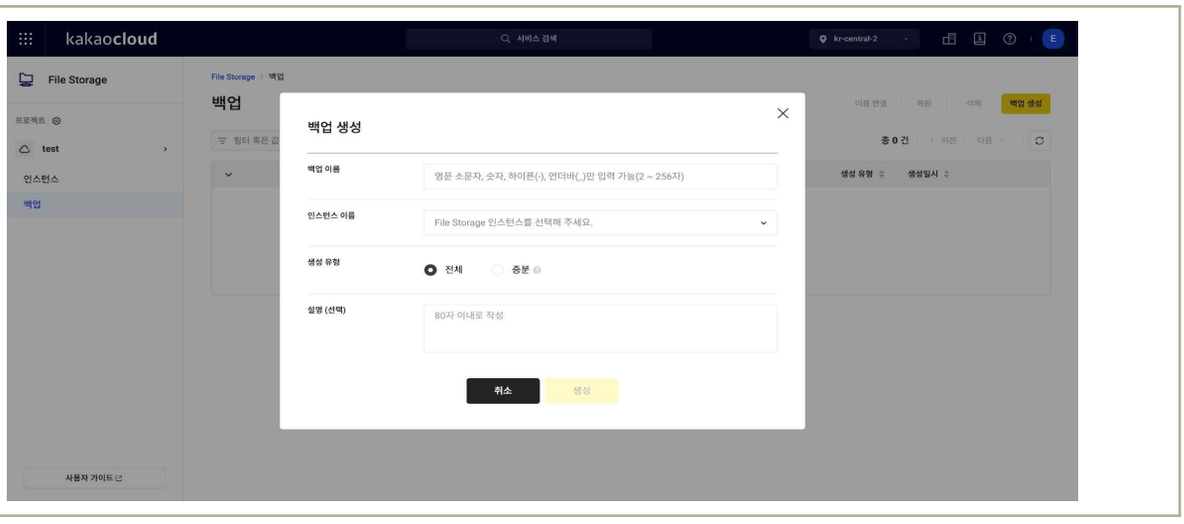
- 전산자료가 보관된 백업 서버의 데이터를 File Storage에 저장하여 원격으로 관리하고, File Storage 백업 기능을 이용해 데이터 복구 필요 시, 신속한 복원이 가능합니다.
  - **(Console)** 'Dashboard' → 'Beyond Storage Service' → 'File Storage' → 백업 기능(전체, 증분)을 통해 백업 생성 및 복원



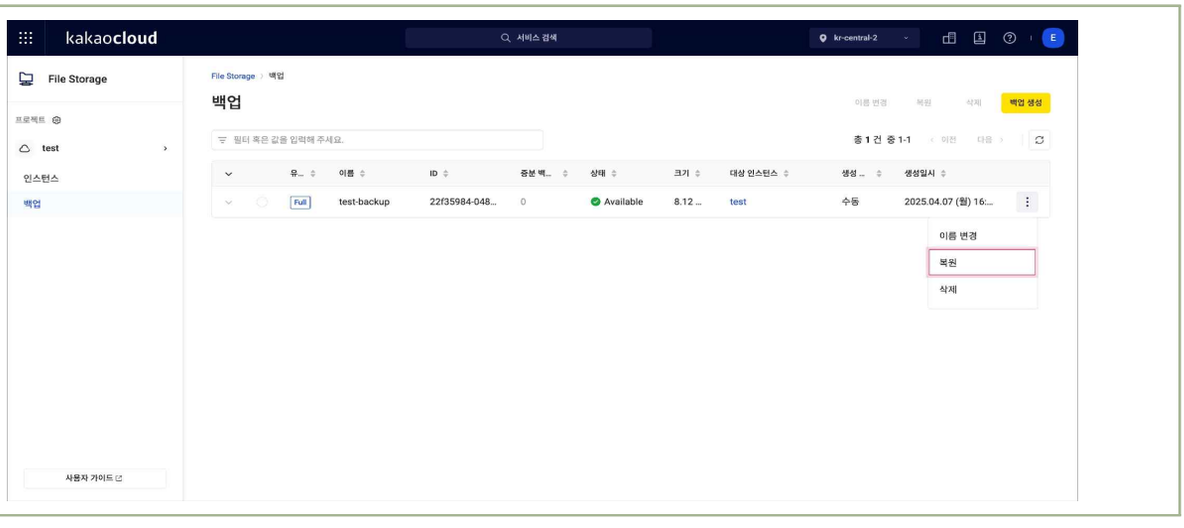
| 그림 8-3-9 | 카카오클라우드 콘솔 〉 File Storage 서비스 이동



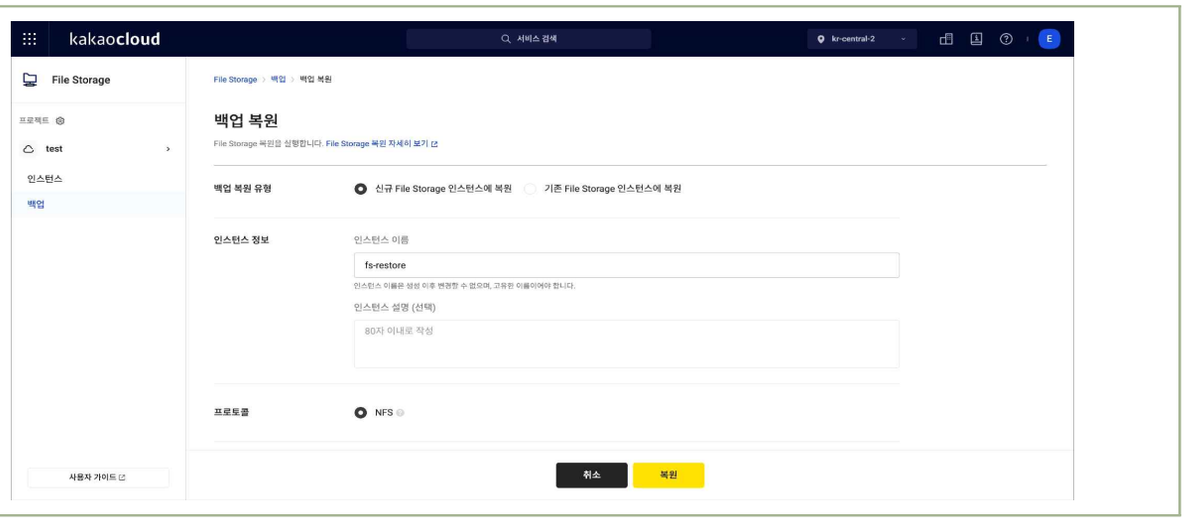
| 그림 8-3-10 | 백업 탭 〉 백업 생성 버튼



| 그림 8-3-11 | 백업 생성 모달

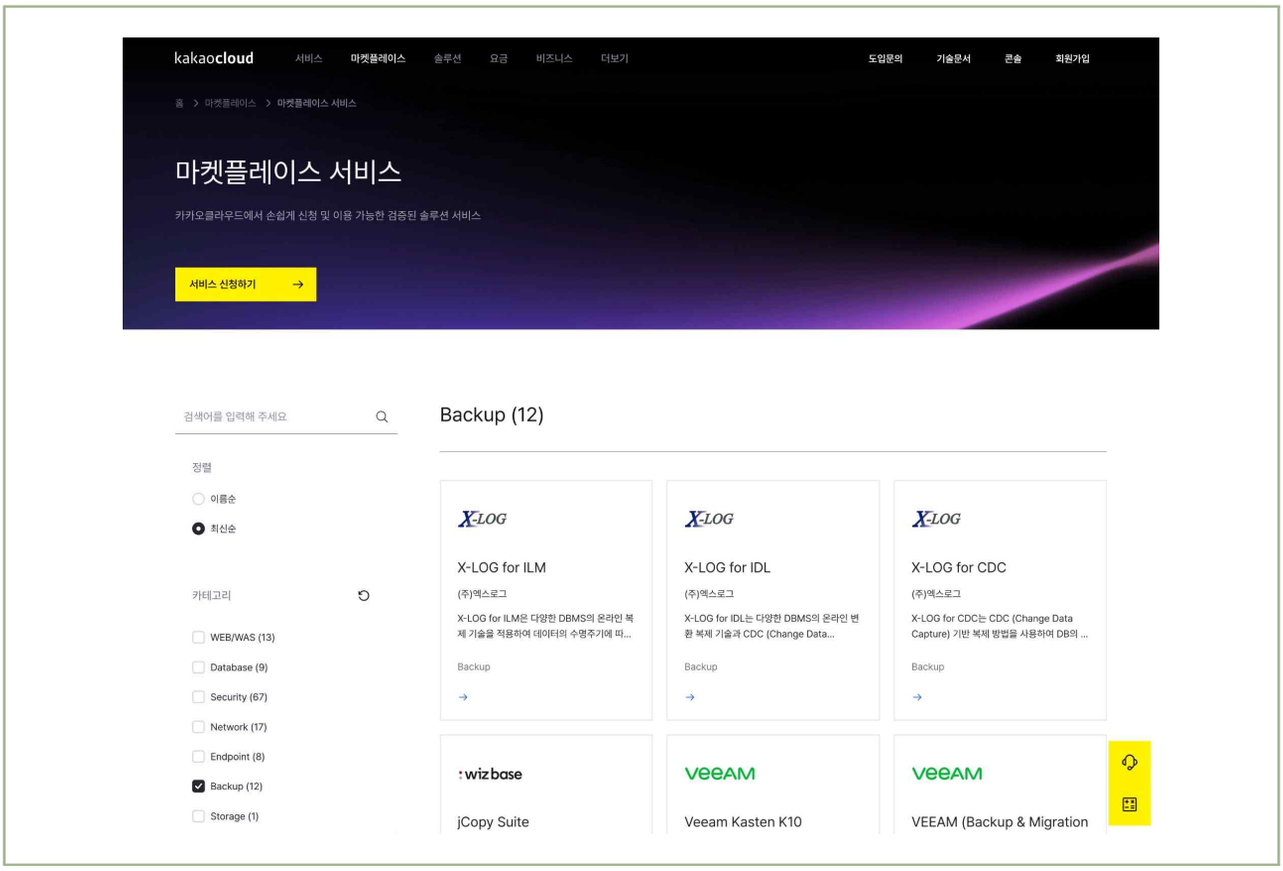


| 그림 8-3-12 | File Storage 백업 복원



| 그림 8-3-13 | File Storage 백업 복원 화면

- 마켓플레이스 3rd-party 백업 솔루션을 이용한 백업이 가능합니다.
  - **(3rd-party 제품)** MarketPlace 중 Backup 상품 군 내 적절한 제품 이용



| 그림 8-3-14 | 마켓플레이스 3rd-party 백업 솔루션 목록

4 참고 사항

- 카카오클라우드 이미지 생성 및 관리 가이드
- 카카오클라우드 스냅샷/일정 생성 및 관리
- 카카오클라우드 File Storage 백업 가이드
- 카카오클라우드 마켓플레이스 Backup 서비스

1 기준

식별번호	기준	내용
8.4.	**금융회사 전산자료 백업 파일 무결성 검증**	**금융회사의 전산자료 백업파일은 무결하게 보관하여야 한다.**

2 설명

- 백업을 통해 보관되고 있는 전산자료에 대해 무결성이 보장되어야 한다.

  - 예시

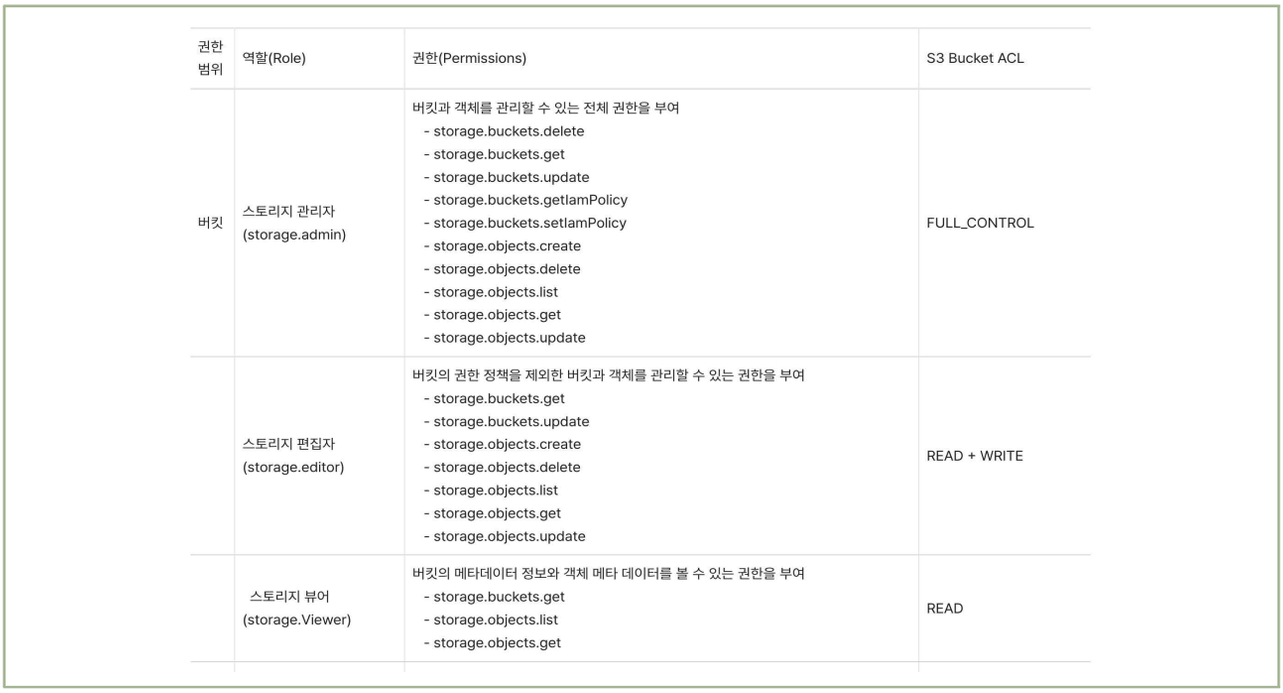
    1) 백업 파일 훼손에 대한 탐지 및 알람 설정

    2) 백업 기능(객체 잠금 등)을 통해 무결성 보장 등

3 우수 사례

- Object Storage를 통해 백업 파일을 저장해두었을 경우, 같은 프로젝트에 속한 구성원을 대상으로 스토리지 객체 접근 권한 및 역할을 개별적으로 부여함으로써 무결성을 보장할 수 있습니다.

  - 역할에 따라 버킷에 대한 임의의 동작(버킷 생성, 객체 조회, 권한 부여 등)이 제한



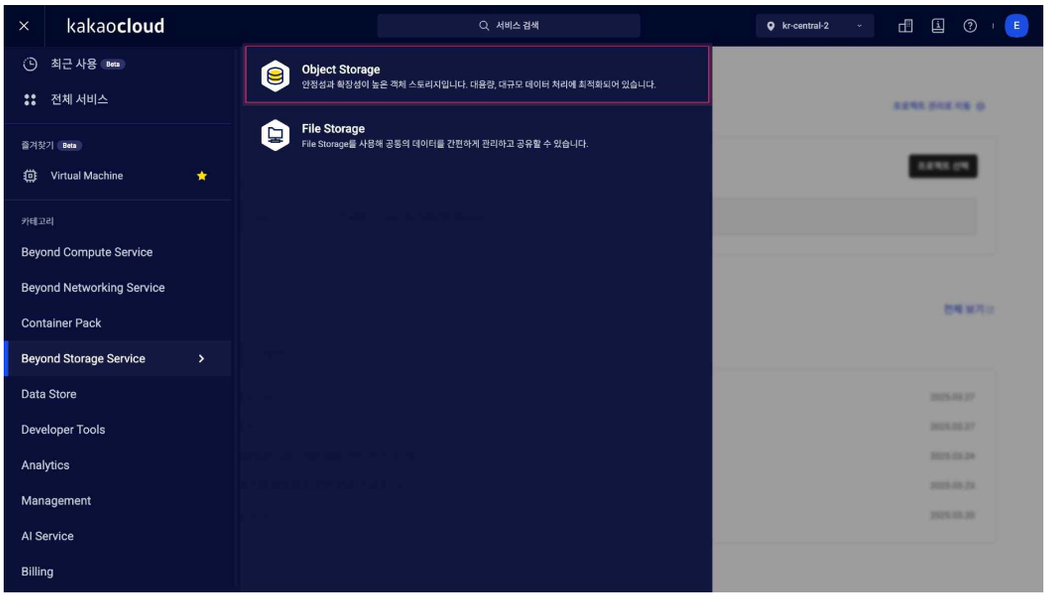
권한 범위	역할(Role)	권한(Permissions)	S3 Bucket ACL
버킷	스토리지 관리자 (storage.admin)	버킷과 객체를 관리할 수 있는 전체 권한을 부여 - storage.buckets.delete - storage.buckets.get - storage.buckets.update - storage.buckets.getIamPolicy - storage.buckets.setIamPolicy - storage.objects.create - storage.objects.delete - storage.objects.list - storage.objects.get - storage.objects.update	FULL_CONTROL
	스토리지 편집자 (storage.editor)	버킷의 권한 정책을 제외한 버킷과 객체를 관리할 수 있는 권한을 부여 - storage.buckets.get - storage.buckets.update - storage.objects.create - storage.objects.delete - storage.objects.list - storage.objects.get - storage.objects.update	READ + WRITE
	스토리지 뷰어 (storage.Viewer)	버킷의 메타데이터 정보와 객체 메타 데이터를 볼 수 있는 권한을 부여 - storage.buckets.get - storage.objects.list - storage.objects.get	READ

| 그림 8-4-1 | Object Storage 역할별 버킷 권한 내용 일부

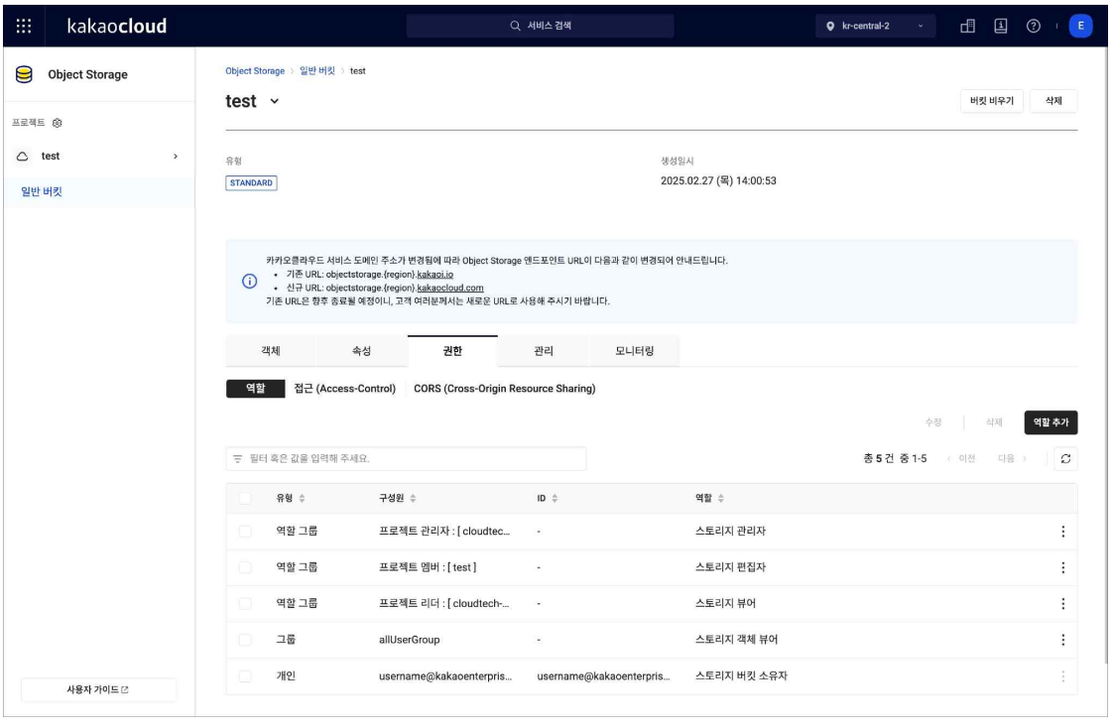
범위	권한(Permission)	기능
버킷	storage.buckets.create	버킷 생성하기
	storage.buckets.delete	버킷 삭제하기
	storage.buckets.list	버킷 목록 조회하기, 버킷의 메타 데이터 조회하기
	storage.buckets.get	버킷의 상세 정보, 메타 데이터 조회하기
	storage.buckets.update	버킷 수정하기 - 예시: 메타 데이터 수정
	storage.buckets.getIamPolicy	버킷 권한 정책 조회하기, Lifecycle 조회
	storage.buckets.setIamPolicy	버킷 권한 정책 등록, 수정, 삭제하기, Lifecycle 설정
객체	storage.objects.create	객체 등록하기 - 예시: 파일 업로드, 폴더 만들기
	storage.objects.delete	객체 삭제하기
	storage.objects.list	객체 조회하기 - 예시: 객체 목록 조회 및 객체의 메타 데이터 조회
	storage.objects.get	객체 상세 정보 조회하기 - 예시: 객체의 메타 데이터 조회, 객체 태그 조회, 파일 정보 조회, 파일 다운로드
	storage.objects.update	객체 수정하기 - 예시: 객체의 메타 데이터 추가/수정, 객체 태그 추가/삭제, 이름 바꾸기
	- storage.objects.create - storage.objects.delete - storage.objects.get	파일 이동하기
	- storage.objects.create - storage.objects.get	파일 복사하기

| 그림 8-4-2 | 버킷 또는 객체에 해당하는 권한별 기능

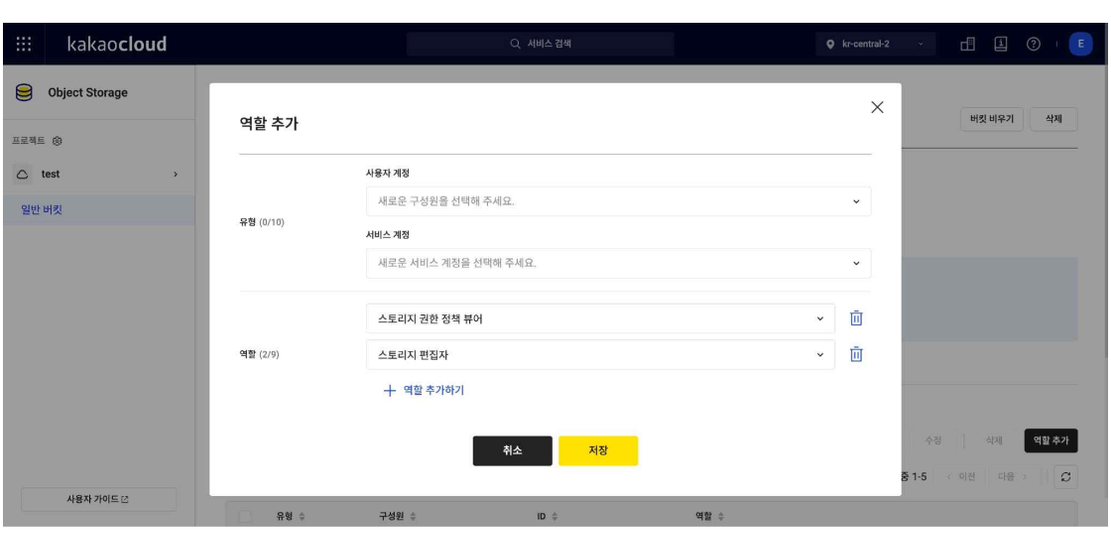
- **(Console)** ‘Dashboard’ → ‘Beyond Storage Service’ → ‘Object Storage’ → 특정 버킷의 ‘권한’ 탭에서 사용자 계정 혹은 서비스 계정에 역할 추가



| 그림 8-4-3 | 카카오클라우드 콘솔 〉 Object Storage 서비스 이동



| 그림 8-4-4 | 버킷 상세 페이지 〉 권한 탭 〉 역할 탭 〉 역할 추가 버튼



| 그림 8-4-5 | 사용자 계정 혹은 서비스 계정에 역할 추가

- 카카오클라우드 Object Storage는 자체 무결성 검증 과정이 있기 때문에 무단 변경이 불가능합니다.

4 참고 사항

1 기준

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

2 설명

- 백업 자료의 생성, 변경, 삭제 등 관련 내역을 기록하고 관리하여야 한다.

  - 예시

    1) 백업 작업 로그 저장

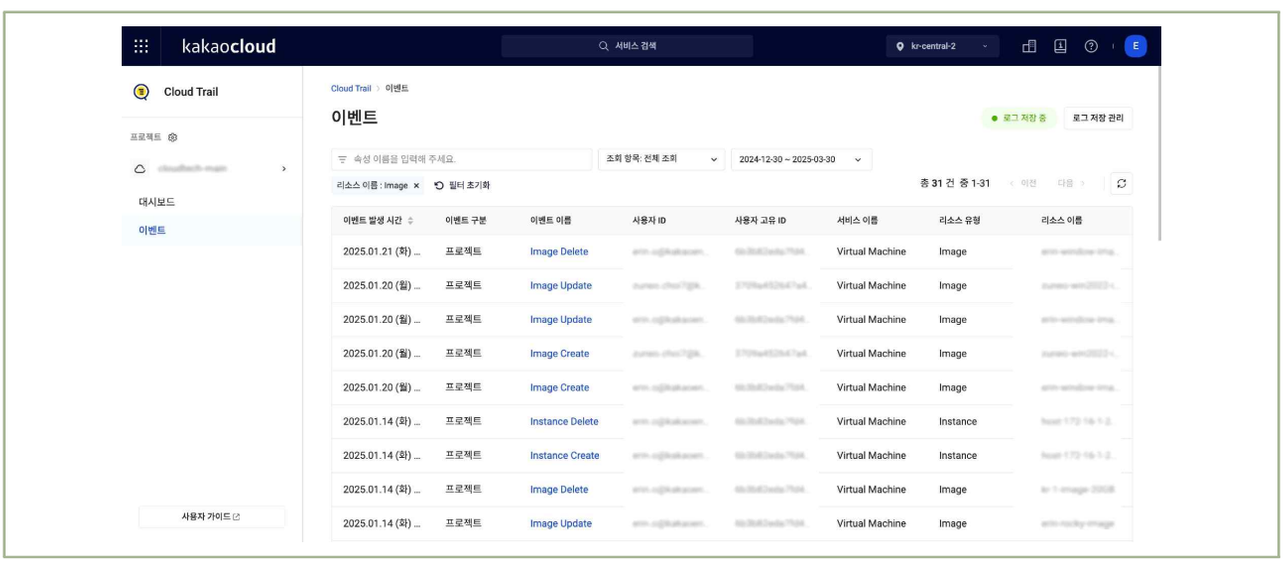
    2) 백업대상, 백업주기, 백업담당자 등 정책 수립

    3) 정상적인 백업 수행 여부에 대한 모니터링 등

3 우수 사례

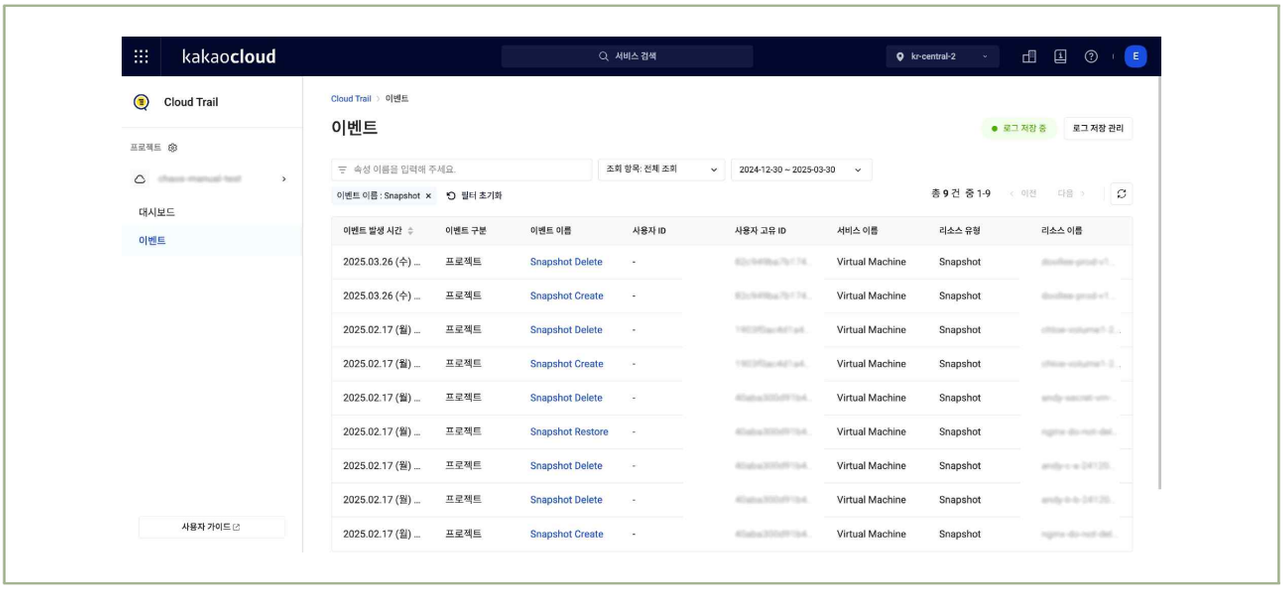
- 백업 서버의 이미지 생성 시, Cloud Trail을 통해 이미지 생성/수정/삭제 작업 이벤트 로그를 확인할 수 있습니다.

  - **(Console)** ‘Dashboard’ → ‘Management’ → ‘Cloud Trail’ → 검색 기능을 통해 이미지 관련 이벤트 로그 확인



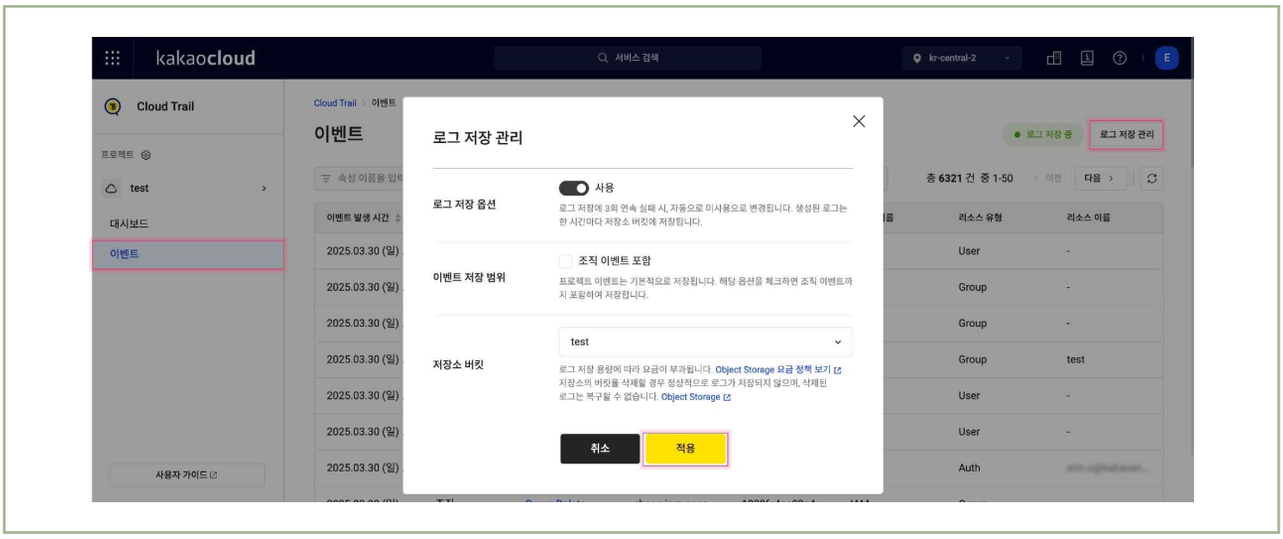
| 그림 8-5-1 | 카카오클라우드 콘솔 〉 Cloud Trail 이벤트의 이미지 관련 이벤트 목록

- 백업 서버의 스냅샷 생성 시, Cloud Trail을 통해 스냅샷 생성/삭제/복원 작업 이벤트 로그 를 확인할 수 있습니다.
  - **(Console)** ‘Dashboard’ → ‘Management’ → ‘Cloud Trail’ → 검색 기능을 통해 스냅샷 관련 이벤트 로그 확인



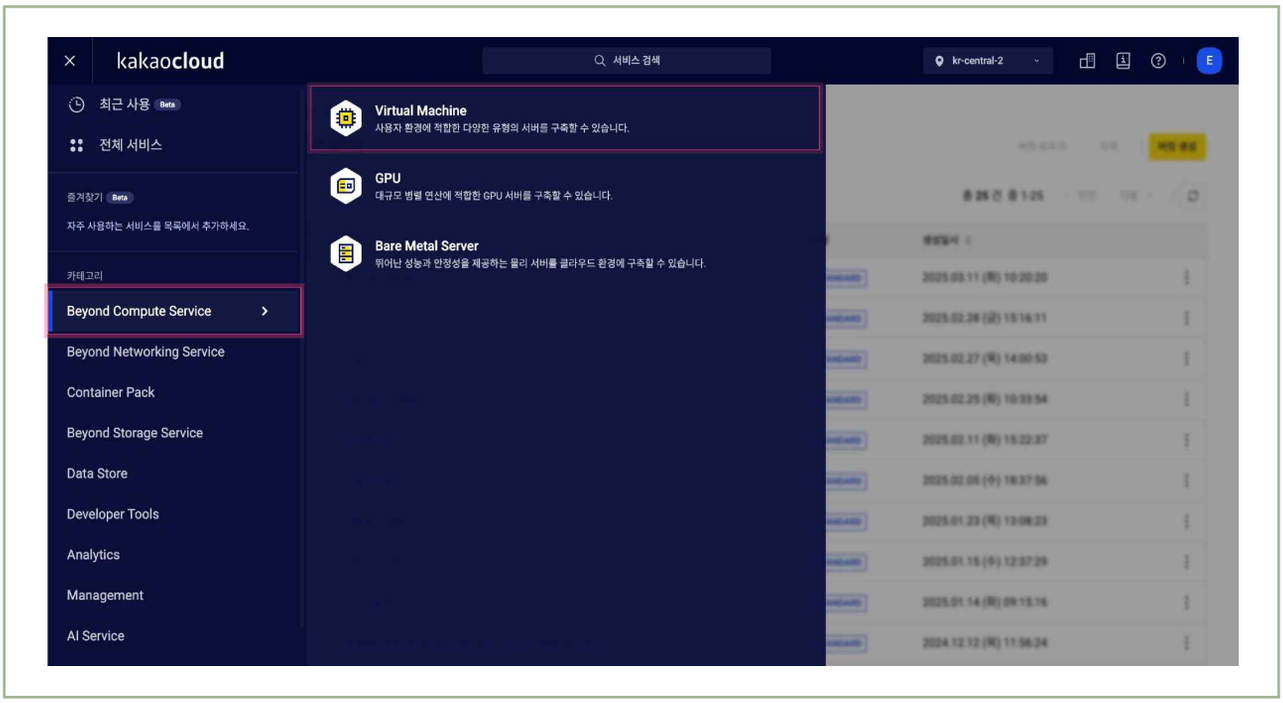
| 그림 8-5-2 | 카카오클라우드 콘솔 〉 Cloud Trail 이벤트의 스냅샷 관련 이벤트 목록

- Cloud Trail에 기록된 이미지 혹은 스냅샷의 이벤트 로그들은 Object Storage 버킷으로 로그를 장기간 보관할 수 있습니다.
  - **(Console)** ‘Dashboard’ → ‘Management’ → ‘Cloud Trail’ → 이벤트 탭에서 로그 저장 기능 활성화

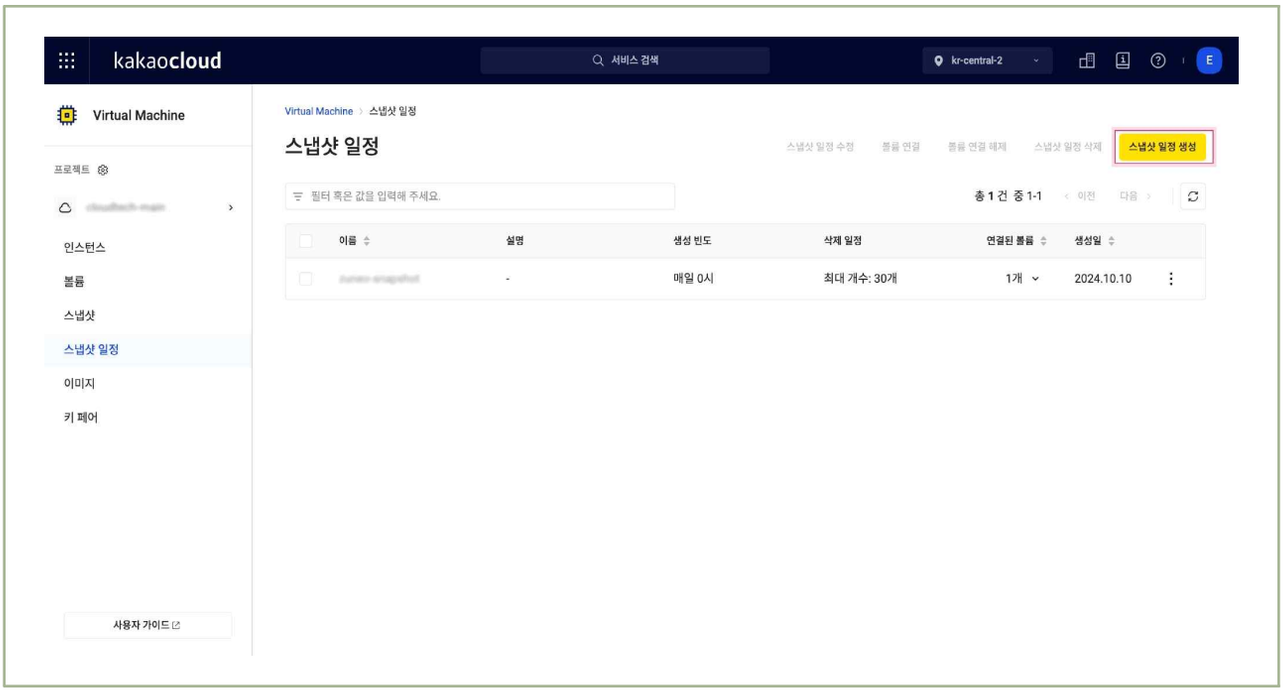


| 그림 8-5-3 | 이벤트 탭 〉 로그 저장 관리 버튼 〉 로그 저장할 버킷 선택하여 로그 장기간 저장

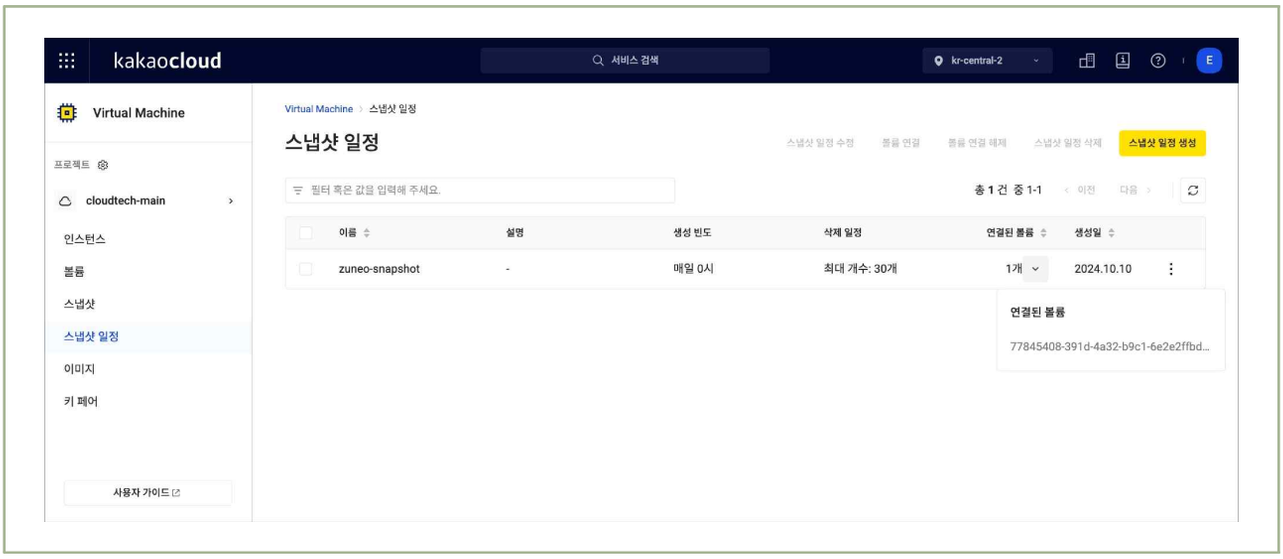
- 백업 서버의 볼륨 상태 변화에 대응하기 위해 스냅샷 생성 주기를 설정할 수 있습니다.
  - **(Console)** 'Dashboard' → 'Beyond Compute Service' → 'Virtual Machine' → 이벤트 탭에서 로그 저장 기능



| 그림 8-5-4 | 카카오클라우드 콘솔 〉 Virtual Machine 서비스로 이동



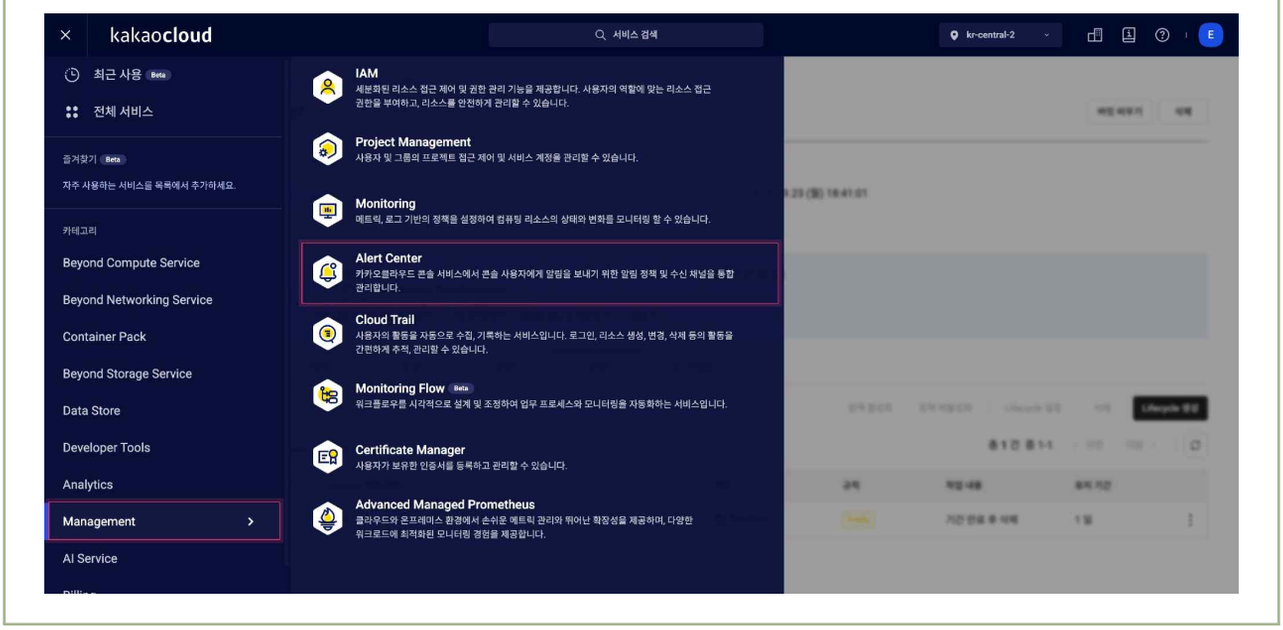
| 그림 8-5-5 | 스냅샷 일정 탭 〉 스냅샷 일정 생성 버튼을 통해 일정 생성 가능



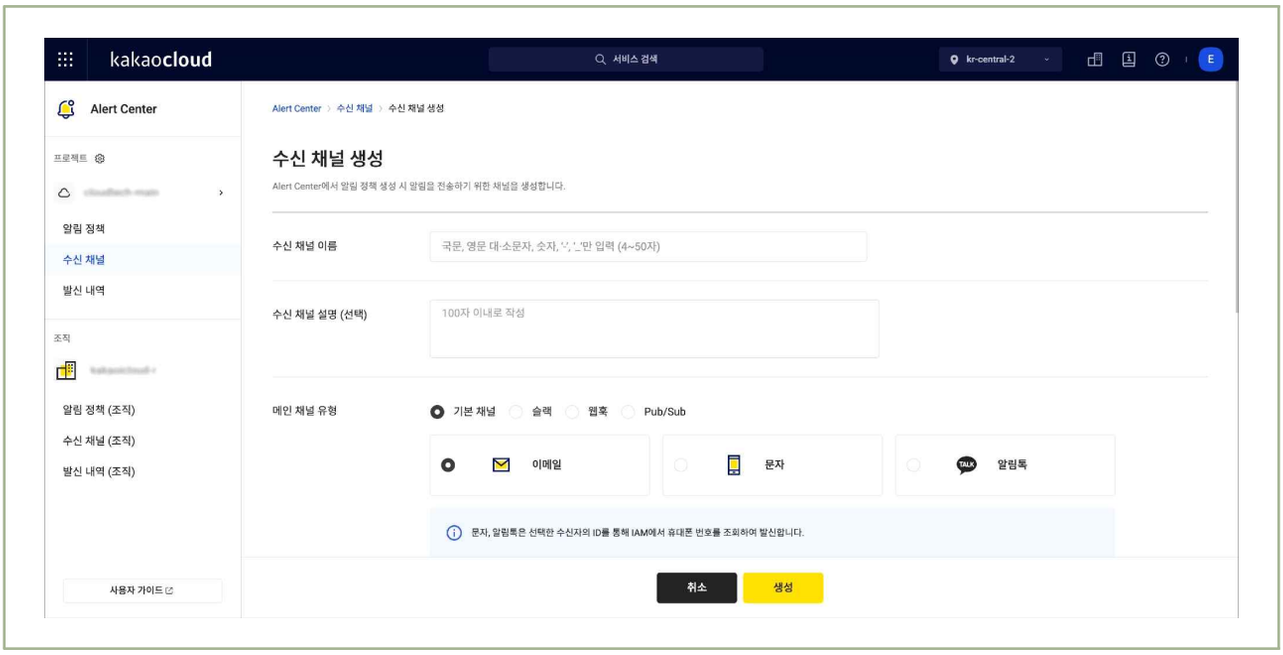
| 그림 8-5-6 | 주기적으로 스냅샷 생성 대상이 될 볼륨 확인 가능

- Alert Center의 이벤트 기반 알림을 통해 백업이 정상적으로 수행되는지 모니터링이 가능합니다.
  - 백업 서버의 이미지 생성 시, 이미지 생성/수정/삭제 이벤트 기반 알림 사용
  - 백업 서버 볼륨의 스냅샷 생성 및 복구 시, 스냅샷 생성/삭제/복구 이벤트 기반 알림 사용

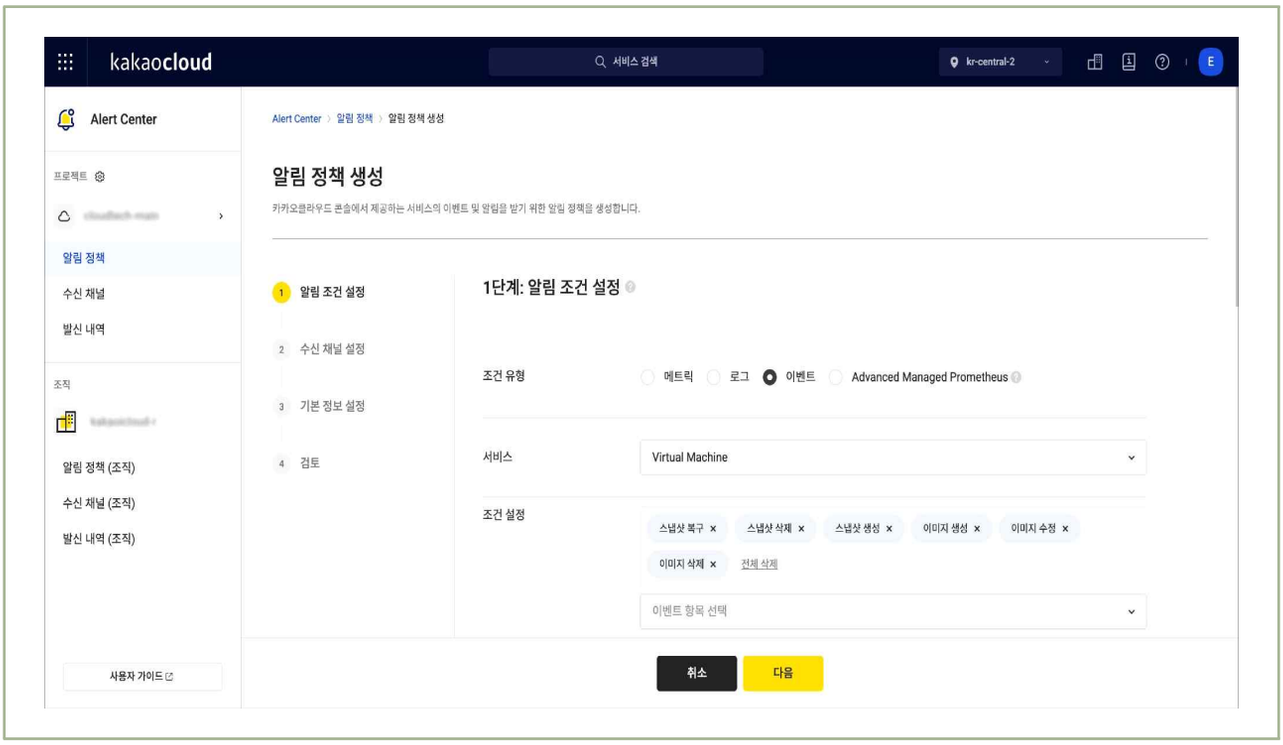
– **(Console)** ‘Dashboard’ → ‘Management’’ → ‘Alert Center’에서 이벤트 기반 알림 설정



| 그림 8-5-7 | 카카오클라우드 콘솔 〉 Alert Center 서비스로 이동



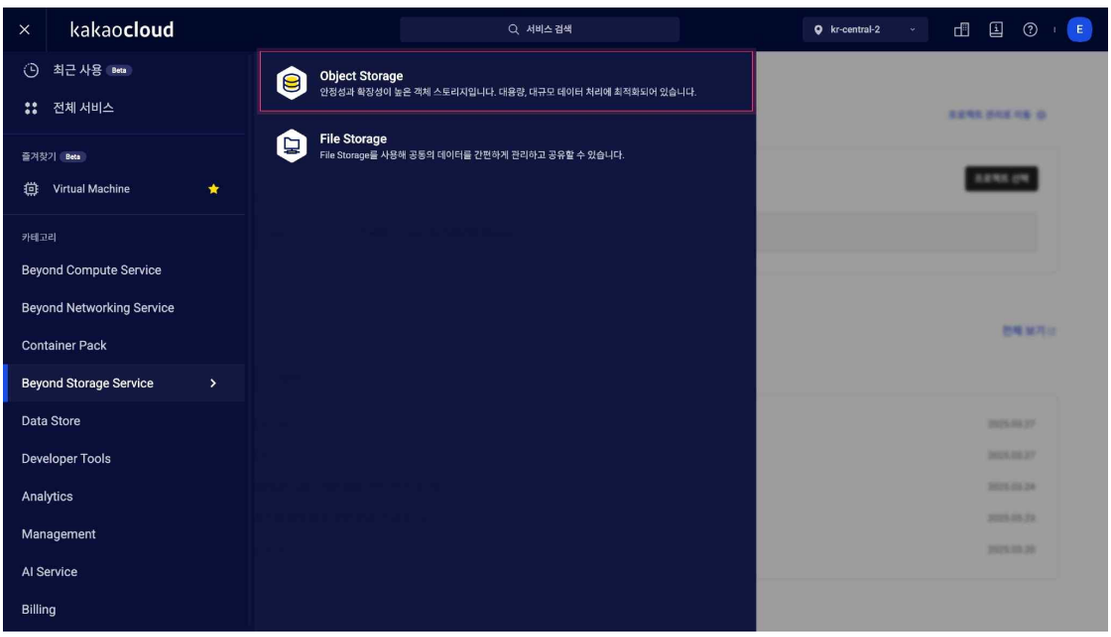
| 그림 8-5-8 | 수신 채널 탭 〉 수신 채널 생성



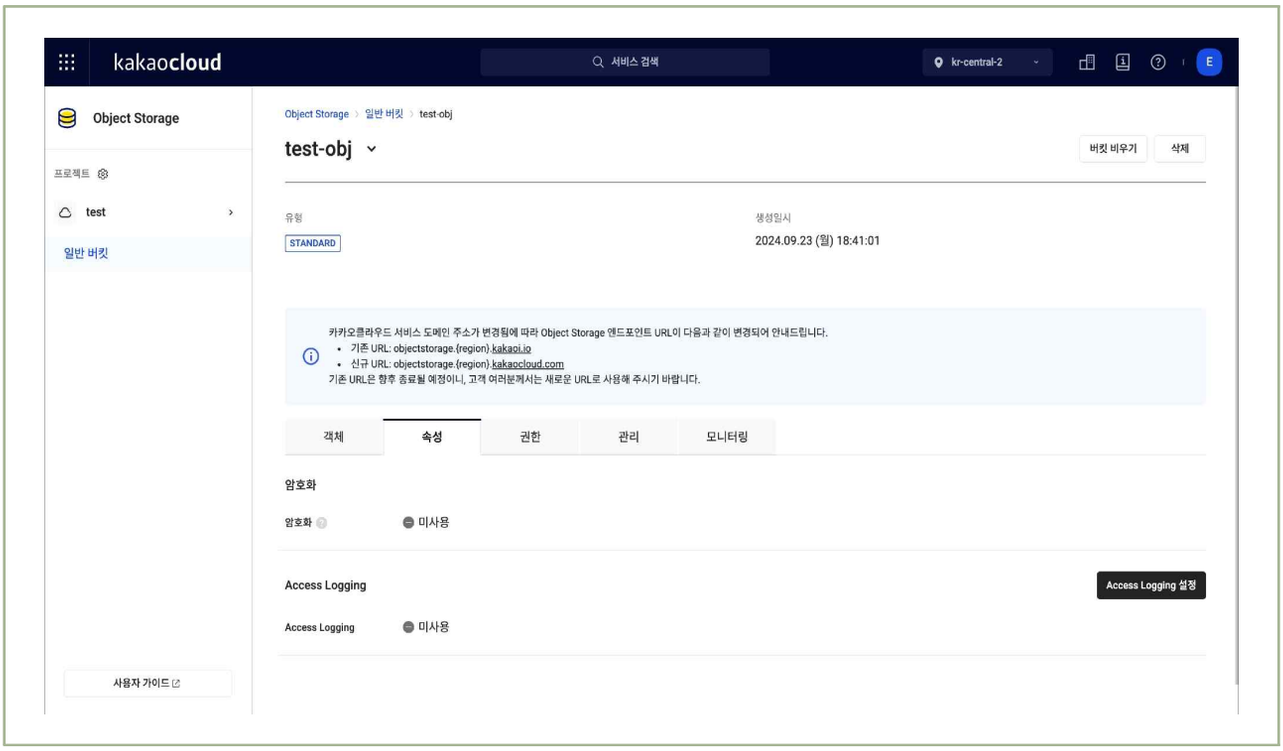
| 그림 8-5-9 | 알림 정책 생성 〉 이벤트 조건 설정 및 기타 설정 완료

| 그림 8-5-10 | 알림 확인

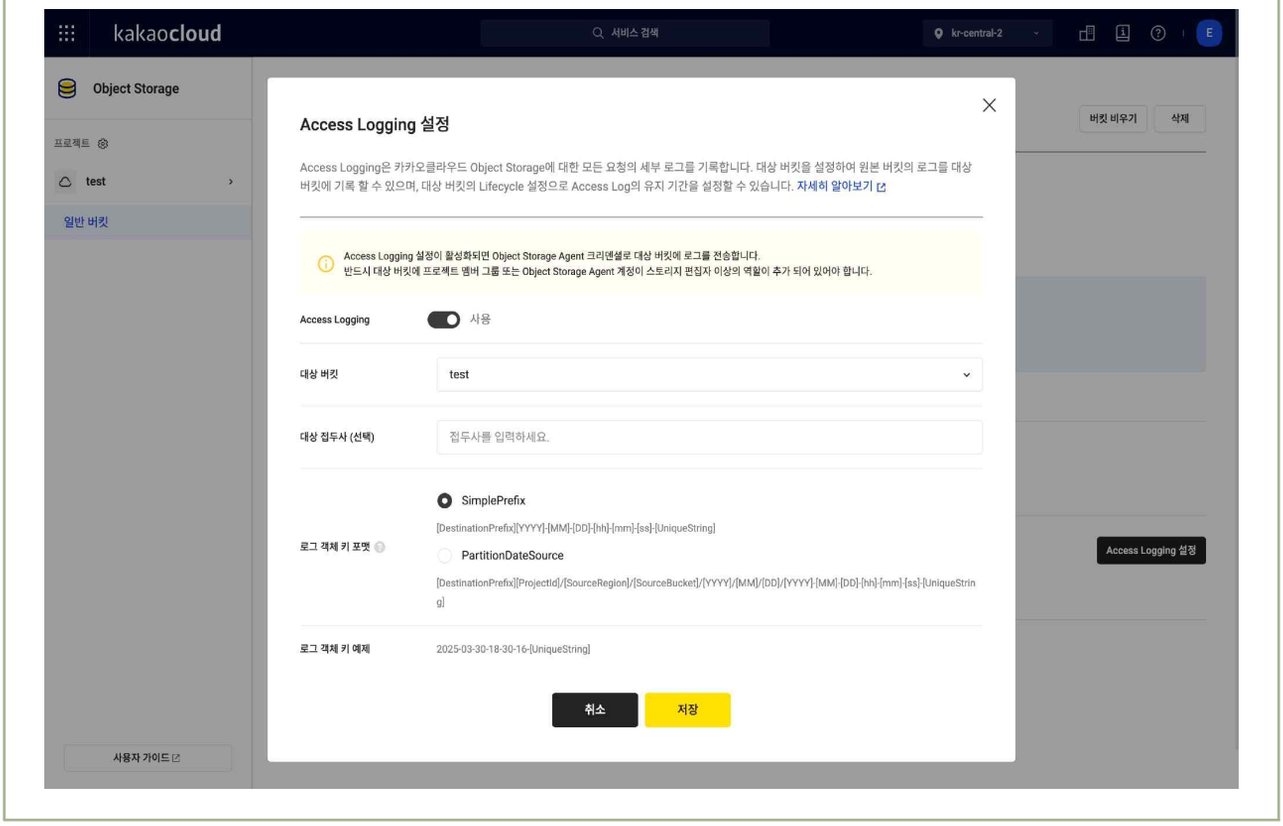
- Object Storage 버킷에 백업 파일을 저장하여 사용 중 일 경우, 버킷의 액세스 로그 설정을 통해 버킷에서 발생하는 이벤트 로그를 다른 버킷에 저장하여 관리가 가능합니다.
  - **(Console)** 'Dashboard' → 'Beyond Storage Service' → 'Object Storage' → 특정 버킷에서 Access Logging 설정



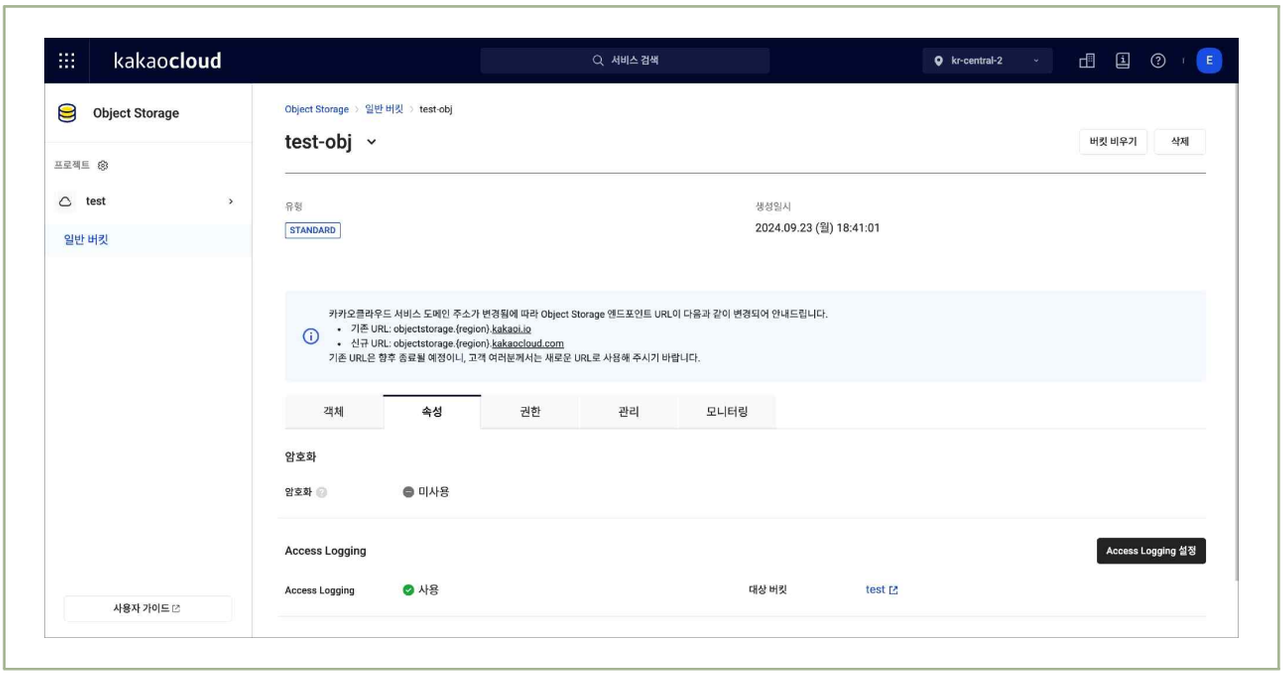
| 그림 8-5-11 | 카카오클라우드 콘솔 〉 Object Storage 서비스 이동



| 그림 8-5-12 | 버킷 상세 페이지 〉 속성 탭 〉 Access Logging 설정 버튼



| 그림 8-5-13 | Access Logging 설정 모달



| 그림 8-5-14 | Access Logging 설정됨 확인

4 참고 사항

- 카카오클라우드 Cloud Trail에서 조회할 수 있는 프로젝트 이벤트 목록
- 카카오클라우드 Cloud Trail 로그 저장 관리 가이드
- 카카오클라우드 스냅샷 일정 생성 및 관리 가이드
- 카카오클라우드 Alert Center로 실시간 알림 설정 튜토리얼
- 카카오클라우드 Object Storage 액세스 로그 설정 가이드
- 카카오클라우드 Object Storage Access Logging 개념 및 활용 가이드

1 기준

식별번호	기준	내용
8.6.	**백업파일 원격 안전지역 보관**	**중요도가 높은 금융회사 전산자료는 원격 안전지역에 소산하여 보관하여야 한다.**

2 설명

- 중요한 금융회사 전산자료는 보안이 강화된 원격 저장소에 보관하여야 한다.

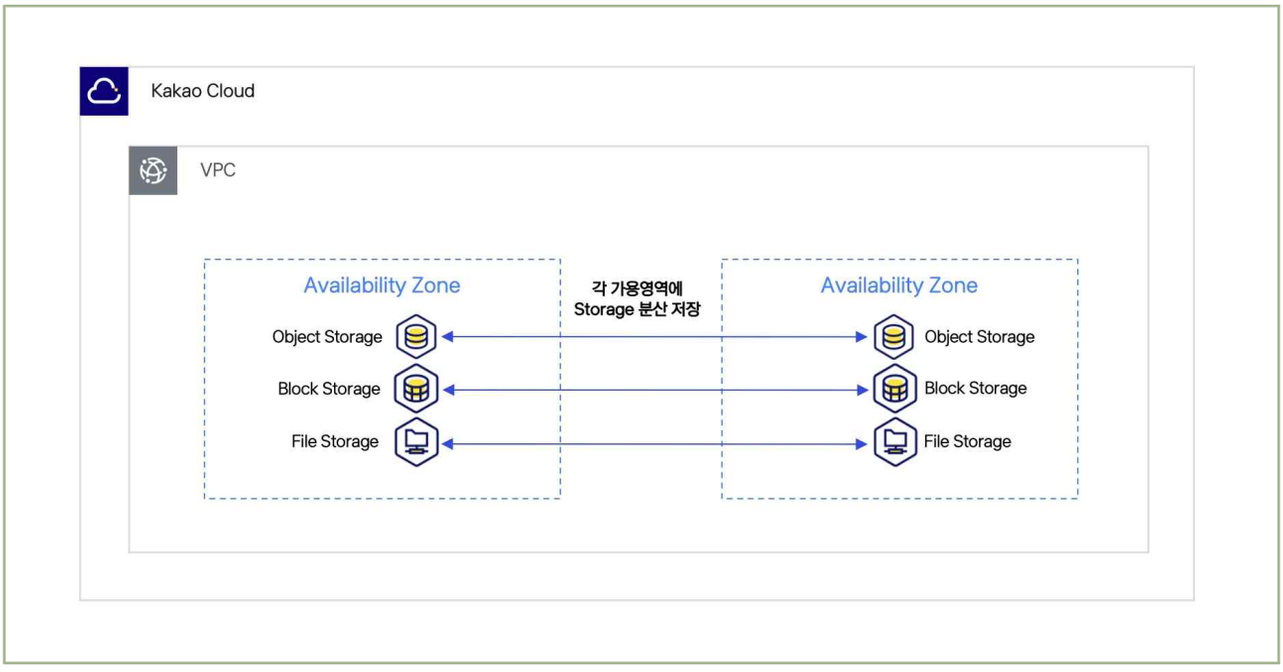
  - 예시

    1) 클라우드 서비스 제공자(CSP)의 DR 서비스 이용

    2) 금융회사 자체 데이터센터로 소산하여 보관 등

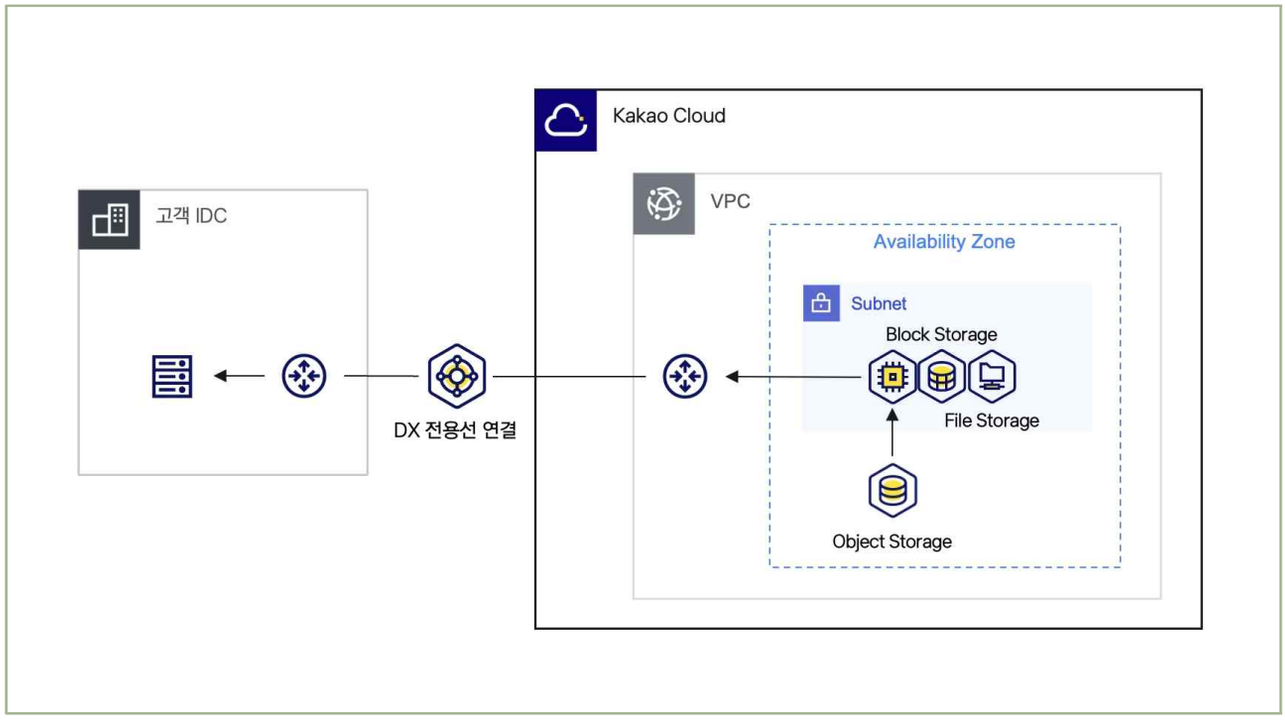
3 우수 사례

- 카카오클라우드의 Storage 서비스는 3-copy 복제 방식을 적용하여 동일한 데이터를 물리적으로 격리된 각 가용영역 2곳에 분산하여 저장함으로써 데이터의 안정성과 내구성을 확보합니다.



| 그림 8-6-1 | 각 가용영역에 Storage 데이터의 분산 저장 구성도

- 카카오클라우드와 금융회사 자체 데이터센터 간의 전용회선을 구성하여, 자체 데이터 센터로 데이터를 소산하여 물리적으로 격리된 데이터 보관이 가능합니다.



| 그림 8-6-2 | 금융회사 자체 데이터 센터로 데이터 소산

4 참고 사항

- 카카오클라우드 DR 이용자 가이드
- 카카오클라우드 Object Storage 서비스 개요
- 카카오클라우드 File Storage 서비스 개요
- 카카오클라우드 Block Storage 서비스 개요

1 기준

식별번호	기준	내용
8.7.	주요 전산장비 이중화	금융회사는 주요 전산장비를 이중화하여 서비스 가용성을 확보하여야 한다.

2 설명

- 금융회사는 클라우드 환경을 통한 인프라 구성 시 가상화 기능을 이용하여 주요 전산장비를 이중화하여야 한다.

  - 예시

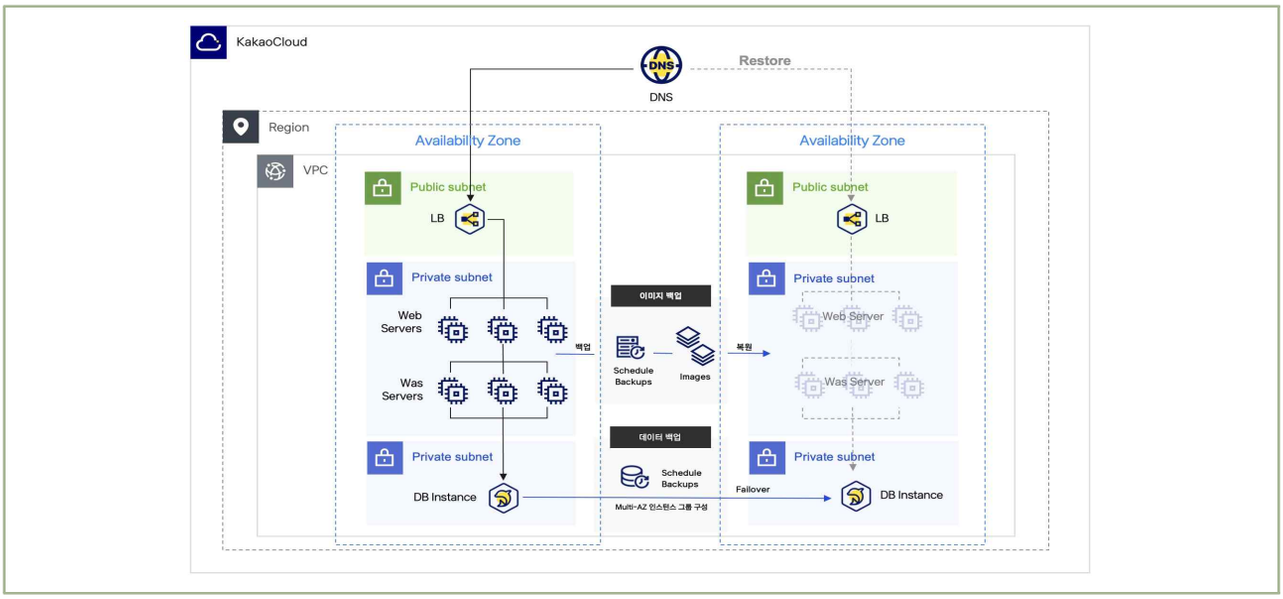
    1) 클라우드 가상화 기능을 이용하여 주요 전산장비(서버, 데이터베이스 등) 이중화 구성

    2) 이중화 구성 시 원격 안전지역 등을 고려

3 우수 사례

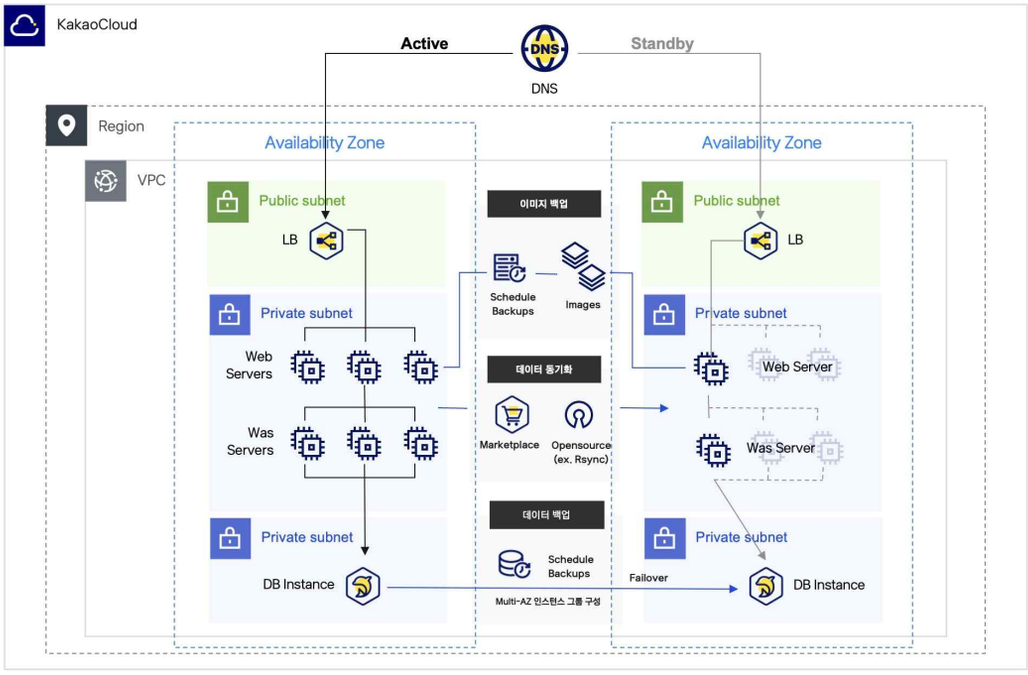
- 카카오클라우드는 다중 가용영역(Multi-AZ) 환경에서 주요 전산장비(서버, 데이터 베이스 등) 이중화 구성이 가능합니다.

  - Backup-Restore 구성: 서비스 중인 특정 AZ에 재해 상황 발생 시, 미리 스케줄링된 백업을 이용하여 효과적으로 데이터 복원이 가능



| 그림 8-7-1 | Backup-Restore 구성도

- Active-Standby 구성: Active AZ에 재해 상황 발생 시, Standby AZ의 인프라가 확장되어 효과적으로 재해 복구가 가능



| 그림 8-7-2 | Active-Standby 구성도

4 참고 사항

금융분야 상용 클라우드컴퓨팅서비스 보안 관리 참고서 (카카오엔터프라이즈)

발 행 일	2025년 10월
발 행 인	금융보안원(원장 박상원)
공 동 발 행 인	카카오엔터프라이즈

금융보안원		카카오엔터프라이즈	
클라우드대응부	부장 김제광	**정보보안실**	실장 배대한
클라우드기획팀	팀장 장지현		팀장 임병두
	차장 정희선		팀원 김기진
	과장 김용규	**서비스개발실**	실장 윤병식
	과장 안성현		팀장 노주용
	과장 마승영		팀원 오예진
	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