# 금융분야 상용 클라우드컴퓨팅서비스 보안 관리 참고서

Cloud

### 카카오엔터프라이즈

**(/)** 



kakao enterprise

1.	가상자원 관리
	1.1. 가상자원 생성 시 최초 계정에 대한 비밀번호 규칙 수립
	1.2. 이용자 가상자원 접근 시 로그인 규칙 적용
	1.3. 가상자원 루트 계정 접근 시 추가인증수단 제공6
	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

#### 

2.1. 업무 목적에 따른 네트워크 구성
2.2. 내부망 네트워크 보안 통제
2.3. 네트워크 보안 관제 수행
2.4. 공개용 웹서버 네트워크 분리
2.5. 네트워크 사설 IP주소 할당 및 관리
2.6. 네트워크(방화벽 등) 정책 주기적 검토61

# 3. 계정 및 권한 관리 66 3.1. 클라우드 계정 권한 관리 67 3.2. 이용자별 인증 수단 부여 74 3.3. 인사 변경사항 발생 시 계정 관리 78 3.4. 클라우드 가상자원 관리 시스템 관리자 권한 추가인증 적용 83 3.5. 클라우드 가상자원 관리 시스템 로그인 규칙 수립 85 3.6. 계정 비밀번호 규칙 수립 87 3.7. 공개용 웹서버 접근 계정 제한 89

금융분야 상용 클라우드컴퓨팅서비스 보안 관리 참고서

## CONTENTS

• • •

4.	암호키 관리	90
	4.1. 암호화 적용 가능 여부 확인	91
	4.2. 암호키 관리 방안 수립	94
	4.3. 암호키 서비스 관리자 권한 통제	97
	4.4. 암호키 호출 권한 관리	98
	4.5. 안전한 암호화 알고리즘 적용	99

#### 

5.1. 가상자원 이용(생성, 삭제, 변경 등)에 관한 행위추적성 확보 101
5.2. 가상자원 이용 행위추적성 증적 모니터링
5.3. 이용자 가상자원 모니터링 기능 확보
5.4. API 사용(호출대상, 호출자, 호출일시등)에 관한 행위추적성 확보 133
5.5. 네트워크 관련 서비스(VPC, 보안그룹, ACL 등)에 관한 행위추적성 확보… 134
5.6. 계정 변동사항에 대한 행위추적성 확보
5.7. 계정 변경사항에 관한 모니터링 수행

## 1. 가상자원 관리

- 1.1. 가상자원 생성 시 최초 계정에 대한 비밀번호 규칙 수립
- 1.2. 이용자 가상자원 접근 시 로그인 규칙 적용
- 1.3. 가상자원 루트 계정 접근 시 추가인증수단 제공
- 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



가상자원 관리



#### 1.1. 가상자원 생성 시 최초 계정에 대한 비밀번호 규칙 수립

#### 1 기준

식별번호	기준	내용
1 1	가상자원 생성 시 최초 계정에	이용자 가상자원 생성 시 최초 계정에 대한 비밀번호 규칙을
1.1	대한 비밀번호 규칙 수립	수립하여야 한다.

#### 2 설명

- ▶ 이용자 가상자원에 접근하는 계정에 대한 비밀번호 규칙 등 보안통제 방안을 수립하여야 한다.
  - 1) 가상머신, 베어메탈 생성 시 PEM키(private key)를 생성한 이용자가 다운로드 받도록 하고, 이후 클라우드 상에서는 공유하는 기능을 제공하지 않는다.
  - 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

1) 이용자가 가상자원 생성 시 비밀번호를 설정할 수 없으며, PEM키를 선택해야 생성이 가능하다.

▶ (Console) 'Dashboard' → 'Beyond Compute Service' → 'Virtual Machine' → '인스턴스 생 성' 시 비밀번호를 입력하는 기능은 없으며, PEM키를 선택하지 않으면 설치가 진행되지 않음



× kakao <b>cloud</b>	Q, 서비스 검색		♀ kr-centr	ral-2 ~	₫
(b) 최근 사용 >	Virtual Machine				
🛟 전체 서비스	사용사 환경에 직접한 나강한 규용의 시여를 구역을 두 있습니다.			THE BARA	-
즐겨찾기 Beta	YPC 논리적으로 격리된 가상 네트워크를 구성할 수 있습니다.		8 33 2 8 1 20	- 10 18	*
자주 사용하는 서비스를 목록에서 추가하세요.	GPU GPU	-	-		
카테고리	대규모 병렬 연산에 직합한 GPU 서버를 구축할 수 있습니다.	172.16.3 15		kr central	20
Beyond Compute Service	Transit Gateway 다수의 VPC와 온프레미스 네트워크를 연결하여 중앙 집중식으로 관리할 수 있습니다.	172.16.5 0		kr central	20
Beyond Networking Service		172.16.1_ ©		kr cantral	20
Container Pack	Object Storage     안정성과 확장성이 높은 객체 스토리지입니다. 대용량, 대규모 데이터 처리에 최적화되어 있습니다.	172.16.5 0		kr central	21
Beyond Storage Service		172.14.5 0		kroentral	20
Data Store	· · · · · · · · · · · · · · · · · · ·	172.16.1 0		krostsi	20
Developer Tools	Alert Center 카가오클라우드 프로 셔비스에서 콘솔 사용자에게 알림을 보내기 위한 알림 정책 및 수신 채널을	172.16.3 0		kr-central	20
Analytics	응입 전리입니다.	172.16.0 15		kr-central	20
Management	Load Balancing 사용자 환경에 직합한 설정을 통해 트래픽 분산을 최적화할 수 있습니다.	172.16.2. 0		kr-central	20
[그림 1.	1.1] 카카오클라우드 콘솔 〉 Virtual Machine	서비스	이동		

iii kakao**cloud** ₫ 🗄 🕐 🗉 Virtual Machine 1 가장 범용적으로 사용하는 머신 유형이며 가격 및 유연성을 위해 최적화되었습니다.자세히 보기 간 프로젝트 요약 정보 볼륨 GB SSD ~ Ū Cloudtech-main 10 , > 루트 볼륨 기본 정보 및 개수 인스턴스 총 1개의 인스턴스 十 볼륨 추가 볼륨 실정할 루트 불롭의 크기가 이 이미지를 생성할 때 사용된 인스턴스의 불률 크기보다 작을 경우, 오유 상태의 인스턴스 가 생성됩니다. test-vm 스냅샷 이미지 스냅샷 일정 Ubuntu 20.04 - 5.4.0-173 Kernel 5.4.0.173 (x86\_64) c82e5896-9bc6-4fbc-bdef-6671ceb2c4bb x86\_64 architecture 이미지 검색어를 입력해 주세요. 키페어 키 페어를 선택해 주세요. 키 페어 인스턴스 유형 외부에서 접근 가능한 퍼블릭 IP는 인스턴스 생성 후 **[퍼블릭 IP 연결]** 메뉴에서 할당 가능합니다. 네트워크 m2a.large 2 vCPU 8 GiB Memory VPC cloudtech-vpc-172 (172.16.0.0/16) 볼륨 10 GB 루트 볼륨 서브넷 SSD . .---//== // = = /== 취소 생성 사용자 가이드 🖸 [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 생성 불가

Request Header					
종류	파라미터	형식	설명		
Heade	er X-Auth-Token*	String	{tokenId}: API 인증 토큰		
Reques	st 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_zo	ne*		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 Bequest 파라미터				

#### 4 참고 사항

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



#### 1.2. 이용자 가상자원 접근 시 로그인 규칙 적용

#### 1 기준

식별번호	기준	내용
1 0	이용자 가상자원 접근 시 로그인	이용자 가상자원 접근 계정에 대한 안전한 로그인 규칙을
1.2	규칙 적용	수립하여야 한다.

#### 2 설명

- 이용자는 패스워드 무작위 대입 공격등에 대응하기 위해 가상자원 접근계정에 대한 안전한 로그인 규칙을 수립하여야 한다.
  - (예시)
    - 1) 로그인 오류에 따른 보안통제 방안 수립 등

#### 3 우수 사례

- 1) 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 설정

kakao <b>cloud</b>	소개 서비스 마켓플레이스 파트너 	리소스 고객지원 기술문서 공공기관용 💌
	<b>Marketplace</b> 카카오클라우드와 함께하는 다양한 서비스를 활용하여 빠르게 비즈니스를 시작하세요.	
	마켓플레이스 서비스 제휴 신청	
	Security (Data) (36) v	Q 검색어를 입력해주세요.
	[그림 1.2.1] 카카오클라우드 마켓플	레이스 상품 소개 페이지

- 4 참고 사항
- ▶ 카카오클라우드 마켓플레이스 소개



#### 1.3. 가상자원 루트 계정 접근 시 추가인증수단 제공

#### 1 기준

식별번호	기준	내용	
1 0	가상자원 루트 계정 접근 시	이용자 가상자원 루트 계정(root, administrator등) 접근	
1.5	추가인증수단 제공	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 Key를 통한 안전한 로그인 수단 확보 등

#### 3 우수 사례

1) 이용 고객은 1.1. 항목을 참고하여 SSH PEM Key를 통한 로그인 정책 적용 필요

#### 4 참고 사항

► N/A



#### 가상자원 생성 시 네트워크 설정 적용 1.4.

#### 기준 1

식별번호	기준	내용
1 /	가상자원 생성 시 네트워크	이용자의 가상자원 생성 시 안전한 네트워크 설정을 적용
1.4	설정 적용	하여야 한다.

#### 2 설명

▶ 외부에서 직접 접속이 불필요한 경우 내부 IP 또는 IP 대역에서만 접근할 수있도록 설정하여야 한다.

- (예시)
  - 1) 가상자원 접속 가능한 퍼블릭 IP(외부) 대역 점검 및 제거
  - 2) 접근 가능한 IP 또는 IP 대역대 설정
  - 3) VPC 및 보안 그룹을 통한 내부 네트워크 대역 접근 설정

#### 3 우수 사례

- 1) 가상자원에 연결된 퍼블릭 IP가 있는지 점검
- ▶ (Console) 'Dashboard' → 'Virtual Machine' → '인스턴스' 화면에서 노출되는 가상자원 목록에 "퍼블릭 IP" 가 연결되어 있는지 확인



iii kakao <b>cloud</b>	Q, 서비스 검색	🗣 kr-central-2 🗸 🗗 🗄 🕐 । Ĕ
Virtual Machine	Virtual Machine > 안스턴스	
프로젝트	인스턴스 시작 정지 제시작 정	제 제사작 종료 인스턴스 삭제 인스턴스 작업 > 인스턴스 생성
	필터 혹은 값을 입력해 주세요.	총 33 건 중 1-20 < 이전 다음 > 20 ~ 3
인스턴스	이름 수 ID 상태 유형 이미지 프라	이빗 IP 퍼블릭 IP 가용 영역 💠 생성일 💠
볼륨	De Contraction de California d	.16.3 🖆 - kr-central 2024.05.31 :
스냅샷	□ De charles M. Ballinks. E ⊘ Active m2a.2xlar 172	.16.5 🗇 - kr-central 2024.05.31 🗄
스냅샷 일정	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	.16.1 🗇 - kr-central 2024.05.31 🗄
키페어	Active m2a.4xlar 172	.16.5 🗁 - kr-central 2024.05.31 🚦
	□ Decoderation and the Code The Octive m2a.4xlar 172	.16.5 🗁 - kr-central 2024.05.31 🔅
	□ 172 m 2.4xlar 172	.16.1 🗁 - kr-central 2024.05.31 🗄
	□ Solution control _ To O Active m2a.large - 172	.16.3 🗁 - kr-central 2024.05.28 🗄
	🗌 🚥 🖬 📾 🔤 🐨 👘 🖉 Active t1i.medium 😲 Ubunt 172	.16.0 🗁 - kr-central 2024.05.28 🗄
	🗌 🖝 😌 Ubunt 172	.16.2 🗇 - kr-central 2024.05.27 🚦
1187171015 (2	🗌 🚥 🚥 🗘 Ubunt 172	.16.1 🗇 - kr-central 2024.05.22 🚦
가동자 사람은 15	🗌 🗰 under the analysis and the second seco	.16.3 🕞 210.109 🕤 kr-central 2024.05.22 🚦
[7	린 1 4 1] VM 이스터스 모로 조히 시 퍼블리	IP 여견 여브 화이
	<u>ㅋ 이 이에 근그</u> 근그 ㅋㅋ 포치 시, 피크ㅋ	$\square \square $

#### 2) 접근 가능한 IP 또는 IP 대역대 설정

▶ (3rd-party 제품) MarketPlace 상품 중 Security(Network) 상품 군에 해당하는 제품을 활용하여 접근 제어 설정

	소개	서비스	마켓플레이스	파트너	리소스	고객지원	기술문서	공공기관용 🦻	
SB3	ns Co., Ltd.					Penta S	ECURITY EN SOCIETY		
RedCastle	러 스즈에 너 내	요고 해이 기바 저	그 토제르 그쳤하여 기	조이 지그 다친 기비	IFOI 141	WAPPLES SA	프리케이션 디아에	트히디 왜 바하려(моь А	pplication Firowall WA
문용제제의 가슴 트워크 보안 솔 한 서버 보안 솔	= 푸푼에지 지 루션에서 탐지 루션입니다.	하지 못하는 공격 *	은 공세를 두천하여, 가 행위를 효과적으로 탐지	는의 지그리지 가는   및 차단할 수 있는	= 완벽	들다구드 원숭에서 법이 F)입니다. 특허받은 지능 SS) 등의 웹 공격에 대응 는 다기능 웹 보안 솔루션	들리카이션 포진에 형 탐지 엔진 COCE 하는 동시에 정보 유 연입니다.	득되면 집 영외득(Web A P™을 통해 SQL Injection ?출, 웹사이트 위변조, Boti	ppication Filewall, WA , Cross-Site Scripting( (봇) 부정행위를 방지하
Security (Net	work)			판매자 : SGA솔	루션즈	Security (Network)			판매자 : 펜타시큐리티
MONI	TOR					SEC	UI		
MONI	TOR	NPP				SEC	Generation Fir	ewall Virtual Editic	'n
MONI AIWAF-VE AIWAF-VE(API 솔루션인 AIWA 화벽입니다.	TOR PLICATION IN F의 가상화 버	NSIGHT Web App 전으로, 클라우드	lication-Virtual Edition 환경에 최적화 설계된 :	n)는 국내 웹 방화! 소프트웨어 형태의	벽 1위 1 웹 방	SEC BLUEMAX Next- BLUEMAX NGF VE는 i 등 차세대 방화벽의 다양 다.	Generation Fire 라우드 네트워크 5 한 보안 기능을 통하	ewall Virtual Editic 보안을 위한 차세대 방화벽 H 클라우드의 중요 정보 지	<b>)n</b> 입니다. 접근제어, VPN 원을 보호할 수 있습니
MONI AIWAF-VE AIWAF-VE(API 솔루션인 AIWA 화벽입니다. Security (Netw	TOR PLICATION IN F의 가상화 버 work)	NSIGHT Web App 전으로, 클라우드	lication-Virtual Edition 환경에 최적화 설계된 :	n)는 국내 웹 방화* 소프트웨어 형태의 판매자 : 모/	벽 1위 웹 방 니터랩	SEC BLUEMAX Next BLUEMAX NGF VE는 1 등 차세대 방화벽의 다일 다. Security (Network)	Generation Fir Beheration Fir B라우드 네트워크 5 한 보안 기능을 통하	ewall Virtual Editio 2만을 위한 차세대 방화벽 내 클라우드의 중요 정보 지	) <b>)</b> 입니다. 접근제어, VPN 원을 보호할 수 있습니 판매자 : 시큐아

#### 3) VPC 및 보안 그룹을 통한 내부 네트워크 대역 접근 설정

▶ (Console) 'Dashboard' → 'VPC' → '라우팅 테이블' 화면에서 확인할 라우팅테이블 선택 → 라우 팅 테이블 상세 페이지에서 라우팅 정보를 확인하여 불필요하게 외부에서 통신이 가능하도록 설정되어 있는 부분이 없는지 점검 (모든 대역을 목적지로 Internet Gateway 로 가도록 되어있는 설정 등)

× kakao <b>cloud</b>	Q 41	비스 검색		♦ kr-central-2 v	di 1 🕐 🗉 🗉
ⓒ 최근 사용			VPC		
\$\$ 전체 서비스	는데ㅋ프로 ㅋㅋ한 가장 패르워니를 가장할 수 있습니다.~		서브넷		
즐겨찾기 Beta	Load Balancing 사용자 환경에 적합한 실정을 통해 트래픽 분산을 최 <u>적회할 수 있습니다</u>		라우팅 테이블		
자주 사용하는 서비스를 목록에서 추가하세요.					
	CDN 대용량의 웹 콘텐츠를 많은 사용자들에게 빠르고 안점적으로 제공하는 네트	트워크 서비스입니다.	퍼블릭 IP		
카테고리			172.16.3. 0	kr central 2 e	2024.05.31
Beyond Compute Service	ONS 손쉽게 DNS 서버를 구축할 수 있고 빠른 응답속도와 안정성 높은 DNS 서비	비스를 제공합니다.	172.16.5. 0 -	kr central 2 b	2024.05.31
Beyond Networking Service >			172.16.1_ 0 -	kr central-2-a	2024.05.31
Container Pack	Transit Gateway 다수의 VPC와 온프레미스 네트워크를 연결하여 중앙 집중식으로 관리할 4	수 있습니다.	172.16.5. 0 -	kr-central-2-b	2024.05.31
Beyond Storage Service			172.16.5. 0 -	ke-central 2-b	2004.05.31
Data Store			172.16.1	ke-cardrai-2-a	2024.05.31
Developer Tools			172.16.3. 0 -	kr-central 2-b	2024.05.28
Analytics			- 172.16.0	kr central 2-a	2024.05.28
Management			- 172.16.2. 0 -	kr central 2-a	2024.05.27
AI Service			- 172.16.1 0 -	kr central 2 a	2024.05.22
Billing	· · · · · · · · · · · · · · · · · · ·			10.109	2024.05.22

[그림 1.4.3] 카카오클라우드 콘솔 〉라우팅테이블 서비스 이동

iii kakao <b>cloud</b>		Q 서비:	스검색	• kr-central	-2 -2 📑 🗐 (	9 · 📧
VPC	VPC > 라우팅 테이블 >	erris sale eduality (1925)				
프로젝트				on 175 pub 40 🗸		
VPC 서브넷	상태 ● Active	라우팅 테이블 ID	VPC cloudtech-vpc-172	기본에	생성일 2024.01.08 (월) 17:50	1
라우팅 테이블 보안 그룹						
퍼블릭 IP	라우팅 2 연결 1					
	라우팅 필터					+ 라우팅 추가
	목적지 🔶	대상 유형 🝦	대상 🔶		상태 💠	
	172.16.0.0/16	Local	Local		Active	:
	0.0.0/0	igw	Internet Gatev	zay	<ul> <li>Active</li> </ul>	:
사용자 가이드 🖄			1			
	[그림 1.4.4] 라의	2팅 테이블 상세	네 페이지에서 리	나우팅 정보를 획	인	



::: kakao <b>cloud</b>		Q	서비스 검색		♥ kr-central-2 ~	i i 🤉 🧯
🊱 VPC	VPC 〉 라우팅 테이블 〉	laf Wills-exclinities (sept				
프로젝트	6215±246-1037	48af 9606 ea304	Peellead (arin-mul	640 <b>·</b>		
VPC 서브넷	상태 ● Active	라우팅 테이블 ID	VPC	기본 아니오	생성일 2024.05.09 (목)	17:04
보안 그룹 퍼블릭 IP	라우팅 2 연결 0					
	라우딩 월터 목적지 수	대상 유형 🔶	대상 👙		상태 🔶	+ 라우팅 추가
	0.0.0.0/0	igw	Internet Gateway	/	● Active	:
	172.10.0.0/1b	Local	1		ے Active	2등 삭제
사용자 가이트 산		이브 저저 귀다	은 이테 Intern	ot Cotour	ᇱᆁᆋ	

 ▶ (Console) 'Dashboard' → 'Virtual Machine' → '인스턴스' 화면에서 확인할 인스턴스 선택 → '인스턴스 상세 페이지' 에서 '보인' 탭 → 인바운드에 대한세부 규칙 확인하여 의도하지 않은 인바운드 규칙이나 모든 대역에 대해 허용되어 있는 규칙이 없는지 점검

× kakao <b>cloud</b>	Q 서비스 검색		kr-central-	·2 ~ 🖽
<ul> <li>· 최근 사용</li> <li>· 전체 서비스</li> </ul>	Virtual Machine 사용자 환경에 적합한 다양한 유형의 서버를 구축할 수 있습니다.	-		-
즐겨찾기 Beta	VPC 논리적으로 격려된 가상 네트워크를 구성할 수 있습니다.		8 33 2 8 1 20	
사주 사용아는 시미스를 폭독에서 주가아세요.	GPU GPU	2.012	121.0	
카테고리	대규모 병렬 연산에 적합한 GPU 서버를 구축할 수 있습니다.	172.16.3 0		kroantral 20
Beyond Compute Service	Transit Gateway 다수의 VPC와 온프레미스 네트워크를 연결하여 중앙 집중식으로 관리할 수 있습니다.	172.16.5 ©		kr-central
Beyond Networking Service	the states a second of a second s	172.16.1_ 0		kr-central-, 20
Container Pack	Object Storage 안정상과 확장성이 높은 객체 스토리지입니다. 대용량, 대규모 데이터 처리에 최적화되어 있습니다.	172.16.5. 15		kr-central
Beyond Storage Service		172.16.5 0		kroentral., 20
Data Store	서분화된 리소스 접근 제어 및 권한 관리 가능을 제공합니다. 사용자의 역할에 맞는 리소스 접근 권한을 부여하고, 리소스를 안전하게 관리할 수 있습니다.	172.16.1 ()		kroentrai., 20
Developer Tools	Alert Center 카카오클라우드 콘솔 서비스에서 콘솔 사용자에게 알림을 보내기 위한 알림 정책 및 수신 채널을	172.16.3 0		kr-central 20
Analytics	통압 관리합니다.	172.16.0. 0		kr-central 20
Management	Coad Balancing 사용자 환경에 적합한 설정을 통해 트레틱 분산을 최적화할 수 있습니다.	172.16.2. 0	-	kr-cantral-, 20
[7]	임 1 / 6] 카카이크라이드 코소 \ Virtual Mach	ning 015		



iii kakao <b>cloud</b>			오 서비	스 검색			Ø kr-cent	ral-2 ~	1 L (	) I (
📑 Virtual Machine	Virtual Machine > 인스턴스 인스턴스			시작	정지 재시작	강제 재시작	종료 인스턴스	삭제 인스턴스	- 작업 ~ <u>인스턴</u>	언스 생성
프로젝트 Cloudtech-main >	· 필터 혹은 값을 입력해 주세요.						총 <b>33</b> 건 중 1-20	< 이전 다음	>   20 ~	. 0
인스턴스	이름 수	ID	상태	유형	이미지	프라이빗 IP	퍼블릭 IP	가용 영역 💠	생성일 수	
볼륨	k8se-cloudtech-f	5e35e604 喧	Active	m2a.2xlar	-	172.16.3 🖆	-	kr-central	2024.05.31	:
스냅샷	k8se-cloudtech-f	5e840d5c 🖻	Active	m2a.2xlar	-	172.16.5 🖻	-	kr-central	2024.05.31	:
스냅샷 일정	k8se-cloudtech-9	8f878f16 🖻	Active	m2a.4xlar	-	172.16.1 🖆	-	kr-central	2024.05.31	:
키페어	k8se-cloudtech-9	0c08d83a 🖆	Active	m2a.4xlar	-	172.16.5 🖆	-	kr-central	2024.05.31	:
	k8se-cloudtech-5	cb19fa63 🖆	Active	m2a.4xlar	-	172.16.5 🖆		kr-central	2024.05.31	:
	k8se-cloudtech-5	1f133730 🖻	Active	m2a.4xlar	-	172.16.1 🖻	-	kr-central	2024.05.31	:
	istio-kube-aae384	d1e2af87 🖻	Active	m2a.large	-	172.16.3 🖻	-	kr-central	2024.05.28	:
	vin-s3-sdk-test	9d170b79 🖆	Active	t1i.medium	😲 Ubunt	172.16.0 🖆	-	kr-central	2024.05.28	:
	erin-monitor-alert	a0d4d6a6 🖆	Active	m2a.large	😲 Ubunt	172.16.2 🖻	-	kr-central	2024.05.27	:
	erin-web	127cfc95 🖆	Active	m2a.large	😲 Ubunt	172.16.1 🖆	-	kr-central	2024.05.22	:
지하지 지하는 다	vin-websocket-cli	21ff071d 🖆	Active	t1i.medium	😲 Ubunt	172.16.3 🖆	210.109 🖆	kr-central	2024.05.22	:
	[그리	1 / 7]	이ㅅ터	ㅅ 사네	MOIT	12 이도				

iii kakao <b>cloud</b>			Q, 서비스 검색		kr-central-2	· d	i 🤊 🗉 🗉
Uirtual Machine	Virtual Machine > 인스턴스 >			시작 <b>정지 재시작 2</b>	강제 재시작 종료	인스턴스 삭제	인스턴스 작업 🗸
○ ·	세부 정보 네트워크	보안 2	볼륨 1 즈	방업 로그 모니터링			
볼륨 스냅샷	보안 그룹						보안 그룹 수정
스냅샷 일정	플 필터 혹은 값을 입력해 주세요.				총 <b>2</b> 2	번 중 1-2 < 이전	다음 > 2
이미지	이름			ID			
키페어	sg-external [2			20070/08-6766-4be3-9860	31aa3211a830 G		
	sg-internal 🖪			5a412944-0004-43x0-0x/2	2740a4586627 G		
	세부규칙						
	· 필터 혹은 값을 입력해 주세요.				총 12 7	변 중 1-5 < 이전	다음 >   S
	보안 그룹 💠	프로토콜 ≑	출발지 수		포트 번호 수	설명	
사용자 가이드 🖸	sg-external	ALL	(11-1-10)(11-10), (11-10)		ALL	artis-burria	
	P						
ב]_	림 1.4.8] 인 <u>스턴</u> :	스 상세 프	이지 〉 보	안 탭 〉 인 <u>바운</u>	드 규칙	확인	

인바운드 규칙 1	아웃바운드 규칙 1 연결된 리소스 0			
인바운드 규칙 필터				안바운드 규칙 관리
프로토콜 💠	출발지 💠	포트 번호 💠	정책 설명	생성일 🗘
TCP	@sg-internal	22	-	2024.06.18 (화) 17:05
			1	
	이 버야고드며취승	초바기그 서저	되어 됐다 H이너그르오 기지	기사대의드미아  저그하 스 이느 그런 새서



#### 4 참고 사항

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



#### 1.5. 가상자원 접속 시 보안 방안 수립

#### 1 기준

식별번호	기준			내용									
1 5	가상자원	접속	시브	보안	방안	이용자	가상자원	접속	시	안전한	인증절차를	통해	접속
1.0	수립					하여야	한다.						

#### 2 설명

▶ 이용자 가상자원(인스턴스) 접속 시 안전한 방식을 통해 접근하여야 한다.

- 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

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



× kakao <b>cloud</b>	Q, 서비스 검색		♀ kr-central-2	2 × 🗇
(한 최근 사용 >				
** 전체 서비스	704 E01 782 702 Tro- MME 1 42 T ME94.	211.011		-
즐겨찾기 Beta	VPC 논리적으로 격리된 가상 네트워크를 구성할 수 있습니다.		8 23 2 8 1 20	
자주 사용하는 서비스를 목록에서 추가하세요.	GPU GPU	2.002.0	-	
카테고리	대규모 병필 연산에 적합한 GPU 서버를 구족할 수 있습니다.	172.56.3. 0	- 1	kreattai. 20
Beyond Compute Service	Transit Gateway 다수의 VPC와 온프레이스 네트워크를 연결하여 중앙 집중식으로 관리할 수 있습니다.	172.14.5. 0	- 1	kr-central 25
Beyond Networking Service		172.16.1_ 0	- 1	kr-central-, 20
Container Pack	Object Storage 안정성과 확장성이 높은 객체 스토리지입니다. 대용량, 대규모 데이터 처리에 최적화되어 있습니다.	172.16.5 0	- 1	kr-central 20
Beyond Storage Service		172.16.5 0	- 1	kr-central
Data Store	제문화한 리조스 접근 세너 및 견안 관리 가중을 제공합니다. 사용사의 역할에 맞은 리조스 접근 권한을 부여하고, 리초스를 안전하게 관리할 수 있습니다.	172.16.1 ()	- 1	kroentral-, 20
Developer Tools	Alert Center 카카오클라우드 콘솔 서비스에서 콘솔 사용자에게 알림을 보내기 위한 알림 정책 및 수신 채널을	172.16.3. 0		kr-central
Analytics	동법 관리합니다.	172.16.0 15	- 1	kr-central
Management	Load Balancing 사용자 환경에 직합한 설정을 통해 트레픽 분산을 최적화할 수 있습니다.	172.16.2. 0		kroantral. 20

[그림 1.5.1] 카카오클라우드 콘솔 > Virtual Machine 서비스 이동

iii kakao <b>cloud</b>		〇、서비스 검색	♀ kr-cer	ntral-2 · 🗄 🗄 🤈 ၊ Ĕ
📫 Virtual Machine	Virtual Machine > 키페어			
프로젝트	21 페이		핑거프린트 조회	퍼플릭 키 조회 기 페이 삭제 키 페어 생성
	😓 필터 혹은 값을 입력해 주세요.			총 1 건 중 1-1 < 이전 다음 > 🛛 🗘
인스턴스	이름 수	유형 💠	현재 프로젝트 내 연결된 리소스 🎯 생성일 🗧	
불물	le2-clinathech	SSH	5개 ~ 2023.11	2.22
스냅샷				핑거프린트 조회
스냅샷 일정				퍼블릭 키 조회
이미지				키 페어 삭제
키페어				
사용자 가이드 🖒				
[그림	1.5.2] 키 페어 관리 화	<u>면 (별</u> 도의 I	나운로드 기능은 제공히	하지 않음)

2) 최초 키페어 생성 시에만 PEM키가 자동으로 다운로드가 할 수 있다.

▶ PEM키에 대한 관리는 이용자 영역이며, 추가 다운로드는 불가하므로 관리 시 주의가 필요하다.

Virtual Machine         Virtual Machine         기 페어           프로젝트         기 페어 생성           인스턴스         여러           별함         kr2	<ul> <li>신규키페어생성하기 기존키업포드하기</li> </ul>	정기프린트 초회 X 생성월 수	퍼블릭 키 조회 총 1 건 중 1-1	키페이 삭제 <b>키페이 중성</b> < 이전 다음 > <b>오</b>
프로젝트	<ul> <li>신규키페어생성하기 기존키업모드하기</li> </ul>	· 생성일 수	총 1 건 중 1-1	< 이전 다음 > [2]
전스턴스 ···································	<ul> <li>신규 키 페어 생성하기</li> <li>기존 키 업로드하기</li> </ul>			
스냅샷		2023.12	.22	:
스냅샷 열정 이용	test			
키 페아 유형 성장	SSH v	- 10		
	취소생성			
사용자 가이드 ሪ				

[그림 1.5.3] 최초 키 페어 생성

🔅 Virtual Machine	Virtual Machine ⇒ श ≋[0] ⊐ा म्यो Ω J	키 페어 생성에 성공하였습니다.		<b>test.pem</b> 1,6798 · 砂星	
프로젝트	기 비나이 코티 혹은 값을 입력해 주세요.			영거프린드 조와 아파 파를백 커 조와 총 2 건 중 1-2	< 이전 다음 > (C
인스턴스	이름 ≑	유형 수	현재 프로젝트 내 연결된 리소스 🕤	생성일 💠	
볼륨	test	SSH	0 개 ~	2024.06.02	:
스냅샷 스냅샷 일정	<ul> <li>kit staatiet</li> </ul>	SSH	5 개 ㆍ	2023.12.22	:
	[그림 1.5.4] 최	초 키 페어 생성 시 P	EM Key 자동	다운로드	



- 3) 가상자원관리시스템에서 콘솔을 통해 이용자의 인스턴스에 직접 접속하는 방법은 제공하지 않는다.
- ▶ (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 않는다.



kakao <b>cloud</b>				C	Q, 서비스 검색				kr-central-2 ~		(?)
Virtual Machine	Virtual Ma	chine > 인스턴스									
L	인스틴	<u> 1</u> 스				시작 정지	재시작 강제 지	시작 중료	인스턴스 삭제 인:	스턴스 작업 👻	<mark>신스턴스 (</mark>
doutlech main	포 필터	혹은 값을 입력해 주세요.						총 <b>33</b> 건	· 중 21-33 < 이전	다음 > 20	~
턴스		이름 💠	ID	상태	유형	0 0 7	프라이빗 IP	퍼블릭 IP	가용 영역 💠	생성일 💠	
		david field	76687774. G	Active	t1i.small	😲 Ubuntu 2	172.16.49 🗈	-	kr-central-2-b	2024.05.16	
£		err-dashboard	0xx140.0x04. 10	Active	m2a.large	😲 Ubuntu 2	172.16.2.2 🗈	-	kr-central-2-a	2024.05.16	
· 일정		Mar-cloudech-4440.	1753663-3. 6	Active	m2a.large		172.16.34 🗈	-	kr-central-2-b	2024.05.10	
и		policy-win1	1349473-0s	Active	m2a.large	Windows	172.16.1.1 🗈		kr-central-2-a	2024.05.09	
		policy-mat	e5446349-68. 15	Active	m2a.large	😲 Ubuntu 2	172.16.0.93 🗈		kr-central-2-a	2024.05.09	
			0630854x-55. To	Active	m2a.large	😲 Ubuntu 2	172.16.35 🖻	-	kr-central-2-b	2024.04.23	
		ern-monttoring		Active	m2a.large	🗘 Ubuntu 2	172.16.0.1 🗈		kr-central-2-a	2024.04.23	
		with only test policy	10:10:10-45. Fg	Active	m2a.large	🗘 Ubuntu 2	172.16.3.27 🗈		kr-central-2-a	2024.04.16	
		tel-object-agi-poby	Cuto 19-6. G	Active	m2a.large	😲 Ubuntu 2	172.16.1.65 🖻		kr-central-2-a	2024.04.11	
		en-le2 cloudinch-ba.	ringer. G	Active	m2a.xlarge	😲 Ubuntu 2	172.16.3.2 🗈	-	kr-central-2-a	2024.03.29	
사용사 가미는 亿			Jablaadt es., To	Active	t1i.large	💠 CentOS	172.16.0.1 🖻		kr-central-2-a	2024.02.13	



: Kakao <b>cloud</b>					Q.4	비스 검색			Q kr-cen	tral-2 ~	- 1 1 0 ∣
Virtual Machine	Virtual Ma 인스틴	achine > 인스턴스 턴스				시작	정지 제	시작 강제 재시작	종료 인스턴스	- 삭제 인스	시작 <b>정지</b>
s cloudlesh main	는 필터	혹은 값을 입력해 주세요.							총 <b>33</b> 건 중 21-33	< 이전	재시작
인스턴스		이름 수	ID		상태	유형	이미지	프라이빗 IP	퍼블릭 IP	가용 영역 💠	강제 재시작
差帚		david level	79464195-	6	Active	t1i.small	😲 Ubuntu	172.16.4 🗈		kr-central-2	종료
스냅샷		erin-destributed	Gertfilde.	6	Active	m2a.large	🔿 Ubuntu	172.16.2 🖆	-	kr-central-2	인스턴스 이름 변경
스냅샷 일정		kfræ-cloudhech-44.	12538443	6	Active	m2a.large	-	172.16.3 🗈	-	kr-central-2	인스턴스 유형 변경
		profity-write1	85488721	6	Active	m2a.large	Windo	172.16.1 🖆	-	kr-central-2	보안 그룹 수정
1 401		perfery-real	e54a6346	6	Active	m2a.large	🗘 Ubuntu	172.16.0 🗈		kr-central-2	퍼블릭 IP 연결
		e11-114/16	b630854a	6	Active	m2a.large	🔿 Ubuntu	172.16.3 🖻	-	kr-central-2	퍼블릭 IP 연결 해제
		eth-munitoring	o463c24 <sup>b</sup> .	5	Active	m2a.large	🗘 Ubuntu	172.16.0 🖆	-	kr-central-2	출발지/목적지 확인 변경
		ada-ong-tent-polity	Melaelle.	6	Active	m2a.large	🗘 Ubuntu	172.16.3 🖻	-	kr-central-2	SSH 면결
		w2-stipsch ago potty	Cata19b.	5	Active	m2a.large	🗘 Ubuntu	172.16.1 🗈		kr-central-2	시스템 로그 보기
		en-le2-cloudhech	7179bd7a	6	Active	m2a.xlarge	🔿 Ubuntu	172.16.3 🖻	-	kr-central-2	이미지 생성
사용자 가이드 🖸			Sufficient?	5	Active	t1i Jarge	CentOS	172 16 0		kr-central-2	인스턴스 삭제

III kakao <b>cloud</b>			×	kr-central-2 v	- i ?	I E
Virtual Machine	Virtual Machine > 인스 인스턴스	<b>SSH 연결</b> SSH 연결을 위한 자세한 설명은 <b>사용자 가이드를</b> 참고하시길 바랍니다.	~	중료 인스턴스 삭제 인스턴	스작업 ~ 인스턴:	스 생성
프로젝트		<ol> <li>인스턴스를 시직한 후, 연결할 수 있도록 인스턴스가 준비될 때까지 몇 분 정도 걸릴 수 있습니다. 인스턴스가 상태가 Active인지 확인합니다.</li> </ol>		5 <b>33</b> 건 중 21-33 < 이전 대	≧ →   20 ~	S
인스턴스 볼륨	이름 \$	<ol> <li>인스턴스의 퍼블릭 DNS 이름 또는 퍼블릭 IP 주소와 인스턴스에 연결하는 데 사용 해야 하는 사용자 이름(ubuntu)을 확인합니다.</li> </ol>		퍼블릭 IP 가용 영역 수 - kr-central	생성일 令 2024.05.16	:
스냅샷 스냅샷 일정	-	<ol> <li>인스턴스와 인센원 모던 그들의 인바운드 정색에 TCP 22만 포트가 허용되어 있는지 확인합니다.</li> <li>david test 에 성정되 ks 2slautteek pers 파인은 증비한 ICt</li> </ol>		- kr-central	2024.05.16	:
이미지	- Marcin	4. Gandreest 에 글 8년 N*2ChouleChipen 적 글 8 번 일 다 일 다. 5. 터미널 또는 별도의 SSH 클라이언트를 실행합니다.		- kr-central	2024.05.10	:
키 페어	- poly-cal	6. kr-2cloudtech.pem 파일이 있는 경로에서 아래 명령어를 실행합니다. ssh -i kr-2cloudtech.pem ubuntu@172.16.49.98 톱		- kr-central	2024.05.09	:
		만약 프라이빗 키의 권한 문제가 발생하는 경우 사용자만 해당 파일을 읽을 수 있도록 다음 명령으로 권한을 설정합니다.		- kr-central	2024.04.23	:
		chmod 400 kr-2cloudtech.pem Fa		- kr-central - kr-central	2024.04.23 2024.04.16	:
				- kr-central	2024.04.11	:
사용자 가이드 亿		닫기		- kr-central	2024.03.29	:
		[그림 1.5.8] SSH 연결 가이드 확인		- kr-central	2024.02.13	1

#### 4 참고 사항

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

#### 1.6. 이용자 가상자원 별 권한 설정

#### 1 기준

식별번호	기준	내용
1.6	이용자 가상자원 별 권한 설정	이용자 직무 및 권한에 따른 가상자원 별 접근통제 방안
		(권한 설성 능)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 기능 제공
- ▶ 상위 개념의 공간인 조직에는 조직소유자(owner), 조직관리자(admin), 조직리더(view) 등의 권한으로 구분. 조직소유자는 조직마다 1명만 존재하며, 권한 이양 가능
- ▶ 조직 하위의 개념인 프로젝트는 실질적인 자원을 생성하고 관리하는 공간이며, 관리자(admin), 멤버 (member), 리더(viewer) 권한으로 구분
- ▶ 가상자원 접근(SSH, RDP 등)에 대한 제어는 마켓플레이스 상품을 통해 이용할 수 있으며, 다양한 접근제어솔루션을 활용하여 유저 및 그룹별 접근통제 기능 제공
- 1) 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



× kakao <b>cloud</b>	Q, 서비스 겸세	🗣 kr-central-2 🗸 🖪 🤄 🗉 🗉
<ul> <li>최근 사용</li> <li>** 전체 서비스</li> </ul>	AM 세분화된 리소스 집근 제이 및 관한 관리 기능을 체공합니다. 사용자의 역할에 맞는 리소스 집근 권원을 부여하고, 리소스를 안전하게 관리할 수 있습니다.	
즐거찾기 Beta	(monitoring) 에트릭, 로그 기반의 정택을 실정하여 컴퓨팅 리소스의 상태와 변화를 고니터링 할 수 있습니다.	
자주 사용하는 서비스를 목록에서 추가하세요. 	Alert Center 카카드릴라우드 문송, 서비스에서 문송, 사용자에게 업질을 보내기 위한 압밀 정책 및 수신 체념을 통합 관리합니다.	
Beyond Compute Service	Cloud Trail 사망지의 활동을 저주으로 수집, 기록하는 서비스입니다. 로그인, 리소스 성성, 변경, 삭제 등의 활동을 관련하게 주제, 관리법 수 있습니다.	84 x7c
Beyond Networking Service Container Pack		201.0.2
Beyond Storage Service		2014.25.26
Data Store		
Developer Tools Analytics		
Management >		
AI Service		Î
Billing		Bare Metal Server

#### [그림 1.6.1] 카카오클라우드 콘솔 > IAM 서비스 이동

iii kakao <b>cloud</b>		Q. 서비스 검색	Ç kr-central-2 ∽ □	i ? • E
😤 іам	IAM > 프로젝트 구성원			
프로젝트	프로젝트 구성원 🖂			
프로젝트 구성원	프로젝트 레벨 역할 10 그 1	류 권한 0		
서비스 계정	프로젝트 레벨 역할: 전체 💙		아이디를 입력 후 엔터를 누르세요. Q	+ 프로젝트 레벨 역할 관리
ক্রম <b>৫</b>	닉네임 (이름)	사용자 아이디 🔶	프로젝트 레벨 역할 💿	
프로젝트		faction of physical strengths and	프로젝트 관리자 (Admin)	:
사용자 그룹	E		프로젝트 관리자 (Admin)	:
역할 조직 관리			프로젝트 관리자 (Admin)	:
		$\int_{0}^{\infty} - \nabla f (x) = \int_{0}^{\infty} \int_$	프로젝트 관리자 (Admin)	:
사용자 가이드 간			프로젝트 관리자 (Admin)	:
	[그림 1.6.2] <u>프로</u> 직	텍트 구성원 중, 프로젝트	레벨 역할 확인	



iii kakao <b>cloud</b>		Q, 서비스 검색	🍳 kr-central-2 🗸 📑 🚺 🕧 🗉
🙈 іам	IAM > 프로젝트 구성원		
프로젝트	프로젝트 구성원 🖂		
프로젝트 구성원	프로젝트 레벨 역할 10 그룹	권한 0	
서비스 계정	프로젝트 레벨 역할: 전체 🛛 🗸		아이디를 입력 후 엔터를 누르세요. Q + 프로젝트레벨 역할 관리
ক্রম্ব <b>নে</b>	닉네임 (이름)	사용자 아이디 💠	프로젝트 레벨 역할 💿
프로젝트		david am@hakaoanterprise.com	프로젝트 관리자 (Admin)
사용자 그룹		eris official assertion price com-	프로젝트 관리자 (Admin) 프로젝트 레벨 역할 관리 프로젝트 관리자 (Admin)
역할 조직 관리	1 mm 2 (***23)	ian 2004alaonetiarpeisa com	프로젝트 관리자 (Admin)
	J planes (planes)	pl.new@kakacenterprise.com	프로젝트 관리자 (Admin)
사용자 가이드 간	J prosph 87 (prosph 87)	prosph 57 ghahacomterprise com	프로젝트 관리자 (Admin)
	[그림 1.6.3] 부적	[절하게 권한이 부여된 경	우 역할 변경

iii kakao <b>cloud</b>			Q, 서비스 검색			kr-central-2 ~	
🙈 IAM	IAM 〉 프로젝트 구성원						
프로젝트	프로젝 👝	프로젝트 레벨 역	할 관리		×		
프로젝트 구성원	프로젝. 프로젝	4E (1997)	ech-main (cloudlech-main)				
지미스 계정	프로젝트 레뷔 사용7	하아이다.	progikakaserterprise.com			를 누르세요.	Q + 프로젝트 레벨 역할 관리
d	<u></u> <u></u>	<b>빅트레벨역할 </b> ② 할당할	역할			프로젝트 레벨 역할 🌍	
프로젝트		프로	젝트 관리자 (Admin)	~ I	Ū	프로젝트 관리자 (Admi	in) :
그룹		+	프로젝트 레벨 역할 추가			프로젝트 관리자 (Admi	in) :
역할 조직 관리			취소 다음			프로젝트 관리자 (Admi	in) :
		ne (d. nee)	yî newîjî deserterpine som			프로젝트 관리자 (Admi	in) :
사용자 가이드 (2		ph.87 (paugh.87)	joseph E <sup>n</sup> gkakasenterprise on			프로젝트 관리자 (Admi	in) :
	[=	1.6.4]	프로젝트 레벨 역할	할 변경 모들	ł		

#### 2) 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

③ 최근 사용       IAM       세분확실 리소스 접근 체어 및 권할 관이 가능을 체공합니다. 사용자의 여할에 맞는 리소스 접근 권한 관계하고, 리소스 월 간원에 끼리할 수 있습니다.         값 전체 서비스       Image: Compute Service       Image: Compute Service       Image: Monitoring 이 때트릭, 로그 기반의 정책을 실정하여 컴퓨팅 리소스의 상태와 변화를 모니터릭 할 수 있습니다.         자주 사용하는 서비스를 목록에서 추가하세요.       Image: Compute Service       Image: Compute Service       Image: Compute Service         Beyond Compute Service       Image: Compute Service       Image: Compute Service       Image: Compute Service	
제가 비해         Monitoring 예트 리, 로그 기반의 정책을 실정하여 협류된 리소스의 상태야 변화를 모니터짐 할 수 있습니다.           시주 시청하는 서비스를 적목해서 추기하세요.	
지주 사용하는 서비스를 탁록에서 추가하세요. 위하고 레이 위치 : 문을 마우드 구축 서비스에서 문출 사용자에게 양업을 보내기 위한 양집 정책 및 수신 체념을 통합 카테고 레이 문 프 카리 : 문 프 카리 : 문 프 카리 : 문 프 카리 : 문 프 프 카리 : 문 프 프 프 프 프 프 프 프 프 프 프 프 프 프 프 프 프 프	
Beyond Compute Service Cloud Trail 신왕지역 함동물 자동으로 수집, 기록하는 시비스입니다. 로그인, 리소스 생성, 범정, 삭제 등의 활동을 건강하여 자목, 고리할 수 있습니다.	
Revand Networking Service	
Container Pack	
Beyond Storage Service	
Developer Tools	
Analytics	
Management >	
Al Service Elements of the server of the ser	

#### [그림 1.6.5] 카카오클라우드 콘솔 > IAM 서비스 이동

iii kakao <b>cloud</b>			Q 서비스 검색	Global	d 1	() I
😤 IAM	IAM >	> 사용자				
프로젝트	사용	<b>자</b>				+ 사용자 등록
○ > 프로젝트 구성원	조직 레	넬 역할: 전체 💙		010121	물입력 후 엔터를 누르세요.	Q
서비스 계정		닉네임 (이름)	사용자 아이디 👙	조직 레벨 역할	그룹 역할 💿	
조직 <b>대</b>		3 -	Metgdgfftestel com	역할 없음	역할 없음	:
프로젝트		-	abbygal ine@kakacerterprise.com	조직 관리자 (Admin)	역할 없음	:
사용자 그룹		A -	after z@kakacenterprise.com	역할 없음	역할 없음	:
국일 조직 관리			alt +3-05y849xgpropriat com	역할 없음	역할 없음	:
		•	antros changgitalianente prisa com	조직 소유자 (Owner) 조직 관리자 (Admin) 빌링 관리자 (Admin) 빌링 매니저 (Manager) 트레일 뷰어 (Viewer)	역할 없음	:
사용자 가이드 🗅				<u>조직 리더 (Reader)</u>		
		[그림 1.6.6] 조직	구성원 중, 조직 레	벨 역할 확인		



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

#### 4 참고 사항

은젝트	사용자	3				┝ 사용자 등
› · ·	조직 레벨 역원	💼 조직 레벌	J 역할 추가		디를 입력 후 엔터를 누르세요.	
너비스 계정		조직 레벨 역할은 IAM 빌링 역할은 Billing /	역할(조직, 빌링, 프로젝트)을 추가 및 삭제할 수 있습니다. H비스에서 리소스 사용량 및 요금을 조회합니다. I <mark>AM 기본 역할 자세히 보기</mark> (	3	그룹 역할 💿	
9 D	0	조직	kalkanic/loud r			
프로젝트		사용자 아이디	abbygal lee jikaka serierprise.com	in)		
사용자 그룹 격화	•	조직 레벨 역할 설정	할당할 역할 조직 레빌 역할 선택	~ 1		
조직 관리			치소 다음			
	- 6		andrea chang@akasenterprise.com	er) in) 빌링 관리자 (Admin) 빌링 매니저 (Manager) 트레일 뷰어 (Viewer)		

22

ii kakao <b>cloud</b>		Q 서비스 검색	© Global		빈 () '
IAM	IAM > kakaoicloud-r > 사용자				
찍트	사용자 💿				+ 사용자
cloudtech-main > 로젝트 구성원	조직 레벨 역할: 전체 💙		01010	를 입력 후 엔터를 누르세요.	
너비스 계정	닉네임 (아름)	사용자 아이디 💠	조직 레벨 역할	그룹 역할 📀	
] kakaoicloud-r	a .	34etgdg@testef.com	역할 없음	역할 없음	
프로젝트	• •	abbygail.lee@kakaoenterprise.com	조직 관리자 (Admin)	역할 없음	
사용자 고룹	■ ▲ ·	adler.z@kakaoenterprise.com	역할 없음	야할 없음 조	용자 정보 직 레벨 역할 추기
4할 5직 관리	A andy.test.user (andy.test.user)	alt.v3-bby84hx@yopmail.com	역할 없음	역할 없음	되 레벨 역할 삭제
	· ·	andrew.chang⊚kakaoenterprise.com	조직 소유자 (Owner) 조직 관리자 (Admin) 빌링 관리자 (Admin) 빌링 매니저 (Manager) 트레일 뷰어 (Viewer)	역할 없음	<u></u> \$사 삭제
사용자 가이드 亿			조직 리더 (Reader)		

#### 1.7. 이용자 가상자원 내 악성코드 통제방안 수립

#### 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

- 1) 이용자가 보유하고 있는 악성코드 통제방안 수립
- ▶ (3rd-party 제품) MarketPlace 상품 중 security(endpoint) 상품 군에 해당하는 제품을 활용하여 악성코드 통제 가능

kakao <b>cloud</b>	소개	서비스	마콋플레이스	파트너	리소스	고객지원	기술문서	공공기관용 💌	Consol	a 회원가입
	Marketi	이미지 에하는 다양 니작하세요.	<b>)</b> 향한 서비스를 활용	올하여						
	마켓플레이스 서비스	제휴 신청								
										요금계산기
	Security (Endpoint) (9)	~ )						Q 검색어를 입력해주세요.	<i>'ମ</i> . ୪୮	남 및 도입 문의
	[그림	1.7.1	카카오	클라우	드마	<u> 겟플레이</u>	스 상품	소개 페이지		



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

kakao <b>cloud</b>	소개 서비스 [	가켓플레이스 파트너 리소스	고객지원 기술문서	공공기관용 🛪	Console 회원가입
	Service <b>Security</b> 고객의 서비스와 데이터를 안전하기	보호할 수 있도록 강력하고 다양한	보안 서비스를 제공합니다		-
	DDoS Defender IDS Managed Se	curity			
	세비스 개요 IDS 고객의 카카오클라우드 인프라를 더	시비스 상으로 하는 침해 시도를 탑지하는	특징 서비스입니다.	<b>ਉ</b> ਰੋ	
	[그림 1.7.2	] 카카오클라우!	E IDS 상품	소개 페이지	

- 카카오클라우드 > Security > Managed Security (보안관제)

kakao <b>cloud</b>	소개 서비스 마켓플레이스	파트너 리소스 고객지원 기	술문서 공공기관용 >	Console 회원가업
	Service <b>Security</b> 고객의 서비스와 데이터를 안전하게 보호할 수 있도	드록 강력하고 다양한 보안 서비스를 제공	합니다.	
	DDoS Defender IDS Managed Security			
	서비스 개요	서비스 특징	52	
	Managed Security	안 관제 서비스입니다.		
	1리 1 7 2] 카카이크라이	E Managad See	urity 사프 ᆺ거 <mark>니 페</mark> (	ודור
	<u>[림 1.7.3]</u> 카카오클라우.	느 Managed Sec	urity 상품 소개 페(	기시



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

		E	
그개니	NC 또한편제 이번	:=	
고 객 자 타 지 며			
님 시 영 탄 지 루		Malware Alert	
탐지 일시		위험 등급	MEDIUM
티켓 번호	CONTRACTOR NOT A CRUCK OF		
출발지 IP		출발지 PORT	
목적지 IP	and the second second second second	목적지 PORT	1000
탐지 장비	I	DS	
이벤트 정보	타지근거 : hacktool_GyptoCurrency_Ininer_Connection [취약점 설명] - 'hacktool_Monero_Miner''는 Monero 암호화폐를 다. 이 악성코드는 주로 이메일 첨부 파일이내 피싱 링크를 hacktool_Monero_Miner는 시스템의 CPU, GPU, 메모리 능이 저하될 수 있습니다. [영향도 분석 결과] - 굴 활동 확인되며, 추가 공격 예방을 위해서 '	채굴하기 위해 시스템 리소스를 통해 유포됩니다. 한번 시스템에 등을 사용하여 Monero를 채굴힙 .악성코드채 .차단하였습니다.	사용하는 악성코드입니 침입하면, File- 니다. 이로 인해 시스템 성 굴 소프트웨어를 통한 채
공격 구문	Packet:		52530
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 Sect - 임시 폴더 내 악성 의심 파일 제거 - 작업 스케줄러 내 미사용 또는 악성 의심 작업 제거 - 백신 정밀 검사 권고	rity Group 강화 권고	



#### 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 사설 IP 주소 할당 및 관리
- 2.6. 네트워크(방화벽 등) 정책 주기적 검토





#### 2.1. 업무 목적에 따른 네트워크 구성

#### 1 기준

식별번호	기준	내용
2.1	업무 목적에 따른 네트워크 구성	클라우드 환경 내 업무 목적*에 따른 네트워크를 구성 하여야 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) 또는 NACL(Network ACL) 등의 기능을 통한 네트워크 구성 및 통제(인/아웃바운드 통제 등)



#### 3 우수 사례

#### 1) 업무 목적에 따른 네트워크 구성 예시



#### 2) VPC 등 네트워크 관련 기능을 통한 네트워크 구성 및 통제

- ▶ 업무 목적에 따라 하나의 프로젝트에 여러 개의 VPC를 구성한다. 예를 들어 네트워크/보안을 위한 VPC, 개발 환경용 VPC, 운영 환경용 VPC를 각각 생성하여 목적에 맞게 네트워크를 분리 구성한다.
- ▶ (Console) 'Dashboard' → 'VPC' → 'VPC 생성' 기능을 통해 업무 목적에 따라 여러 VPC를 생성한다.

× kakao <b>cloud</b>	Q. 시비스 검색	♥ kr-central-2
① 최근 사용		
\$\$ 전체 서비스		
즐겨찾기 Beta	Load Balancing 사용자 환경에 적합한 실정을 통해 트래픽 분산을 최적화할 수 있습니다.	
자주 사용하는 서비스를 목록에서 추가하세요.	CDN	
카테고리	내용양의 웹 관련츠를 많은 사용자들에게 빠르고 안정적으로 제공하는 네트워크 서비스입니다.	
Beyond Compute Service	DNS 손쉽게 DNS 서비를 구축할 수 있고 빠른 용답속도와 안정성 높은 DNS 서비스를 제공합니다.	84 M.1
Container Bask	Transit Gateway	
Bevond Storage Service	다수의 VPC와 온프레미스 네트워크를 연결하여 중앙 집중식으로 관리할 수 있습니다.	2014.04.08
Data Store		2014.01.05
Developer Tools		
Analytics		
Management		
Al Service		Î
Billing		Bare Metal Server

#### [그림 2.1.2] 카카오클라우드 콘솔 > VPC 서비스 이동

iii kakao <b>cloud</b>		Q, 서비스 검색		• kr-central-2	· 1	1 ? · E
🏟 урс	VPC > VPC					
프로젝트	VPC Ø					+ VPC 생성
VPC	VPC 필터					
서브넷	VPC \$	상태 💠	IP CIDR 블록 💠	서브넷 ≑	기본 VPC 🛊	
라우팅 네이를 보안 그룹	devalues appendix app	<ul> <li>Active</li> </ul>	172.16.0.0/16	4개	ଜା	:
퍼블릭 IP		1				
사용자 가이드 亿						
	[그림 2.1.3	8] VPC 생성 버	튼 클릭			



::: kakao <b>cloud</b>		Q, 서비스 검색		Q kr-central-2 ↔	di 1 () - E
🚱 VPC	VPC > VPC > VPC 생성				
프로젝트	VPC 생성				
> > VPC					
서브넷	VPC 정보	VPC 이름			
라우팅 테이블		알파벳 대소문자(a-z, A-Z), 숫자(0-9), ''만 입력 (4~200자)			
보안 그룹		VPC IP CIDR 블록			
퍼블릭 IP		10.0.0/16	65,520개 사용 가능		
		VPC는 CIDR 행식으로 안약 가능하며, 취용되는 것은 아래하 관습니다. VPC의 IP-44 CIDR 발록 크기는 /16 - /24 북해스크여의 합니다. 10.0.00 - 10.255 236 255 (10.0.008) 172 16.0.0 - 172 31 255 255 (172.16.0.072) 192 168.0.0 - 192 168 255 255 (192.168.0.0746)			
	Availability Zone	가용 영역 개수			
사용자 가이드 亿		취소	생성		
		[그림 2.1.4] VPC 생성	페이지		

▶ (Console) 'Dashboard' → 'Transit Gateway' → 'Transit Gateway 생성' 기능을 통해 Transit Gateway를 생성하여 서로 간에 통신이 필요한 VPC를 연결한다.

× kakao <b>cloud</b>	Q. 서비스 검색	🗣 kr-central-2 🗸 🗗 🚹 🕐 🗉 Ĕ
④ 최근 사용		
💲 전체 서비스		
즐겨찾기 Beta	Load Balancing 사용자 환경에 직합한 설정을 통해 트래픽 분산을 최적화할 수 있습니다.	
자주 사용하는 서비스를 목록에서 추가하세요.		**
카테고리	대용량의 웹 콘텐츠를 많은 사용자들에게 빠르고 안정적으로 제공하는 네트워크 서비스입니다.	
Beyond Compute Service	DNS 손쉽게 DNS 서버를 구축할 수 있고 빠른 용답속도와 안정성 높은 DNS 서비스를 제공합니다.	84 M/10
Beyond Networking Service >		
Container Pack	Transit Gateway 다수의 VPC와 온프레미스 네트워크를 연결하여 중앙 집중식으로 관리할 수 있습니다.	Billing and State of
Beyond Storage Service		2024.05.28
Data Store		2014.0.2
Developer Tools		
Analytics		
Management		
Al Service		
Billing		Bare Metal Server
「기릳	2 1 5] 카카오킄라오드 코속 > Transit (*	Gateway 서비스 이동



iii kakao <b>cloud</b>	Q. 세비스 컴M - • 대 표 · · · · · · · · · · · · · · · · · ·
💮 Transit Gateway	Transit Gateway > Transit Gateway
프로젝트	Transit Gateway (2)
Transit Gateway	
Attachment	
라우팅 테이블	
	Transit Gateway가 없습니다.
사용자 가이드 간	
-	

#### [그림 2.1.6] Transit Gateway 생성 버튼 클릭

III kakao <b>cloud</b>		Q. 서비스 뀹색	9 kr-central-2 · E	
Transit Gateway Transit	isit Gateway > Transit Gateway			
프로젝트 <b>T</b>			+ Transit Gateway 생성	
C · · · · ·	Transit Gateway	생성	×	
Attachment	Transit Gateway 이름	알파벳 대소문자(a-z, A-Z), 숫자(0-9), '만 입력 (4~250자)		
라우팅 테이블	기본 연결	실정 라우팅 테이블에 Attachment가 자용으로 연결됩니다.		
		● 저중 다른 프로젝트의 Attachment 추가를 자동으로 하용합니다.		
	공유 수락 설정	● 수용 다른 프로젝트의 Attachment 추가을 수용으로 권리합니다.		
		위소 생정		
사용자 가이드 (2				
[그림 2.1.7] Transit Gateway 생성 페이지				

- 3) 보안그룹(Security group) 또는 NACL(Network ACL) 등의 기능을 통한 네트워크 구성 및 통제(인/아웃바운드 통제 등)
- ▶ 하나의 VPC에서도 업무 목적에 따라 Subnet을 구분하여 구성할 수 있다.
- ▶ (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 사용한다.



금융보안원

× kakao <b>cloud</b>	오, 서비스 검색	🍳 kr-central-2 🗸 🗗 🧵 🕐 🗉 🗉
③ 최근 사용	응 VPC	
** 전체 서비스		
즐겨찾기 Bets	사용자 환경에 적합한 실정을 통해 드래픽 분산을 최적화할 수 있습니다.	
자꾸 사람이는 시미드를 속속에서 두가하세요. 	CDN 대용량의 웹 콘텐츠를 많은 사용자들에게 빠르고 안정적으로 제공하는 네트워크 서비스입니다.	
Beyond Compute Service		
Beyond Networking Service >		
Container Pack	Transit Gateway 다수의 VPC와 은프레미스 네트워크를 연결하여 중앙 집중식으로 관리할 수 있습니다.	2004.01.01
Beyond Storage Service		2024.05.28
Data Store		2004-05.08
Developer Tools		
Analytics		
Management		
Al Service		۱
Billing		Bare Metal Server

#### [그림 2.1.8] 카카오클라우드 콘솔 > VPC 서비스 이동

iii kakao <b>cloud</b>		Q. 서비스 점색		kr-central-2	, ⊂∎	i ? • 🗉
🥞 VPC	VPC > VPC					
프로젝트	VPC 🖾					+ vpc 생성
VPC ,	VPC 聖터					
서브넷 라운티 테이블	VPC \$	상태 ≑	IP CIDR 블록 💠	서브넷 👙	기본 VPC 💠	
보안 그룹	clouding report 172 entrangel (the color has an elembarity) (the	<ul> <li>Active</li> </ul>	172.16.0.0/16	4개	બા	:
퍼블릭 IP		1				
사용자 가이드 (2						

#### [그림 2.1.9] VPC 생성 버튼 클릭

iii kakao <b>cloud</b>		오, 서비스 점색	🍳 kr-central-2 🗸 🖽 🗓 🧷 🗉 Ĕ
····································	서브넷 설정	첫 번째 가을 영역적 되철픽 서보넷이 가든으로 양성되며, 성상 후 수정하거나 삭제될 수 있습니다. (1) 세보병의 IP-44 ODR 정류 크거는 것요 ~ /20 년엔스프에어 됩니다. 전쟁 성장가능된 시비넷은 24개에어, 다수의 시비넷 영성 시 순사적으로 자동 성성됩니다.	
····································		가용 영역당 퍼블릭 시보넷 개수 1	
		kr-central-2-b           패블릭 셔브넷 IPv4 CIDR 블록           0.0.0.0/0         0개 사용 가능	
사용자 가이드 간		1112 <b>111</b> 0	
[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 설정한다.

kakaocloud			Q 서비스 검색	Q kr-centr	al-2 - 💾 🛓 🖓 🗆
Virtual Machine	Virtual Machine > 인스탠스 > ✔		시작	정지 재시작 강제 재시작 종	료 인스턴스 삭제 인스턴스 작업 🗸
, 턴스	세부 정보 네트워크	보안 2	볼륨 1 작업 로그 !	모니터링	
샷	보안 그룹				보안 그룹 수전
샷 일정	· 필터 혹은 값을 입력해 주세요.				2건중1-2 < 이전 다음 > :
지	이름		ID		
l어	sg-external ⊵		20079	Ref 6766-4540 4950 354432114820 🕤	
	sg-internal ⊡		6ar112	544 8804 4348 5472 274044586c31 🖆	
	세부 규칙 인바운드 아웃바운드 - 필터 혹은 값을 입력해 주세요.			÷ 1	2 건 중 1-5 < 이전 다음 > / ;
	보안 그룹 💠	프로토콜 수	출발지 💠	포트 번호 💠	설명
	보안 그륨 💠 sg-external	프로토콜 수	출발지 수	포트 번호 💠	설명
	보안 그륨 💠 sg-external sg-external	프로토콜 수	출발지 수	포트 번호 수	설명

보기 Virtual Machine 로젝트 C · · ·	Virtual Machine > 인스턴스 : ♥			시작 정지 재시작			
인스턴스					상세 세시작 전	S료 인스턴스 삭제	인스턴스 작업 🛛 🗸
	세부 정보 네트워크	<b>보안</b> 2	볼륨 1 작업 로그	모니터링			
볼륨 스냅샷 스냅샷 일정	보안 그룹 - 필터 혹은 값을 입력해 주세요.				충	2건중1-2 < 이전	보안 그룹 수정 다음 >
ןעוםוס	이름			ID			
λ] π(σ)	sg-internal 亿 세부 규칙			6x4125d4-8804-43d8-6x42			
	인바운드         아웃바운드				ě.	12 건 중 1-5 < 이전	다음 > 📿
	보안 그룹 💠	프로토콜 수	출발지 💠		포트 번호 💠	설명	
	sg-external	ALL	211.107.16.7/02		ALL	ercin ficarma	
	sg-external	102	172.16.0.0/20		22	spc_ash	
사용자 가이드 亿	sg-external	ALL	125.244.3.124/32		811	101-1121114	

금융보안원

iii kakao <b>cloud</b>			Q, 서비스 검	색		🗣 kr-central-2 🗸 💾 🗓 🕐 🛙
🏟 VPC	VPC > 보안 그룹 >	2007/07ke sifes when effect classic	14000			
프로젝트	sg-exte	ernal ~				
VPC 서브넷	보안 그룹 ID				생성일	
라우팅 테이블 보안 그룹					2024.03.29 (급) 10.00	
퍼블릭 IP	인바운드 규칙 9	) 아웃바운드 규칙 1 연결된	리소스 14			
	인바운드 규칙 필터	1				인바운드 규칙 관
	프로토콜 ≑	출발지 👙	포트 번호 💠	정책 설명		생성일 👙
	ALL	211.107.16.7/02	ALL	etit home		2024.03.29 (금) 16:06
	TCP	172.16.0.0/20		191,107		2024.05.07 (화) 19:58
	ALL	125.244.3 124/37	ALL	ian horne		2024.03.29 (금) 16:06
사용자 가이드 🖸	ALL	124.60.221.105/82	#L1.	ji hora		2024.03.29 (급) 16:06
۔ – ۲	7리 2 1	13] 보아 ㄱ호	르 사세 페이	тини	이바우드 구초	과기 크리

						~	
	보안 그룹 정책 김	관리				X	
,	보안 그룹 이름						
	보안 그룹 설명 (선택)	vpc 외부에서 접근 시 시	8				
	저용된 정책						
	인바운드 규칙	아웃바운드 규칙					
	프로토콜	출발지 💿	포트 번호 🔞	정책 설명 (선택)			
	ALL ~		ALL		적용	Ū	생성일 👙
	TCP ~				적용	Ū	2024.03.29 (금) 16:0
	ALL ~		ALL		적용	Ū	2024.05.07 (화) 19:5
	ALL ~		ALL		적용	Ū	2024.03.29 (금) 16:0
	ALL ~		ALL		적용	Ū	2024.03.29 (금) 16:0

# 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



# 2.2. 내부망 네트워크 보안 통제

#### 1 기준

식별번호	기준	내용
2.2	내부망 네트워크 보안 통제	클라우드 환경 내 내부망 구성 시 보안 통제 방안을 수립

#### 2 설명

- 클라우드 환경 내 내부망을 구성하는 경우 외부 침입, 비인가 접근 등으로 보호될 수 있도록 보안 통제 방안을 수립하고 적용하여야 한다.
  - (예시)
    - 1) VPC 등 네트워크 관련 기능을 통한 네트워크 접근 통제(인터넷망 등)
    - 2) 보안그룹(Security group) 또는 NACL(Network ACL) 등의 기능을 통한 네트워크 구성(인/아 웃바운드 통제 등)
    - 3) 내부망으로 구현한 가상자원(서버, 데이터베이스 등)에 퍼블릭 IP 미 할당
    - 4) 방화벽 서비스를 통한 IP 통제 등

#### 3 우수 사례

- 1) VPC 등 네트워크 관련 기능을 통한 네트워크 접근 통제 (인터넷망 등)
- ▶ 카카오클라우드에서는 하나의 VPC 내에 Internet Gateway 가 존재한다.
- 라우팅 테이블에 Internet Gateway를 대상(target)으로 하는 라우팅을 설정하고, 해당 라우팅 테이 블에 서브넷을 연결하면 연결된 서브넷은 퍼블릭 서브넷이 된다.



iii kakao <b>cloud</b>		Q, 서비스 검색	♥ kr-central-2 -	1 ? - E
• VPC — — — — — — — — — — — — — — — — — — —	상태 ● Active	IP CIDR 블록 172.16.0.0/16	생성의 2024.01.08 (월) 17:50	
C > VPC	세부 정보 토폴로지	셔브넷 4		
라우팅 테이블 보안 그룹 퍼블릭 IP	VPC Virtual Private Cloud cloudtach-opc-172 172-58.8.016	서보였 (4) UPC 내 가용 영역당 사보였 bc-entral-2-8 Pub172-8-8 기2715-00-29 연령원 사소 (24) (3 Pt-172-8-8-4 전 15-16-029 연령원 사소 (1) (3 Pt-172-8-8 Pt-172-8-8 Pt-172-8-8 Pt-172-8-8 전 문 제소소 (9) (3 Pt-172-8-8 Pt-182-8 Pt-172-8-8 Pt-172-8-8 Pt-172-8 Pt-172-8-8 Pt-172-8 Pt	라운당 태어철 (5) 비트워크 트리워 광려를 제어 다운 네트워크의 (14 년 위크 테이어 (14 아po 172 pub b) (14 vpo 172 pub b)	(1) 연결
사용자 가이트 간				
	[그림 2.2.1]	Internet Gateway 연결	된 퍼블릭 서브넷	

- 하나의 서브넷은 하나의 라우팅 테이블을 가질 수 있고, 하나의 라우팅 테이블은 여러 서브넷에 연결 될 수 있다. (서브넷 : 라우팅 테이블 = N : 1 관계)
- ▶ (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 사용한다.

× kakao <b>cloud</b>	Q. 서비스컵세	🍳 kr-central-2 🗸 📑 🛓 ⊘ । 🔳
④ 최근 사용	ジアC     と리적으로 격리된 기상 네트워크를 구성할 수 있습니다.	
\$\$ 전체 서비스		
즐겨찾기 Beta	Load Balancing 사용자 환경에 적합한 설정을 통해 트래픽 분산을 최적화할 수 있습니다.	
자주 사용하는 서비스를 목록에서 추가하세요.		
카테고리	대용량의 웹 콘텐츠를 많은 사용자들에게 빠르고 안정적으로 제공하는 네트워크 서비스입니다.	
Beyond Compute Service	DNS 손쉽게 DNS 서버를 구축할 수 있고 팩른 용답속도와 안정성 높은 DNS 서비스를 제공합니다.	
Beyond Networking Service >		
Container Pack	Transit Gateway 다수의 VPC와 온프레미스 네트워크를 연결하여 중앙 집중식으로 관리할 수 있습니다.	2024.20.21
Beyond Storage Service		2024.05.28
Data Store		2004.05.28
Developer Tools		
Analytics		
Management		
Al Service		Â
Billing		Bare Metal Server
	[기린 2 2 2] 카카오클라으드 코손 > VP(	2 서비스 이동



::: kakao <b>cloud</b>		Q. 서비스 검색		kr-central-2	· d	1 ? · E
🏟 VPC	VPC > VPC					
프로젝트	VPC					+ VPC 생성
VPC	VPC 핖터					
서브넷	VPC \$	상태 💠	IP CIDR 블록 💠	서브넷 🛊	기본 VPC 🛊	
다구닝 데이를 보안 그룹	ethodilectivage 177 antorioti don ottor taki oti ritaatistiti 🔞	Active	172.16.0.0/16	4개	ଜା	:
퍼블릭 IP		1				
사용자 가이드 간						

#### [그림 2.2.3] VPC 생성 버튼 클릭

		(시 제미스 감색	V Kr-central-2	·	L E
프로격트	서브넷 설정	X 번째 가용 양역의 제몰픽 서브넷의 기본으로 상상되며, 상상 후 수장하거나 삭제될 수 있습니다.         시브 것의 IPv4 CIDR 등록 크기는 20 ~ 20 년 것으 ~ 20 년 것으로 이야 입니다.         한 것 양기는 전 LIDR 등록 기는 20 ~ 20 년 것으로 이야 입니다.         가용 양역담 퍼블릭 서브넷 개수 ···································			
사용자 가이드 산		kr-central-2-b 패블릭 서브넷 IPv4 CIDR 블록 0.0.0.0/0 0개 사용 가능 체소 생성			

- ▶ 단, 서브넷 간 접근 통제는 보안 그룹(Security Group) 설정을 통해 접근 통제가 가능하다.
- ▶ 또는, (Console) 'Dashboard' → '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 된다.



× kakao <b>cloud</b>	Q 사비스 검색	♥ kr-central-2 ✓ 💾 🗓 😗 🗉 Ĕ
<ul> <li>최근 사용</li> <li>전체 서비스</li> </ul>	VPC 놀리적으로 격리된 가상 네트워크를 구성할 수 있습니다.	
즐겨찾기 Beta	Load Balancing 사용자 환경에 적합한 실정을 통해 트레픽 분산을 최적화할 수 있습니다.	
자주 사용하는 시비스를 목록에서 추가하세요. 	CDN 대응량의 웹 콘텐츠를 많은 사용자들에게 빠르고 안정적으로 제공하는 네트워크 서비스입니다.	**
Beyond Compute Service	DNS 손쉽게 DNS 서비를 구축할 수 있고 팩른 응답속도와 안정성 높은 DNS 서비스를 제공합니다.	
Container Pack	Transit Gateway 다수의 VPC와 온프레미스 네트워크를 연결하여 중앙 집중식으로 관리할 수 있습니다.	2014.01.01
Beyond Storage Service Data Store		2048.9 2048.9
Developer Tools		
Analytics Management		
Al Service	······································	۱
Billing		Bare Metal Server

#### [그림 2.2.5] 카카오클라우드 콘솔 > VPC 서비스 이동

iii kakao <b>cloud</b>		Q. 서비스 검색		kr-central-2	· E i	() I
🏟 VPC	VPC > 라우딩 테이블					
프로젝트	라우팅 테이블 🖂				+ 라우팅	님 테이블 생성
VPC	라우팅 테이블 필터					
서브넷 라우팅 테이블	라우팅 테이블 🔶	상태 👙	VPC \$	연결된 리소스 🖕	기본 ≑	
보안 그룹		<ul> <li>Active</li> </ul>	dauthich-spo 17) ensered der Köte han an Haath.	<b>0개</b>	아니오	:
퍼플릭 IP		<ul> <li>Active</li> </ul>	claudiach-apo 172 amarach-chor 4000 fais chortaath.	1개 <sup>5</sup>	아니오	:
		<ul> <li>Active</li> </ul>	claudiach-up-172 wheredition - clair has striftacts.	1개 5	아니오	:
	Andre 172 prior	<ul> <li>Active</li> </ul>	cloudlach-spo 17) antaineth their ethic tain the standa.	1개 <sup>1</sup>	아니오	:
	Ange 170 public Francisco de la constante de la	Active	developer 17) anticisette chen 4000 halte ette filmacile.	1개	а	:
			1			
사용자 가이드 [2						
	[그림 2.2.6] 라우팅	테이블 > 리	<b>바우팅 테이블 생</b>	성 버튼 클릭		



::: kakao <b>cloud</b>			Q, 서비스 검색			kr-central-2	· · ·	? · E
VPC	VPC > 라우팅 테이블							
프로젝트	라우팅 테이블						+ 라우팅	테이블 생성
○ ,	라우팅 테이블 필터	라우팅 테이블 생	성		×			
서브넷 라우팅 테이블	라우팅 테이블 🔶	라운티 테이블 이름	악파벳 대소문자(a-z	4-7) 수자(0-9) 는 '만 입력 (4~20자)		연결된 리소스 👙	기본 💠	
보안 그룹	anter-maditi-et All'hadres 1001° ettad 100					07#	아니오	:
퍼블릭 IP	et apper 1720 pade la Autoritation construction at	VPC	VPC를 선택해 주세요	. ~	·	1개	아니오	:
	en agus 172 gail tá an thatcha anns achair th		취소	생성		1개	아니오	:
	strage 172 pri a chamar anno anno son sa	G		and all the state of the second	0	1개	아니오	:
		ā	Active		6	1개	예	:
				1				
사용자 가이드 전								

#### [그림 2.2.7] 라우팅 테이블 생성 모달

iii kakao <b>cloud</b>		Q, 세비스	검색	0	kr-central-2 - 🔳 🛓 🛙	? · E
🥳 VPC	VPC > 라우팅 테이블 >	# Gab2dfam.dentil				
프로젝트	bffe99e1-80b3-49	59-8645-Out-2	/5e6de68 (rtq	pc-172-pri-a)	~	•••
VPC 서브넷	상태 라이 • Active	우팅 테이블 ID	VPC	기본 아니오	생성일 2024.01.08 (월) 18:03	
라우팅 테이블 보안 그룹 퍼블릭 IP						
	라우팅 1         연결 1           연결 필터					+ 연결 수정
	서브넷 🔶		가용 영역 🝦		IP CIDR 블록 👙	
	pri-172-az-a	ā	kr-central-2-a		172.16.16.0/20	
			1			
사용자 가이드 더						
[그림 2.1	2.8] 생성된 라 <u>우팅</u>	테이블 상세	페이지에서 연	년결된 프라이 <u>!</u>	빗 서브넷 <u>확인</u>	



#### 2) 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 설정한다.

iii kakao <b>cloud</b>			Q 서비스 검색	•	kr-central-2 - 📋 🧵	] ⑦ • 📧
Uirtual Machine	Virtual Machine > 인스턴스 : ✔		মৃহ	정지 재시작 강제 재시작	중료 인스턴스 삭제 2	민스턴스 작업 🗸
	세부 정보 네트워크	보안 2	볼륨 1 작업 로그	모니터링		
보드 보드 볼륨 스냅샷	보안 그룹					보안 그룹 수정
스냅샷 일정	· · · · · · · · · · · · · · · · · · ·				총 2 건 중 1-2 < 이전 드	18 >   C
이미지	이름			ID		
키페어	sg-external 🔝			20079/84 6766-4be3-4850-35aa3211a83	6	
	sg-internal 🖸			5a412944-8804-43d8-berf2-8740a4586c1	6	
	세부 규칙 인바운드 야웃바운드 -				총 <b>12 건 중 1-5</b> < 이전 디	18 >   C
	보안 그륨 💠	프로토콜 💠	출발지 수	포트 번호 🔅	설명	
	sg-external	41.1	213.527.56.7/22	ALL	artin hisma	
	sg-external	102	172.16-0-0/20		101.00	
사용자 가이드 亿	sg-external	ALL	125.244.3 124/32	81.5	ign horne	
	[그림 2.2.9] 연	<u> 스턴스</u> ·	상세페이지에서	인바운드 규칙 흑	확인	

Randociouu			Q, 서비스 검색	♥ kr-central-2	· 1 1 0 ·
Virtual Machine	Virtual Machine > 인스턴스 ;	~	시작	정지 재시작 강제 재시작 종료	인스턴스 삭제 인스턴스 작업 🗸
· 던스	세부 정보 네트워크	표 보안 2	볼륨 1 작업 로그 모	니터링	
샷 샷 일정 지	보안 그룹 도 필터 혹은 값을 입력해 주세요.		D	홍2건 중	보안 그를 수정 1-2 < 이전 대응 > 비 도
IM	sg-external [2]		20079/0 6x41250		
	세부 규칙 인바운드 아웃바운드 			총 12 건 중	I-5 < 이전 다음 >   【
	보안 그룹 💠	프로토콜 수	출발지 ⇔	포트 변호 💠 설탕	ġ
	보안 그룹 💠 sg-external	프로토콜 수	查监지 ¢	포트 변호 수 섬임	3
	보안 그룹 수 sg-external sg-external	프로토콜 수 ~~~~ 107	香城口 ↔	포트 번호 수 섬1	9

iii kakao <b>cloud</b>			Q 서비스 검색	4		♀ kr-central-2 → 🗗 🛓 ⑦ । 🚦
PC 🚱	VPC > 보안 그룹 :	2007/s/bit-s/tan-stand-stland Stand27	hadili i			
프로젝트	<b>SG-exte</b> vpc 외부에서 접근 A	ernal ~				
VPC 서브넷 라우팅 테이블	보안 그룹 ID	6 - 11 - 11 - 11 - 11 - 11 - 11 - 11 -			생성일 2024.03.29 (금) 16:06	
보안 그룹 퍼블릭 IP	인바운드 규칙	9 아웃바운드 규칙 1 연결된	리소스 14			
	인바운트 규칙 필터	5				인바운드 규칙 관
	프로토콜 💠	출발지 💠	포트 번호 💠	정책 설명		생성일 👙
	ALL	213.507.56.7/32	ALL	erin home		2024.03.29 (금) 16:06
	TCP	172.16-0-0/20	22	101,000		2024.05.07 (화) 19:58
	ALL	125.244.3 124/32	ALL	ian homa		2024.03.29 (금) 16:06
사용자 가이드 亿	ALL	124.60.221.105/82	ALL	phone		2024.03.29 (己) 16:06

[그림 2.2.11] 보안 그룹 상세 페이지에서 인바운드 규칙 관리 클릭

iii kakao <b>cloud</b>			Q, 서비스 검색			kr-central	-2 · E E
Sec. (1) VPC						×	
프로젝트	보안 그룹 정잭 관	리					
	보안 그룹 이름						
VPC 서브넷	보안 그룹 설명 (선택)	vpc 외부에서 접근 시 시	용				
라우팅 테이블							
보안 그룹	지수리 되어						
퍼블릭 IP	역송한 영역 인바운드 규칙	아웃바운드 규칙					
	프로토콜	출발지 📀	포트 번호 💿	정책 설명 (선택)			인바운드 규칙 관리
	ALL ~		ALL		적용	Ū	생성일 💠
	TCP ~				적용	Ū	2024.03.29 (금) 16:06
	ALL ~		ALL		적용	Ū	2024.05.07 (화) 19:58
	ALL ~		ALL		적용	Ū	2024.03.29 (금) 16:06
사용자 가이드 亿	ALL ~		ALL		적용	Ū	2024.03.29 (금) 16:06
	[7]	빌 2 2 1 2]	이바운ㄷ	규칙 산제 및	츠가		

금융보안원

- 3) 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 않는다. 설정되어 있는 경우에는 해당 라우팅 설정을 삭제한다.

iii kakao <b>cloud</b>		Q 서비2	느검색	•	kr-central-2 ·	E
🏟 урс	VPC 〉 라우팅 테이블 〉	4750-1,472-1,070-7223-4,1747				
프로젝트	bb0e54/5-9aa5	-4798-6472-6967	/3204c1ef (ma	im) ~		
VPC 서브넷	상태 ● Active	라우팅 테이플 ID	vрс vpc-10	기본	생성일 2024.06.04 (화) 09:13	
라우팅 테이블 보안 그룹 퍼블릭 IP	라우팅 2 연결 ()					
	라우팅 빌터				+ 2945	팅 추가
	목적지 🔶	대상 유형 🖕	대상 🗢		상태 💠	
	10.0.0/16	Local	Local		Active	:
	0.0.0/0	igw	Internet Ga	ateway	Active	:
			1			
사용자 가이트 亿						
[그리 2 '	2 13] Internet	Gatoway를 대	사이리 하는 리	나으티에 이느	가이티 데이브	

::: kakao <b>cloud</b>		Q 서비2	느겁색	Q k	r-central-2 - 🗂 🗓	(?) I E
🥳 VPC	VPC > 라우딩 테이블 >	010-85-4° (up)20545.0x00				
프로젝트	bffe99e1-80b3	4959-8645-0ab3	15665de68 (r1 -q	pc-172-pri-a)	~	
VPC 서브넷 라우팅 테이블	상태 ● Active	라우팅 테이ờ ID	VPC cloudtech-vpc-172	기본 아니오	생성일 2024.01.08 (월) 18:1	03
보안 그룹 퍼블릭 IP	라우팅 1 연결 1					
	라구성 필터 목적지 ≑ 172.16.0.0/16	대상 유형 👙 Local	대상 ㅎ Local		상태 수 ● Active	+ 라우팅 추가
			1			
사용자 가이드 건						
[그림 2.2	2.14] Internet	Gateway를 대	상으로 하는 라	우팅이 없는	라우팅 테이블	



▶ 또는, 서브넷에 연결된 라우팅 테이블에 Internet Gateway를 대상으로 하는 라우팅이 있다고 하더 라도 해당 서브넷에 생성한 자원에 퍼블릭 IP를 연결하지 않는다.

::: kakao <b>cloud</b>			ৎ ধ	비스 검색			• kr-centr	al-2 ~	d 1 (	0 1
<b>ाः</b> Virtual Machine	Virtual Machine > 인스턴스 인스턴스	0		시작	정지 재시작	강제 제시작	종료 인스턴스	삭제 인스턴스	논작업 v <u>인스</u> 턴	턴스 생성
	· 코디 속은 값을 접역에 무세	E.	사태	<b>9</b> 8	010131		중 404 전 중 21-40 퍼블리 ID	718.0101 ▲	Allerigi 🔺	
볼륨		manar . fo	Active	πe m2a.large	Ubunt	172.16 🖻	-	kr-central	2024.05.20	:
스냅샷	kitter cloudlech 4	604 TO 1	Active	m2a.large	-	172.16 🖆	-	kr-central	2024.05.20	:
스냅샷 일정	- MadaughtST parts	in the second	Active	m2a.xlarge	-	172.16 🖻	-	kr-central	2024.05.20	:
기페어	- Hadoog Millik, just	60 - 60 To	Active	m2a.xlarge	-	172.16 🖆	-	kr-central	2024.05.20	:
		404-979 E	Active	m2a.xlarge	-	172.16 🗈		kr-central	2024.05.20	:
	68xe-cloudlech-4	64. Addie - 15	Active	m2a.large	-	172.16 🗈	-	kr-central	2024.05.18	:
		67-43-64. To	Active	m2a.large	Rocky	172.16 🖻	-	kr-central	2024.05.18	:
		Maximin 6	Active	t1i.small	😲 Ubunt	172.16 🖻	-	kr-central	2024.05.16	:
	en-dalboard	6er 1000 - 6	Active	m2a.large	😲 Ubunt	172.16 🖻	-	kr-central	2024.05.16	:
	kline-cloudhech-4	1253bos3. To	Active	m2a.large	-	172.16 🖆		kr-central	2024.05.10	:
		63496679 G	Active	m2a.large	Windo	172.16 🖻	-	kr-central	2024.05.09	:
사용자 가이드 亿	pulling-mail	eStations. To	Active	m2a.large	😲 Ubunt	172.16 🖻		kr-central	2024.05.09	:
	grin-master	66.30854e. Fo	Active	m2a.large	😲 Ubunt	172.16 🖻	L	kr-central	2024.04.23	:



외부 접근이 필요한 경우 NAT Instance, Bastion 서버 등을 활용하여 접근한다. 이 때, NAT 인스턴스, Bastion 서버는 퍼블릭 서브넷에 위치한다.









#### 4) 방화벽 서비스를 통한 IP 통제 등

▶ 마켓플레이스 방화벽 상품을 활용하여 내부로 접속하는 IP들을 제한할 수 있다.
 (그림 2.1.1 네트워크/보안 프로젝트 내 UTM, WAF 구성 참고)

kakao <b>cloud</b>	소개 서비스 마켓플레이스 파트너	리소스 고객지원	기술문서 공공기관용 🦻	Console 회원가입
	<b>Marketplace</b> 카카오클라우드와 함께하는 다양한 서비스를 활용하여 빠르게 비즈니스를 시작하세요.			7
	<b>마켓플레이스 서비스</b> 제휴 신청			
	Security (Network) (11) v	Panta	Q 검색아를 입력해주세요. SFC/URITY	<ul> <li>□ 요금계산기</li> <li>※ 상담 및 도입 문의</li> </ul>
L				
	[그림 2.2.18] 카카오클라	우드 마켓플레(	이스 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



# 2.3. 네트워크 보안 관제 수행

#### 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)
  - 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

1) 보안 관제를 위한 IDS 상품을(마켓플레이스) VPC 내 구성하고, 금융회사의 보안관제 시스템과 IPSec VPN 또는 전용선을 통해 연동하여 관제 수행

kakao <b>cloud</b>	소개 서비스 마켓플레이	스 파트너 지원	리소스 공공기관용	1 Console 회원가입
	Marketplace			/
	카카오늘라우드와 임께아는 나양만 서미스를 활용하다 빠르게 비즈니스를 시작하세요.	1		
	미케플케이스 서비스 - 귀엽 시청			
	학옷을레이드 카이드 - 제유 근종			
	전체 (99) ~ )		Q. 검색어를 입력해주세요.	
	[그림 2.3.1] 카카오클리	우드 마켓플	플레이스 상품 소개 페이	אן





- 1. 24x365 모니터링을 통해 카카오클라우드를 이용하는 고객 자원에 대한 다양한 위협 대응
- 2. Managed Security, DDoS Defender, IDS 서비스

# 4 참고 사항

▶ 카카오클라우드 보안 서비스 안내



# 2.4. 공개용 웹서버 네트워크 분리

#### 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

- 1) VPC 등 네트워크 분리 기능을 통한 DMZ 망 구축 후 공개용 웹서버 구현
- 하나의 프로젝트에 외부망, DMZ 망, 내부망으로 구분되는 여러 VPC를 생성한다. VPC 간 통신을 연결하기 위해 Transit Gateway를 생성한 후, TGW 라우팅 테이블에 VPC 간 통신이 필요한 구간에 대해서만 라우팅 설정을 추가한다.
- 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 연결한다.



iii kakao <b>cloud</b>		Q 서비.	스검색	•	kr-central-2 - 💾 🗎 🕐	) I E				
K VPC	VPC > 라우팅웨이블 >									
프로젝트	bb0e5475-9aa5	4798-6472-6963	/3204c1ef (ma	· ·						
VPC 서브넷	ेथम ● Active	라우팅 데이플 ID	VPC vpc-10	기본에	생성일 2024.06.04 (회) 09:13					
보안 그룹 퍼블릭 IP	라우팅 2 연결 0									
	라우딩 필터				+	· 라우팅 추가				
	목적지 🔶	대상 유형 🖕	대상 💠		상태 👙					
	10.0.0.0/16	Local	Local		<ul> <li>Active</li> </ul>	:				
	0.0.0/0	igw	Internet G	ateway	<ul> <li>Active</li> </ul>	:				
			1							
사용자 가이트 문										
[그림 2.	.4.1] Internet G	ateway를 대성	상으로 하는 리	우팅이 있는	라우팅 테이블					

#### kakao**cloud** d 1 0 kr-central-E K VPC VPC > 라우딩 테이블 > || 프로젝트 bffe99e1-80b3-4959-864f-0ab2d6e6de68 (rt-spc-172-pri-a) -0 VPC 생성일 상태 라우팅 테이블 ID 기본 아니오 2024.01.08 (월) 18:03 Active h-vpc-172 서브넷 라우팅 테이블 보안 그룹 퍼블릭 IP 라우팅 1 연결 1 라우팅 필터 + 라우팅 추가 대상 유형 👙 대상 😄 목적지 👌 상태 🗄 172.16.0.0/16 Local Active ÷ Loca 1 사용자 가이드 [2 [그림 2.4.2] Internet Gateway를 대상으로 하는 라우팅이 없는 라우팅 테이블

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

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

▶ 이후 외부망 또는 DMZ 망에 접근 통제를 위한 마켓플레이스 보안 상품을 구성하여 외부에서 공개용



웹서버 접근 시 해당 상품이 설치된 인스턴스를 거치도록 설정한다.

kakao <b>cloud</b>	소개	서비스	마켓플레이스	파트너	지원	리소스	공공기관용	1 Console	l원가입
	Marketpla	се							
	카카오클라우드와 함께하는 빠르게 비즈니스를 시작하,	- 다양한 서비 네요.	스를 활용하여						
	<b>마켓플레이스 서비스</b> 제휴 신·	707							
	전체 (99) ~						Q. 검색어를 입력해주세요.		
	[그림 2.4.3	] 카키	오클라ና	으드 미	<mark>ነ</mark> 켓플	레이	스 상품 소개 페이	지	

#### 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

# 2.5. 네트워크 사설 IP주소 할당 및 관리

#### 1 기준

식별번호	기준				내용
2 5	네트워크	사설	IP주소	할당	클라우드 환경을 통한 내부망 네트워크 구현 시 사설 IP부여
2.5	및 관리				등으로 보안을 강화하고, 내부IP 유출을 금지하여야 한다.

#### 2 설명

▶ 클라우드 환경 내 내부망 네트워크 구현 시 사설IP를 부여하고 주기적으로 현황을 검토하여야 한다.

- (예시)

1) 인터넷 게이트웨이, NAT 게이트웨이 등 관련 기능을 통해 사설IP부여 및 IP 관리 수행

2) 프라이빗 IP 할당 현황에 대한 주기적 검토 수행

#### 3 우수 사례

1) 인터넷 게이트웨이, NAT 인스턴스 등 관련 기능을 통해 프라이빗 IP 부여 및 IP 관리 수행

카카오클라우드에서는 RFC 1918 규격에 따라 프라이빗 IP 주소 범위에서 허용된 블록 크기에 맞춰 VPC를 생성한다.







#### [그림 2.5.2] 카카오클라우드 가이드 문서에 기재된 RFC 1918 규격에 따른 프라이빗 IP 주소 범위

• 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)	10.0.0/16				
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				
192.168.0.0 - 192.168.255.255 (192.168.0.0/16)	192.168.0.0/24				

- VPC에 CIDR 블록은 1개 설정할 수 있습니다.
- 허용된 블록 크기는 /16 ~ /24 넷마스크입니다.

VPC에 CIDR 블록을 설정할 경우 다음 규칙이 적용됩니다.

카카오클라우드 VPC는 IPv4 주소를 지원합니다. VPC를 생성할 때 VPC의 IPv4 주소 범위를 Classless Inter-Domain Routing(CIDR) 블록 형태로 지정 해야 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.

#### VPC IP CIDR 블록

iii kakao <b>cloud</b>		Q 서비스 검색	🍳 kr-central-2 🗸 💼 🗓 🕐 🗉 🗉
S VPC	VPC > VPC > VPC 생성		
프로젝트	VPC 생성		
VPC			
서브넷 라오티 테이블	VPC 정보	VPC 이름 알파벳 대소문자(a-z, A-Z), 숫자(0-9), ''만 입력 (4~200자)	
보안 그룹		VPC IP CIDR 블룩	
퍼블릭 IP		10.0.0.0/16 65.520개 사용 가능	
		▲ 기존 VPC IP와 중복되는 VPC CIDR 철복입니다. 향후 VPC간의 동신을 원할 때 어려울 수 있습니다.	
		VPC는 CIDR 확석으로 알짝 가능하며, 해용되는 같은 아래와 같습니다.           VPC: 이 IP-4 CIDR 활동 2:12:16 - 724 JUM-2:30% 문니다.           100.00 - 1023 255:25 (12.00.00%)           172:16.00 - 1723 1252 50 (12.16.00/12)           192:168.00 - 1723 1252 50 (12.16.00/16)	
	Availability Zone	가용 영역 개수	
-		2 ~	
사용자 가이드 🗅		취소 생성	
[그림 2.5	5.1] VPC <u>생</u> 상	성 시, RFC 1918 규격에 따른 <u>프라이빗</u>	IP 주소 범위 확인

VPC 에는 예약된 IP 주소가 있습니다. 해당 주소들을 제외한 나머지 주소 범위 내에서 생성된 자원에 프라이빗 IP 가 부여됩니다.

예약된 IP 주소						
VPC의 CIDR 블 예약되어 있습니	를록에서 첫 4개의 IP 주소와 마지막 IP 주소는 예약되어 있습니다. 예를 들어 VPC의 CIDR 블록이 10.0.0.0/24일 경우, 다음의 5개 IP 주소는 I다. 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 구	고성 에시					
	[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 서브 넷에는 Internet Gateway를 대상으로 하는 라우팅이 없는 라우팅 테이블을 연결한다.



금융보안원





#### [그림 2.5.5] 프라이빗 서브넷에 연결된 라우팅 테이블

iii kakao <b>cloud</b>		Q 서비	스 검색	•	kr-central-2 - 🗂 🗎 🕻	2 · E
🏟 урс	VPC > 라우팅 테이블 >	47-4750-0-472-0200-7222040-744				
프로젝트	bb0e5475-9aa	5-4798-6472-696	73204c1ef (n	naim) •		
VPC 서브넷 라우팅 테이블	상태 ● Active	라우팅 테이블 ID	VPC vpc-10	기본 에	생성일 2024.06.04 (幹) 09:13	
보안 그룹 퍼블릭 IP	라우팅 2 연결 0					
	라우팅 필터		CHAR		ALCH .	+ 라우팅 추가
	학생자 ÷ 10.0.0.0/16	ਪਾਲ ਜਾਣ ਦ	Local	Ÿ	isiuni ⇒ ● Active	:
	0.0.0/0	igw	Intern	et Gateway	Active	:
			1			
사용자 가이트 근						
[그림 2.	5.6] Internet	Gateway를 대성	상으로 하는	라우팅이 있는	라우팅 테이블	



iii kakao <b>cloud</b>		Q 서비스	검색	♥ kr-central-	2 - 🖞 🗓 🕐	E
🏟 урс	VPC 〉 라우핑 테이블 〉	19-85-9" Call Cillion don't				
프로젝트	bffe99e1-80b3-	4959-864f-0ab3	d5e6de68 (r1 vp	e-172-pri-a) 🗸		
VPC 서브넷	상태 ● Active	라우팅 테이블 ID	VPC cloudtech-vpc-172	기본 아니오	생성일 2024.01.08 <b>(월) 18:0</b> 3	
다우닝네이를 보안 그룹 퍼블릭 IP	라우팅 1 연결 1					
	라우팅 필터 목적지 수	대상 유형 🔶	대상 💠		+ 라우 상태 수	우팅 추가
	172.16.0.0/16	Local	Local		Active	:
사용자 가이드 간						
[그림 2.	5.7] Internet G	ateway를 대상	<u> </u>	우팅이 없는 라우	팅 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 한다. 이때, NAT 인스턴스, Bastion 서버는 퍼블릭 서브넷에 위치한다.

#### 2) 프라이빗 IP 할당 현황에 대한 주기적 검토 수행

▶ (Console) 'Dashboard' → 'VPC' 페이지에서 프라이빗 IP 할당 현황을 확인하고자 하는 VPC 선택
 → '토폴로지' 탭에서 각 서브넷 별 연결된 리소스 정보를 확인하여 해당 서브넷 대역에서 사용 중인
 프라이빗 IP 현황을 확인한다.



× kakao <b>cloud</b>	Q শগত শ্বপ	🕈 kr-central-2 🗸 🗗 🛓 🕐 🗉
<ul> <li>최근사용</li> <li>전체 서비스</li> </ul>	VPC 는라적으로 계리된 가상 네트워크를 구성할 수 있습니다.	
즐거찾기 Bea	Coad Balancing 사용자 환경에 직합한 실정을 통해 트래픽 분산을 최적화할 수 있습니다.	
자주 사용하는 서비스를 목록에서 추가하세요. 	CDN 대용장의 웹 콘텐츠를 많은 사용자들에게 빠르고 안정적으로 제공하는 네트워크 서비스입니다.	
Beyond Compute Service	DNS 손쉽게 DNS 서비를 구축할 수 있고 팩은 응답속도와 안정성 높은 DNS 서비스를 제공합니다.	84 x7+
Container Pack	Transit Gateway 다수의 VPC와 알프레이스 네트워크를 연결하여 중앙 집중식으로 관리할 수 있습니다.	2014.01.01
Beyond Storage Service Data Store		204.05.0 204.05.0
Developer Tools		
Analytics		
Al Service	•	۱
Dining		Bare Metal Server

#### [그림 2.5.8] 카카오클라우드 콘솔 > VPC 서비스 이동

iii kakao <b>cloud</b>		Q, 서비스 검색		kr-central-2	· d (	i ? • E
🏟 VPC	VPC > VPC					
프로젝트	VPC					+ VPC 생성
۵	VPC 필터					
VPC						
라우팅 테이블	VPC \$	상태 💠	IP CIDR 블록 ≑	서브넷 ≑	기본 VPC 👙	
보안 그룹	developed-ope 173 enter etc. door rate test resultant? De	Active	172.16.0.0/16	4개	ଜା	:
퍼블릭 IP		1				
사용자 가이드 ①						
	[그림 2.5.9] 프라이빗	IP 할당 현황을	· 확인할 VP	C 선택		



iii kakao <b>cloud</b>		Q, 서비스 검색		♀ kr-central-2 ✓ 🖽 🛓 ⑦	E
• vpc           ===           •	세부 정보 토플로지 서브넷 4				
VPC	VPC Virtual Private Cloud	<b>서브넷 (4)</b> VPC 내 가용 영역당 서브넷	<b>라우팅 테이블 (5)</b> 네트워크 트래픽 경로를 제어	<b>네트워크 연결 (1)</b> 다른 네트워크에 연결	
라우팅 테이블	cloudtech-vpc-172	kr-central-2-a	erin-multi-rt	IGW	
보안 그룹	172.16.8.0/16	pub-172-az-a 172.16.0.0/20 인전된 리소스 (22) [2	rt-vpc-172-pub-b		
퍼블릭 IP		pri-172-az-a	rt-vpc-172-pub-a		
		172.16.16.0/20 연궐된 리소스 (1) [2	rt-vpc-172-pri-a		
		kr-central-2-b	rt-vpc-172-pri-b		
		pri-172-az-b 172.16.48.0/20 연궐된 리소스 (5) [2			
		pub-172-az-b 17216-32.0/20 연궐된 리쇼스 (6) 군			
사용자 가이드 간					
	[그림 2.5.10] 토폴리기	지 탭에서 할당된	! 프라이빗 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



#### 네트워크(방화벽 등) 정책 주기적 검토 2.6.

#### 기준 1

식별번호	기준			내용	
26	네트워크(방화벽	등) 정	성책	클라우드 서비스를 통해 구현한 네트워크 정책	에 대해
2.0	주기적 검토			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

-----

- 1) 방화벽 정책에 관한 주기적 검토 수행
- ▶ 방화벽의 경우 마켓플레이스 상품을 통해 구성 가능하며, 방화벽 설정은 방화벽 솔루션에 접속하여 관리 가능

kakao <b>cloud</b>	소개	서비스	마켓플레이스	파트너	지원	리소스	공공기관용	1	Console	회원가입	
	<b>Marketpla</b> 카카오클라우드와 함께하는 빠르게 비즈니스를 시작하기	<b>C은</b> 다양한 서비: II요.	스를 활용하여								
	마켓플레이스 서비스 제휴 신경	9									
	전체 (99) ~						Q 검색어를 입력해주세요.				
	[그림 2.6.1	] 카카	오클라ና	으므	ŀ켓플	레이크	스 상품 소개 페이지				



- 2) ACL 정책에 관한 주기적 검토 수행
- ▶ NACL 서비스는 24년 3Q 제공예정.

#### 3) 보안그룹에 관한 주기적 검토 수행

 ▶ (Console) 'Dashboard' → 'VPC' → '보안 그룹' 페이지에서 보안 그룹 목록을 확인하고, 확인을 원하는 보안 그룹의 이름을 클릭하여 보안 그룹 상세 페이지에서 인바운드/아웃바운드 규칙 확인 및 연결된 리소스 정보를 확인한다.

× kakao <b>cloud</b>	Q. 서비스 검색	🗣 kr-central-2 🗸 🗗 🗓 🕐 🔳
③ 최근사용	VPC 논리적으로 적직된 가상 네트워크를 구성될 수 있습니다.	
전세 서비스 즐거찾기 Beta	Load Balancing 사용자 환경에 제합한 삶영품 통해 트레픽 분산을 최적화할 수 있습니다.	
자주 사용하는 서비스를 목록에서 추가하세요.	CDN 대화관 및 프해소를 많은 사용자들에게 빠르고 안정적으로 제공하는 네트워크 서비스입니다.	**
भध्याञ्च Beyond Compute Service		
Beyond Networking Service >	E EM UNS ANN 별 가족을 가 있고 찍는 등 감독도와 인생용 뿐은 UNS ANN도록 제공됩니다.	
Container Pack Beyond Storage Service	다수의 VPC와 은프레이스 네트워크를 연결하여 중앙 집중식으로 권리할 수 있습니다.	2014-05.28
Data Store		2014.01.28
Developer Tools Analytics		
Management		
Al Service Billing	•••• ••• •••	۲
		Bare Metal Server

#### [그림 2.6.2] 카카오클라우드 콘솔 > VPC 서비스 이동

iii kakao <b>cloud</b>	Q 서비스 검색	🗣 kr-central-2 🗸 🗗 🛓 🕐   🗉
🚱 VPC	VPC > 보안그룹	
프로젝트	보안 그룹 🐵	十 보안 그룹 생성
C → VPC	보안 그용 필터	
서브넷 라우팅 테이블	보안그룹 🔶	생성일 수
보안 그룹	erite adv eg     e	2024.05.22 (수) 18:04 :
퍼블릭 IP	at These to be desired that the state of the	2024.05.22 (수) 16:42
	Section 2010 And Annual Section 2010 Annual Section 2010 Annual Section 2010	2024.05.21 (勢) 23:52
	the charter for charter charter in the index to balls to group control plane     todayting again again this with the initial court of the initial court	2024.05.20 (월) 13:02
	disculations of cluster clusters in many ratio is due to group worker     water ratio with were work rationalization         ()	2024.05.20 (월) 13:02
	participation (CE 27) hadrong schedule (all high ethic integration) (6)	2024.05.20 (程) 10:31
사용자 가이드 간	C make a more with control and the	2024.05.18 (토) 21:54



iii kakao <b>cloud</b>		Q 서비스 검색		🍳 kr-central-2 🗸 📑 🧐 🗉 🗉
PC	VPC > 보안 그룹 >			
프로젝트	erin-alb-sg ~			
VPC 서브넷 라우팅 테이블	이 왔는 일보 0		생성열 2024.05.22 ( <b>수</b> ) 18:04	
보안 그룹 퍼블릭 IP	인바운드 규칙 5 아웃바운드 규칙 1 연결된 리소	스 1		
	인바운드 규칙 필터			인바운드 규칙 관리
	프로토콜 🝦 출발지 👳	포트 번호 💠	정책 설명	생성일 🖕
	TCP 172.16.0.11/32	80	hc	2024.05.22 (个) 18:04
	TCP 172.16.0.101/32	80	hc	2024.05.22 (수) 18:04
사용자 가이드 간	TCP 172.16.3.47/32	80	lb	2024.05.22 (수) 18:04

#### [그림 2.6.4] 인바운드 규칙 확인

iii kakao <b>cloud</b>	Q 서비스 검색	🍳 kr-central-2 🗸 👖 🛓 🕐 🗉 🗉
🤹 VPC	VPC > 보안 그룹 >	
프로젝트	erin-alb-sg ~	
VPC 서브넷 라우팅 테이블	보인 그렇 ID 정성의 D <b>2024.05.22 (수) 18:04</b>	
보안 그룹		
	인데코드 파악 이 가지방코드 파악 I 고달인 티스스 I 아웃바운드 규칙 웹테 프로토물 승 목적지 포트 번호 정책 설명	아웃바운드 규칙 관리 생성일 : 0
	ALL 0.0.0/0 ALL -	2024.05.22 (个) 18:04
사용자 가이드 안		
	[그림 2.6.5] 아웃바운드 규칙 확인	



iii kakao <b>cloud</b>	Q 서비스 광책 • kr-central-2 · 립 ② · E
🥳 VPC	VPC > 보안그룹 >
프로젝트	erin-alb-sg ~
VPC 서브넷 라우링 테이블	보인 그룹 ID 생성일 5 2024.05.22 (수) 18:04
보안 그룹	
에 바람보	안바운드 규칙 5         아웃바운드 규칙 1         연결된 리소스 1           연결된 리소스 1         연결된 리소스 1         연결 리소스 수정
	연결 유형 ☆ 연결된 리소스 이름 ☆ 연결된 리소스 상태 ☆ 연결된 리소스 실명 ☆
	인스템스 erin-web I2 • Active -
	1
사용자 가이드 간	
	[그림 2.6.6] 연결된 리소스 확인

#### 4) 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 확인한다.

× kakao <b>cloud</b>	Q. 서비스 검색	🗣 kr-central-2 🗸 🗗 🚹 🕐 📕
( 최근 사용	VPC E리적으로 격려된 기상 네트워크를 구성할 수 있습니다.	
\$\$ 전체 서비스		
즐겨찾기 Beta	Coao Balancing 사용자 환경에 적합한 설정을 통해 트레픽 분산을 최적화할 수 있습니다.	
자주 사용하는 서비스를 목록에서 추가하세요.		
카테고리	대용량의 웹 콘텐츠를 많은 사용자들에게 빠르고 안정적으로 제공하는 네트워크 서비스입니다.	
Beyond Compute Service	DNS 손쉽게 DNS 서버를 구축할 수 있고 뼈른 응답속도와 안정성 높은 DNS 서비스를 제공합니다.	84 x7c
Beyond Networking Service >		
Container Pack	Transit Gateway 다수의 VPC와 잔프레미스 네트워크를 연결하여 중앙 집중식으로 관리할 수 있습니다.	2004.01.01
Beyond Storage Service		2014.05.08
Data Store		2014.05.04
Developer Tools		
Analytics		
Management		
Al Service		Î
Billing		Bare Metal Server
	[그림 2.6.7] 카카오클라우드 콘솔 > VPC	C 서비스 이동



iii kakao <b>cloud</b>		Q, 서비스 검색		• kr-central-2	· d	i 🤉 🗉
🚱 VPC	VPC > VPC					
프로젝트	VPC					+ VPC 생성
	VPC 뒢터					
서브넷	VPC $\Leftrightarrow$	상태 💠	IP CIDR 블록 💠	서브넷 🖕	기본 VPC 👙	
라우팅 테이블 보안 그룹	daudach op 173	Active	172.16.0.0/16	4개	ଜା	:
퍼블릭 IP		1				
사용자 가이드 건						

#### [그림 2.6.8] 프라이빗 IP 할당 현황을 확인할 VPC 선택

VPC	세부정보 토플로지 서브넷 4			
2C	VPC Virtual Private Cloud	<b>서브넷 (4)</b> VPC 내 가용 영역당 서브넷	<b>라우팅 테이블 (5)</b> 네트워크 트래픽 경로를 제어	<b>네트워크 연결 (1)</b> 다른 네트워크에 연결
1=>>	cloudtech-vpc-172	kr-central-2-a	erin-multi-rt	IGW
보안 그룹	172.16.0.0/16	pub-172-az-a 172.16.0.0/20 인권된 리소스 (22) [2	rt-vpc-172-pub-b	
더블릭 IP		pri-172-az-a	rt-vpc-172-pub-a	
		172.16.16.0/20 연결된 리소스 (1) [2	rt-vpc-172-pri-a	
		kr-central-2-b	rt-vpc-172-pri-b	
		pri-172-az-b 172.16.48.0/20 연렬된 리소스 (5) [건		
		pub-172-az-b 172.16.32.0/20 연절된 리소스 (6) [2		
사용자 가이드 간				
사용사 가이드 년				

#### 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





# 3.1. 클라우드 계정 권한 관리

#### 1 기준

식별번호	기준	내용
3.1	클라우드 계정 권한 관리	클라우드 서비스 이용 시 업무 및 권한에 따라 계정을 관리 하여야 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 부여 할 수 있다.

금융보안원

iii kakao <b>cloud</b>		Q 서비스 검색	♀ kr-central-2 ~ 🖽 🗓	0 · 🗉
😤 іам	IAM > 프로젝트 구성원			
프로젝트	프로젝트 구성원 🗵			
프로젝트 구성원	프로젝트 레벨 역할 10 그룹	권한 0		
서비스 계정	프로젝트 레벨 역할: 전체 🛛 🗸		아이디를 입력 후 엔터를 누르세요. Q + 프로젝트	. 레벨 역할 관리
조직 <b>년</b>	닉네임 (이름)	사용자 아이디 💠	프로젝트 레벨 역할 💿	
프로젝트	D david son (david son)	david arrightalasertarprise.com	프로젝트 관리자 (Admin)	:
사용자 그룹		erin oğlukuserlerprise.com	프로젝트 관리자 (Admin)	:
역할 조직 관리		ian Sijikakasenterprise com	프로젝트 관리자 (Admin)	:
		jd. new [likakasenterprise.com	프로젝트 관리자 (Admin)	:
사용자 가이드 亿		pough 82 (Juakacenterprise.com	프로젝트 관리자 (Admin)	:
[그림 3.1.1	] 카카오클라우드 콘을	속의 IAM 서비스에서 확인 <sup>*</sup>	할 수 있는 프로젝트와 조직	<u>i</u>

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

iii kakao <b>cloud</b>		Q, 서비스 검색	O Giobal 🗗 🛓 🕐 🗉 🖪
😤 IAM	iam > ~ 역할		
프로젝트	역할 🖉		
프로젝트 구성원	분류	역할	설명
서비스 계정	조직	조직 소유자 (Owner)	조직 관리자 역합을 포함합니다. 조직과 사용자를 관리하는 최상위 권만입니다. 조직 소유자 역할은 식제할 수 없으며, 역합을 이양하 이 담당자를 변경할 수 있습니다.
đ	조직	조직 관리자 (Admin)	조직과 프로젝트(리소스 계획)를 관리합니다. 사용자 및 IAM 역황을 추가 또는 삭제함 수 있습니다.
프로젝트 사용자	조직	조직 리더 (Reader)	조직과 프로젝트(리소스 계외)를 조회할 수 있습니다. 사용자 및 IAM 역할을 조회할 수 있습니다.
역할	조직	빌링 관리자 (Admin)	빈장 메니지 여항을 포함합니다. Billing 서비스에서 결제 수단 및 크레팃, 청구서, 리소스 사용량 및 예상 요금 등을 관리할 수 있습니 다.
조직 관리	조직	빌링 매니저 (Manager)	보딩 뷰어 역할을 포함합니다. Billing 시비스에서 청구서와 프로젝트의 리소스 사용량 및 예상 요금을 조회할 수 있습니다.
사용자 가이트 년	조직	빌링 뷰어 (Viewer)	권한이 있는 프로젝트의 예상요금 및 사용량을 조회할 수 있습니다.
[그리 312]	카카이크라이드 크	코속이 IAM 서비스()	비서 화이하 스 이느 ㅈ지 레베 여하 으혀

▶ 프로젝트 레벨 역할 유형은 프로젝트 관리자(Admin), 프로젝트 멤버(Member), 프로젝트 리더 (Reader) 가 있다.

금융보안원

iii kakao <b>cloud</b>		Q, 서비스검색	o Giobal 🗗 🗋 🕐 🛙 🗈			
	조직	빌링 뷰어 (Viewer)	권한이 있는 프로젝트의 예상요금 및 사용량을 조회할 수 있습니다.			
프로젝트 구성원 서비스 계정	조직	트레일 뷰어 (Viewer)	Cloud Trail의 조직 이벤트 조회 권한입니다. Cloud Trail > Event에서 프로젝트 이벤트와 함께 프로젝트 생성, 삭제, 콘솔 로그인, 로 그아웃, 빌링 조의 등 조직 이벤트를 조의할 수 있습니다.			
	조직	Alert Center 관리자 (Admin)	Alert Center 서비스의 조직 가능 권한이 있습니다.			
조직	프로젝트	프로젝트 관리자 (Admin)	프로젝트 내 모든 리소스의 전체 권한(생성, 조희, 수정, 삭제)을 기지고 있으며, '프로젝트 멤버' 역할을 포함합니다. 프로젝트 관리자 는 각 프로젝트 구성원이 프로젝트 역왕을 관리할 수 있습니다.			
프로젝트	프로젝트	프로젝트 멤버 (Member)	프로젝트 내에 권한이 있는 리소스를 조회 또는 수정할 수 있습니다. 프로젝트 멤버의 상세 권한은 각 서비스마다 다를 수 있습니다.			
그룹	프로젝트	프로젝트 리더 (Reader)	프로젝트 내에 권한이 있는 리소스를 조회할 수 있습니다. 상세 권한은 각 시비스마다 다를 수 있습니다.			
조직 관리	프로젝트	Kubeflow 관리자 (Admin)	Kubeflow 서비스의 리소스를 생성, 조회, 수징, 식체할 수 있습니다.			
사용자 가이드 년						
[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 권장한다.
- 조직 소유자는 다른 사용자를 초대하여 조직 레벨 역할 권한을 부여하거나, 프로젝트를 생성한 후 사용자를 해당 프로젝트의 권한을 부여한다.

iii kakao <b>cloud</b>		Q 서비스 검색	9 Giobal	d 1 2 0 -	•
😤 іам	IAM > kakaoicloud-r > 사용자				
프로젝트	사용자 🗊			+ 사용자 등록	ł
프로젝트 구성원	조직 레벨 역할: 전체	~	아이디를 일	김력 후 엔터를 누르세요. (	λ
서비스 계정	닉네임 (이름)	사용자 아이디 🖕	조직 레벨 역할	그룹 역할 💿	
조직 <b>1</b> 월	3.	34etgdg@textef.com	역할 없음	역할 없음	
프로젝트	A -	abiygal leejjhataoerterprise.com	조직 관리자 (Admin)	역할 없음 조직 레벨 역할 추가	]
그룹	-	adhe zijikakaoemterprisa com	역할 없음	역할 없음 사용자 사제	
국 <u>교</u> 조직 관리		r (andy test user) alt <> (äydelhuğyopmat.com	역할 없음	역할 없음	
사용자 가이드 (2	-	andres changlikakaserkepina con	조직 소유자 (Owner) 조직 관리자 (Admin) 빌링 관리자 (Admin) 빌링 매니저 (Manager)	역할 없음 :	
		[그림 3.1.4] 조직 레벨 역할 취	추가		


iii kakao <b>cloud</b>		Q 서비스 검색	♀ kr-central-2 ~	di 🛓 🕐 ' 🗉		
😤 іам	IAM > 프로젝트 구성원					
프로젝트	프로젝트 구성원 🙄					
프로젝트 구성원 서비스 계정	프로젝트 레벨 역할: 전체 🗸	그룹 전선 0	아이디를 입력 추 엔터를 누르세요. Q	+ 프로젝트 레벨 역할 관리		
조직 <b>C</b> 립	닉네임 (이름)	사용자 아이디 👙	프로젝트 레벨 역할 📀			
프로젝트	D david am (david am)	david am@kakaoemterprisa.com	프로젝트 관리자 (Admin)	:		
사용자 그룹		erin oğluşkaserterprise.com	프로젝트 관리자 (Admin)	프로젝트 레벨 역할 관리 프로젝트에서 내보내기		
역할 조직 관리		un Sijkakaoerterprise com	프로젝트 관리자 (Admin)	÷		
		pl.new@kakasenterprise.com	프로젝트 관리자 (Admin)	:		
사용자 가이드 化	J prosph 87 (prosph 87)	pooph Elifikakaoerteeprise.com	프로젝트 관리자 (Admin)	:		
	[그림 3.1.5] 프로젝트 레벨 역할 추가					

▶ 단, 조직 소유자 권한을 가진 계정으로만 2단계 인증 설정, IdP 연동, 조직 삭제 신청이 가능하다.

iii kakao <b>cloud</b>		Q, 서비스 검색	Global	L 1 2 .
😤 іам	IAM > 조직 -	관리 > 계정 설정		
ক্রম <b>৫</b> ৪	로그인 설정			
프로젝트 사용자 그룹	조직 정보	이름 사용자 아이디 『고		
역할 조직 관리	계정 설정	IdP 계정으로 로그인을 연동한 이후에는 올라우드 계정으로 변경할 수 없습니다. 8 • 클라우드 계정 IdP 계정	#라우드 계정으로 변경이 필요함 경우에는 <b>헬프데스크</b>	12 로 문의해 주세요.
	2단계 안중	조직의 모든 사용자에게 적용됩니다. 플라우드 계정 로그인을 사용하는 조직인 2건 • 사용 안 함 · 사용	제 인칭을 사용할 수 있습니다.	
사용자 가이드 亿		취소 저장		
	[그릴	316] 2단계 인증 및 IdP 연동	특석정	

::: kakao <b>cloud</b>		Q, 서비스 검색	♀ Global	1 ? 1
😤 IAM	IAM > · · · · · 조직 관리			
조직	조직 관리 🖸			
프로젝트	조직 정보			조직 삭제 신청
사용자 그룹	मद्रम= 1 71	<sup>사용자</sup> 各 명	<sup>⊸⊚</sup> <b>終 0 개</b>	
역열 조직 관리				
	로그인 설정 보안 설정			
				로그인 설정
	조직 이름	조직 아이디	5553a0a0a0ac24455da2933a04556291e1 6	
	계정 클라우드 카카오클라우드	2단계 인증 설정 🍚	● 사용 안 함	
사용자 가이트 亿				
[그림 3.1.7] 조직 삭제 신청				

▶ 조직 소유자의 행위는 Cloud Trail 서비스를 통해 추적이 가능하다.

iii kakao <b>cloud</b>		Q *	네비스 검색			kr-central-2	·	0
Cloud Trail	Cloud Trail > Dashboard							
로젝트 3	Dashboard							
Dashboard Event	프로젝트 이벤트 현황 조희 기간   2024.05.28 ~ 2024.0 Block Storage Tinstance Proje VPC	06.03 ct Public IP Security Grou 49 2024.05.29	p = Listener = Backu	p Keypair Alert Policy 56 2024 05 31	Load Balancer 1     4     2024.06.01	Target Group  Healt	1주 전 h Check = Bucket = 11 2024.06.0	v image
	최근 프로젝트 이벤트 목록 이벤트 발생시간 이벤트	트이름		사용자 / 사용자 고유 ID		서비스 이름 7	전체 이번 다원 유형 자원	벤트 기록 보기 빈 이름
사용자 가이드 亿				erts official accention of				



iii kakao <b>cloud</b>			Q, 서비스 검색			♀ kr-central-2 ~	di 🗴 🕐 🗉
Cloud Trail	Cloud Trail > 이벤트 이벤트					• 로그지	장 여러 발생 로그 저장 관리
۵	👳 속성 이름을 입력해 주세요.		조회 항목: 전체 조회	▼ 1일 전	~	총 <b>279</b> 건 중 1-50	< 이전 다음 > [ 3
대시보드	필터	이벤트 이름	사용자	사용자 고유 ID	서비스 이름	리소스 유형	리소스 이름
이벤트	이벤트 이름			41-10-11-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1			
	사용자 사용자 고유 ID						
	서비스 이름 리소스 유형						10000
	리소스 이름						
	2024.06.18 (화) 16:2 프로젝트			41.0000.000-10000.000			
	2024.06.18 (화) 16:2 조직			-			
	2024.06.18 (화) 16:2 조직						
	2024.06.18 (화) 16:2 프로젝트						
	2024.06.18 (화) 16:2 프로젝트			******			
	2024.06.18 (화) 16:2 조직			Report Office (1996) 19.			
사용자 가이드 亿	2024.06.18 (화) 16:1 조직						
[그림 3.1.9]	이벤트 목록에서	사용자, 시	용자 고유	ID로 검색	하여 계정	성 관련 로	그를 확인

Cloud Trail에서 발생하는 이벤트 데이터를 Pub/Sub과 Alert Center를 통해 모니터링 알림을 구성 할 수 있다.



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

iii kakao <b>cloud</b>		Q 서비스 검색	Ç Global	1 1 0 1
😤 іам	IAM > > 조직 관리 > 콘	솔 접근 제어 설정		
조직	콘솔 접근 제어 설정			
C3 프로젝트 사용자 그룹	콘솔 접근 제어 설정	<ul> <li>→ 사용</li> <li>● 사용</li> </ul>		
역할 조직 관리	접근 허용 IP	역 명철 역		
		office	내 IP 주소 🕕	
		+ 접근 허용 IP 추가하기	□ 현재 IP 주소 복사하기	
		존속 접근 제어 기능을 사용 시, 접근 하용 IP 목록에 등록되지 않은 IP는 모든 콘솔 현재 접속한 IP 주소가 하용 목록에 등록되지 않으면, 사용자들은 콘솔에 접근할 4	:에 접근이 제한됩니다. - 없습니다.	
사용자 가이드 Ư		취소 저장		
	[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

# 3.2. 이용자별 인증 수단 부여

#### 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 사용한다.

	kakao <b>cloud</b>		
	콘솔 로그인		
	조직 이름		
	클라우드 계정 아이디(이메일 주소) 입력		
	비밀번호	비밀번호 재설정	
	비밀번호 입력	Ø	
	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		
	이전		
[_	[그림 3.2.1] 카카오클라우드 콘솔 로그인 화면		



추가로 2단계 인증 설정을 통해 메일이나 SMS 로 인증하도록 설정 가능하다. 단, 해당 설정은 조직 소유자 권한을 가진 계정으로만 가능하다.

iii kakao <b>cloud</b>		Q. 서비스 검색	Global	
😤 іам	IAM 〉 조직 관리	> 계정 설정		
조직	로그인 설정			
프로젝트 사용자 그룹	조직 정보	이름 사용자 아이디 『고		
역할 조직 관리	계정 설정	IdP 개장으로 로그만을 연동한 이후에는 플라우드 개정으로 변경할 수 없습니다. 플라우 • 클라우드 개정 IdP 개정	는 계정으로 변경이 필요한 경우에는 <b>행프데스크</b> (	g 로 문의해 주세요.
	2년계 인종 💿	조직의 모든 사용자에게 적용됩니다. 클라우드 계정 로그인을 사용하는 조직인 2단계 인	i종을 사용할 수 있습니다.	
사용자 가이드 군		<b>취소</b> 저장		
		[그림 3.2.2] 2단계 인증 설정		

kakao <b>cloud</b>
로그인 2단계 인증
이메일 인증 휴대폰 번호 인증 • e****@k*******.com 등록된 휴대폰 번호 없음 @
<mark>인증번호 발송</mark> 이전
[그리 3 2 3] 카카이클라이드 코소 ㄹ그이 2다계 이즈



▶ 그 외에도 IdP 연동을 통해 Microsoft Entra ID 를 연동하여 사용하도록 설정 가능하다.

iii kakao <b>cloud</b>		Q 서비스 검색	<b>Q</b> Global	
🙈 іам	IAM 〉 chaos-ella-company-10 〉 조직 관리			
조직	조직 관리 💿			
e chaos-ella-company-10 프로젝트	조직 정보			조직 삭제 신청
사용자 그룹	프로젝트 1개	<sup>사용자</sup> 6 명	<sup>□≝</sup> 양 기	
역할 조직 관리				
	로그인 설정 보안 설정			로그인 설정
	조직 이름 chaos-ella-company-10	조직 ID		_
	로그인 계정 클라우드 카키오클라우드	2단계 인종 설정 💮	◎ 사용 만함	
l		[그림 3.2.4] 로그인 설정		

::: kakao <b>cloud</b>		Q MINA 284 Q Global El L 🕐 I
😤 IAM	IAM > chaos-ella-company-10 > 조직 관리 > 로	그런 설정
조직 데 chaos-ella-company-10	로그인 설정	
프로젝트 사용자 그루	조직 정보	이를 chaos-ella-company-10 ID To To
역할 조직 관리	로그인 계정	ldP 계정으로 로그인들 면동한 이후에는 클라우드 계정으로 변경할 수 없습니다. 클라우드 계정으로 변경이 필요한 경우에는 별프 데스크 않 로 문의해주세요. 클라우드 계정 ● IdP 계정
	연동 프로토콜	OIDC(OAuth 2.0) SAML 2.0
	연동 정보	IdP(자격 증명 공급자) Azure Active Directory ~
		Authorization 타입 선택 🔹
		Authorization URL IdP에서 제공하는 Authorization URL을 입력해 주세요.
		Token URL IdP에서 제공하는 Token URL을 입력해 주세요.
사용자 가이트 간		Client ID 취소 저장
	[그림	3.2.5] 연동 정보 입력



# 4 참고 사항

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



# 3.3. 인사 변경사항 발생 시 계정 관리

#### 1 기준

식별번호	기준	내용
2.2	인사 변경사항 발생 시 계정	이용자의 인사변경(휴직, 전출, 퇴직 등) 발생 시 지체 없이
<u> </u>	관리	이용자 계정 삭제, 중지 등의 조치를 수행하여야 한다.

#### 2 설명

- 클라우드를 이용하는 임직원의 인사 변경사항 발생 시 지체 없이 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 제공한다.

iii kakao <b>cloud</b>		Q, 서비스 검색	Global		?
A IAM	IAM > 사용자				
프로젝트	사용자 🖸				╋ 사용자 등
프로젝트 구성원	조직 레벨 역할: 전체 💙			를 입력 후 엔터를 누르세요.	
서비스 계정	닉네임 (이름)	사용자 아이디 💠	조직 레벨 역할	그룹 역할 📀	
ч П	B .	Metgdgjjitestel com	역할 없음	역할 없음	
프로젝트	A -	abbygal leejikakaoerterprise.com	조직 관리자 (Admin)	역할 없음	
사용자 그룹 역학	A -	ader sjänkaserterprise com	역할 없음	역할 없음	
~ <del>=</del> 조직 관리	A analy head user (prody head user)	alt of bhydelhoglyopmail.com	역할 없음	역할 없음	
	• •	andres chang@altaserterprise.com	조직 소유자 (Owner) 조직 관리자 (Admin) 빌링 관리자 (Admin) 빌링 매니저 (Manager) 트레일 뷰어 (Viewer)	역할 없음	
사용자 가이드 [2			조진 리더 (Reader)		



iii kakao <b>cloud</b>		Q, 서비스 검색	Global	d i 🤉 🗉
😤 IAM	IAM > kakaoicloud-r > 사용자			
프로젝트 C cloudtech-main >	사용자 💿			+ 사용자 등록
프로젝트 구성원	조직 레벨 역할: 전체 💙		아이디네	· 입력 후 엔터를 누르세요. Q
서비스 계정	닉네임 (이름)	사용자 아이디 👙	조직 레벨 역할	그룹 역할 💿
조직 년 kakaoicloud-r	<b>3</b> .	34etgdg@testef.com	역할 없음	역할 없음
프로젝트	A -	abbygail.lee@kakaoenterprise.com	조직 관리자 (Admin)	역할없음
그룹	• •	adler.z@kakaoenterprise.com	역할 없음	사용자 정보 역할 없음 조직 레벨 역할 추가
ㅋ르 조직 관리	A andy.test.user (andy.test.user	r) alt.v3-bby84hx@yopmail.com	역할 없음	역할 없음 사용자 삭제
	•	andrew.chang@kakaoenterprise.com	조직 소유자 (Owner) 조직 관리자 (Admin) 빌링 관리자 (Admin) 빌링 매니저 (Manager) 트레일 뷰어 (Viewer)	역할 없음
사용자 가이드 🗅			조직 리더 (Reader)	
	[기리_221	) 지지 <u>- 지지 레베 여</u>	하 스저	

iii kakao <b>cloud</b>			Q 서비스 검색	Ģ Glob	al 🔲	i ? • E
😤 ІАМ	IAM >	> 사용자				
프로젝트	사용자	3]		_		+ 사용자 등록
· · ·	조직 레벨 역회	률 조직 레벨	l 역할 추가	×	이디를 입력 후 엔터를 누르세요.	Q
서비스 계정		조직 레벨 역할은 IAM ' 빌링 역할은 Billing 서	역할(조직, 빌링, 프로젝트)을 추가 및 삭제할 수 있습니다. 비스에서 리소스 사용량 및 요금을 조회합니다. IAM 기본 역할 자세히 보기 [2		그룹 역할 💿	
조직 đ		조직	kalasitinut -			:
프로젝트	• (	사용자 아이디	ebhygal leeğikakaserterprise.com	in)		:
사용자 그룹 영화		조직 레벨 역할 설정	향당할 역함 조직 레벨 역할 선택	• Ū		:
조직 관리						:
			쉬조 나음	er)		
			andress chargeflakkasenteeprises com	빌링 관리자 (Admin) 빌링 매니저 (Manager) 트레일 뷰어 (Viewer)		:
사용자 가이드 亿				조직 리더 (Reader)		
		그림 3.3.	3] 조직 - 조직 레벨 역할 수	정 모달		

금융보안원

iii kakao <b>cloud</b>		Q 서비스 검색	♀ kr-central-2 ~	I I ? - E
😤 іам	IAM > 프로젝트 구성원			
프로젝트	프로젝트 구성원 🖸			
프로젝트 구성원	프로젝트 레벨 역할 10	그룹 권한 0		
서비스 계정	프로젝트 레벨 역할: 전체 🛛 🗸		아이디를 입력 후 엔터를 누르세요. Q	+ 프로젝트 레벨 역할 관리
조직 <b>년</b>	닉네임 (이름)	사용자 아이디 💠	프로젝트 레벨 역할 💿	
프로젝트		dan ti um gladagaan targetaa can	프로젝트 관리자 (Admin)	:
사용자 그룹	E		프로젝트 관리자 (Admin)	:
역할 조직 관리			프로젝트 관리자 (Admin)	:
		$\beta = 0 + 1 + 2 + 2 + 2 + 2 + 2 + 2 + 2 + 2 + 2$	프로젝트 관리자 (Admin)	:
사용자 가이드 亿			프로젝트 관리자 (Admin)	:
	[그림 3.3.4]	프로젝트 - 프로젝트 i	레벨 역할 확인	

iii kakao <b>cloud</b>		Q, 서비스 검색	🗣 kr-central-2 🗸 💾 🗓 🕐 🗆
A IAM	IAM > 프로젝트 구성원		
프로젝트	프로젝트 구성원 🖂		
프로젝트 구성원	프로젝트 레벨 역할 10 그룹 권한	10	
서비스 계정	프로젝트 레벨 역할: 전체 💙		아이디를 입력 후 엔터를 누르세요. Q + 프로젝트레벌 역할
ع م	닉네임 (이름)	사용자 아이디 💠	프로젝트 레벨 역할 💿
프로젝트	D david are (david are)	david am@kakasamterprise.com	프로젝트 관리자 (Admin)
사용자 그룹		erin oğlukasınlarşıras con	프로젝트 관리자 (Admin) 프로젝트 레벨 역할 관리 프로젝트에서 내보내기
역할 조직 관리	1 mm.2 (***23)	un 2584kanerterprise.com	프로젝트 관리자 (Admin)
	U pi new (pi new)	pl.rew@kakacerterprise.com	프로젝트 관리자 (Admin)
사용자 가이드 군	J prompth 87 (prompth 87)	jourph 87 [[kakaoartarprise.com	프로젝트 관리자 (Admin)



::: kakao <b>cloud</b>	Q. 시비스 감세	🛛 kr-central-2 🔹 🗇 🗉 🖪
😤 ІАМ	IAM > 프로젝트 구성원	
프로젝트	프로젝 👝 프로젝트 레벨 역할 관리	×
프로젝트 구성원	프로젝.프로젝트	
서비스 계정	프로젝트 레킹 사용자 아이디	# 누르세요. Q <b>+ 프로젝트 레벨 역할 관리</b>
ক্রম টো	프로젝트 해명 역함 💿 위단한 역한	프로젝트 레벨 역할 💿
프로젝트	프로젝트 관리자 (Admin) ~	፲] 프로젝트 관리자 (Admin) :
사용자 그룹	+ 프로젝트 레벨 역할 추가	프로젝트 관리자 (Admin) :
역할 조직 관리	취소 다음	프로젝트 관리자 (Admin) :
	I I Maran (Maran) Maran (Maran Sanatara) and	프로젝트 관리자 (Admin) :
사용자 가이드 안	C (2) prospite 27 (prospite 27) (prospite 27)	프로젝트 관리자 (Admin)
	[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 인사변 경에 따른 조치를 진행한다.

😤 IAM	IAM > 프로젝트 구성원		
프로젝트	프로젝트 구성원 💿		
프로젝트 구성원	프로젝트 레벨 역할 10 그룹 권한 0		
서비스 계정	프로젝트 레멜 역할: 전체 🗸 🗸		아이디를 입력 후 엔터를 누르세요. Q + 프로젝트 레벨 역할 관리
조직 <b>d</b> 년	닉네임 (이름)	사용자 아이디 💠	프로젝트 레벨 역할 💿
프로젝트	D dent an (dent an)	david am@kakaoerterprise.com	프로젝트 관리자 (Admin)
사용자 그룹	E ====(245)	erin oğluslasorriterprise com	프로젝트 관리자 (Admin) 프로젝트 관리자 (Admin)
역할 조직 관리		un 2 (Makaoerterprise.com	프로젝트 관리자 (Admin) :
	U pineer (pineer)	pl.rendjitakaserterprise.com	프로젝트 관리자 (Admin)
사용자 가이드 간	J prosph 87 (prosph 87)	pauph.87@ahaorriteprise.com	프로젝트 관리자 (Admin)

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



iii kakao <b>cloud</b>		Q, 서비스 검색	Global	
😤 іам	IAM > kakaoicloud-r > 사용자			
프로젝트	사용자 🖸			+ 사용자 등록
프로젝트 구성원	조직 레벨 역할: 전체 💙		아이디를	입력 후 엔터를 누르세요. Q
서비스 계정	닉네임 (이름)	사용자 아이디 👙	조직 레벨 역할	그룹 역할 💿
조직 <b>CE</b>	<b>3</b> ·	Sheiging (Sector Cours	역할 없음	역할 없음
프로젝트	• •	alitypel inspirateorem com	조직 관리자 (Admin)	사용자 정보 역할 없음 조직 레벨 역할 추가
그룹	A -	aðir sjíkakaseringríse som	역할 없음	역할 없음 사용자 삭제
조직 관리		alt +3-55y6-the@yopmail.com	역할 없음	역할 없음 :
사용자 가이드 亿	• •	andres chang@kakasenteprise.com	조직 소유자 (Owner) 조직 관리자 (Admin) 빌링 관리자 (Admin) 빌링 매니저 (Manager)	역할 없음
	[그림 3.3.8] !	퇴사자의 경우, 사용자	삭제 진행	

iii kakao <b>cloud</b>			Q, 서비스 검색			Q Global	
A IAM	IAM > kakaoiclou	Ar > 사용자					
프로젝트	사용자	사용자 삭제			×		+ 사용자 등록
	조직 레벨 역호	사용자 1명을 삭제하기 위 삭제된 사용자는	위해서는 '조직에서 사용자 삭제'를 입력하{ 조직에 더 이상 접근할 수 없습니다	십시오 . ŀ.		아이디를 입력 후 엔터를 누르시	I£. Q
서비스 계정		조직에서 사용자 삭제				그룹 역할	
조직		이름	사용자 아이디				:
			Distply[ht	satial com			
사용자						in) 역할 없음	:
그룹 역할							:
조직 관리			취소				:
						er)	
사용자 가이드 12			andrew.chang@kakac	penterprise.com	조직 관리자 (Adn 빌링 관리자 (Adn 빌링 매니저 (Mar	lin) 역할 없음 ager)	:
		[]	림 3.3.9] 사용	자 삭제 모	달		

# 4 참고 사항

▶ 카카오클라우드 IAM 역할 관리 가이드

# 3.4. 클라우드 가상자원 관리 시스템 관리자 권한 추가인증 적용

#### 1 기준

식별번호	기준	내용
2.4	클라우드 가상자원 관리 시스템	클라우드 서비스 관리자 권한으로 로그인 시 추가인증
3.4	관리자 권한 추가인증 적용	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 한다. 인증 수단은 이메일 또는 휴대폰 인증을 사용한다.

iii kakao <b>cloud</b>		Q, 서비스 검색	Global	
😤 іам	IAM > 조직	권리 > 계정 실정		
ক্রম্ টো	로그인 설정			
프로젝트 사용자 그룹	조직 정보	이름 사용자 아이디 『급		
역할 조직 관리	계정 실정	ldP 계정으로 로그인을 연동한 이후에는 플라우드 계정으로 변경할 수 없습니다. 플라식 ● 클라우드 계정 ○ IdP 계정	x드 계정으로 변경이 필요한 경우에는 <b>헬프데스크</b> (2	5 로 분의해 주세요.
	2번계 인종 💿	조직의 모든 사용자에게 적용됩니다. 클라우드 계정 로그만을 사용하는 조직만 2단계 약	1종을 사용할 수 있습니다.	
사용자 가이드 간		<b>취소</b> 저장		
		[그림 3.4.1] 2단계 인증 설정		



kakao <b>cloud</b>
로그인 2단계 인증
이메일 인종 휴대폰 번호 인종 • e****@k*******.com 등록된 휴대폰 번호 없음 @
<mark>인증번호 발송</mark> 이전

# 4 참고 사항

▶ 카카오클라우드 로그인 2단계 인증 가이드



#### 클라우드 가상자원 관리 시스템 로그인 규칙 수립 3.5.

#### 기준 1

식별번호	기준	내용
2 5	클라우드 가상자원 관리 시스템	이용자 가상자원 관리 시스템 접근 계정에 대한 안전한
3.0	로그인 규칙 수립	로그인 규칙을 수립하여야 한다.

#### 설명 2

▶ 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

- 1) 로그인 오류에 따른 보안통제 방안
- ▶ 카카오클라우드에서는 비밀번호를 5회 이상 잘못 입력할 경우, 비밀번호 재설정이 필요하다.



kakao <b>cloud</b>	
콘솔 로그인	
조직 이름	
플라우드 계정	
비밀번호	비밀번호 재설정
******* 아이디 또는 비밀번호 정보가 알치하지 않습니다. (실폐 횟수 : 1 / 5) 5회 이상 실패할 경우, 비밀번호 재성경이 필요합니다.	Ø
콘솔 로그인	
이전	

또한, 비밀번호 만료 설정 기능을 통해 비밀번호를 새로 설정해야하는 주기를 설정할 수 있다.
 30~180일 이내로 설정 가능하다.

iii kakao <b>cloud</b>		Q 서비스 검색	Global	₫ ≗ ♡ ⊦ ▪	
🙈 іам	IAM > > 조직 관리	리 → 비밀번호 만료 설정			
조직 <b>년</b>	비밀번호 만료 설정				
프로젝트 사용자 그룹	비밀반호 만료 설정	<ul> <li>→ 사용 안 함</li> <li>● 사용</li> </ul>			
역할 조직 관리	비밀번호 만료일	60일       90일       120일       180일         직접 입력       1       일         실정한 기간이 지나면 로그인 계정의 비밀번호는 만료됩니다. 이후 큰슬 로그만을 1	위해신 반드시 비밀번호를 변경해야 합니다.		
사용자 가이드 亿		취소 저장			
	[그림 3.5.2] 비밀번호 만료 설정 기능				

### 4 참고 사항

- ▶ 카카오클라우드 로그인하기 가이드
- ▶ 카카오클라우드 비밀번호 만료 설정 가이드

#### 계정 비밀번호 규칙 수립 3.6.

#### 1 기준

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

#### 2 설명

▶ 클라우드 가상자원 관리시스템 접근 가능한 계정 생성 시 안전한 비밀번호 규칙을 수립하여 적용하여 야 한다.

#### - (예시)

1) 제3자가 쉽게 유추할 수 없는 비밀번호 작성 규칙 수립

## 3 우수 사례

1) 제3자가 쉽게 유추할 수 없는 비밀번호 작성 규칙 수립

▶ 비밀번호는 최근 사용한 3개의 암호는 재설정 시 사용이 불가능하다.

	kakao <b>cloud</b>	
	비밀번호 재설정	
	*	
	새로운 비밀번호 Ø 최근에 사용한 비밀번호 3개는 사용할 수 없습니다.	
	비밀번호 제입력	
	비밀번호 재설정	
	콘솔 바로가기	
[그림 3.6.	1] 최근에 사용한 비밀번호 3개는 /	사용 불가능 문구



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

kakao <b>cloud</b>	
비밀번호 재설정	
8	
새로운 비밀번호	
비밀번호 입력	ø
영어 대·소문자, 특수문자, 숫자 조합, 9~30자	
비밀번호 재입력	
비밀번호 재입력	Ø
비밀번호 재설정	
콘솔 바로가기	
1림 3.6.2] 비밀번호 재 <u>설정 시.</u>	요구

▶ 비밀번호는 초대 이후 12시간 이내 미설정 시 재설정 요청을 통해서만 설정이 가능하다.

k	akao <b>cloud</b>			
비밀번호 지실 비밀번호 재설정 링크 응	★ 서설정 메일 발송 완료 정 이메일을 확인하시기 바랍니다. 유효기간은 발송 후 12시간 이내입니다.			
	콘솔 바로가기			
[그림 3.6.3.] 비밀번호 재설정 메일 발송 완료 안내				

## 4 참고 사항

▶ 카카오클라우드 비밀번호 변경/재설정 가이드



#### 공개용 웹서버 접근 계정 제한 3.7.

#### 기준 1

식별번호	기준	내용
27	고개요 의녀비 저그 게저 피하	클라우드를 통해 공개용 웹서버를 운영하는 경우 접근
3.7	승제용 접시미 접근 계정 세인	계정을 적절하게 제한하여야 한다.

#### 설명 2

▶ 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 설정 가능

kakao <b>cloud</b>	소개 서비스 미	마켓플레이스 파트너 리소스	고객지원 기술문서 공공기관용 -	Console 회원가업
	<b>Marketplace</b> 카카오클라주드와 함께하는 다양한 빠르게 비즈니스를 시작하세요.	서비스를 활용하여		
	마것물레이스 시비스 제유 신왕 Security (Data) (36) v		Q BB	<ul> <li>■ 요금계산기</li> <li>※ 상담 및 도입 문의</li> <li>↑</li> </ul>
[]	L림 3.7.1] 카카S	오클라우드 마	켓플레이스 상품 소	개 페이지

#### 참고 사항 4

▶ 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





# 4.1. 암호화 적용 가능 여부 확인

#### 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

- \* 현재 카카오클라우드는 고객 제공용 KMS 서비스를 운영하지 않고 있으며, 추후 서비스 출시 예정
- \* 내부 서비스(Storage 류)는 카카오클라우드 내부 사용 KMS로 암호화 하고 있음

#### 1) 이용자가 운영중인 KMS를 활용하여 구성

- On-premise IDC와 전용선 연결 후 On-premise KMS를 통하여 암복호화 수행(그림 3.1.1 TGW)
   를 활용한 외부 IDC 연동 구성 참고)
- 2) (DISK 암호화) 카카오클라우드 Storage Service는 모두 Disk 암호화가 적용되어 있음
- ▶ [File Storage] 기본 적용으로 별도의 설정 필요 없음
- ▶ [Object Storage] (Console) 'Beyond Storage Service' → 'Object Storage' → '버킷 만들기'
   에서 암호화 "사용"으로 변경 이후 사용

타입	STANDARD
이름	영문 소문자, 숫자, 하이픈(-), dot(.)을 입력해 주세요. (4~63자)
암호화 🕜	<ul> <li>사용 안함</li> <li>사용</li> </ul>



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

kakao <b>cloud</b>	소개	서비스 마켓플레이스	파트너	지원	리소스	공공기관용	1	Console	회원가입	I
	<b>Marketpla</b> 카카오를라우드와 함께하는 빠르게 비즈니스를 시작하세	<b>C은</b> 다양한 서비스를 활용하여 요.								
	마랫플레이스 셔비스 제휴 신청 전체 (99) ~					Q 검색어플 입력해주세요.				
•	[그림 4.1.2]	카카오클라우	우드 마	켓플	레이스	느 상품 소개 페이지				

#### 참고 사항 4

▶ 카카오클라우드 마켓플레이스 상품 안내



# 4.2. 암호키 관리 방안 수립

#### 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 기능 없음
- ▶ 다만 File, Object Storage 활용시 아래와 같이 암호 키 갱신 가능
- ▶ [File Storage] Disk 암호키는 2년 주기로 자동 갱신
- [Object Storage] 버킷별로 암호키가 생성되어 적용되므로, 신규 버킷 생성 후 파일 이동 후 기존 버킷 삭제를 통해 버킷 암호화 키 갱신 가능
- ▶ (Console) 'Beyond Storage Service' → 'Object Storage' → 'Bucket' → {{기존 Bucket}}
   선택 → 이동할 파일 전체 선택 → 하단 이동 → {{옮겨갈 Bucket}} 선택 후 이동
  - \* BYOK(Bring Your Own Key)는 추후 기능 개선 예정 사항



iii kakao <b>cloud</b>		Q, 서비스 검색		• kr-central-2	· d 1	(?) I E
Gbject Storage	Object Storage > Bucket >					
프로젝트						
۰ معدد م						
Bucket	타입 STANDARD		생성일 2024.03.14 11:25			
	객체 속성	권한 관리 모니터링				
	🖬 obj-erin				파일 업로드 🖸	폴더 생성
	<ul> <li>멀티 파트 업로드 진행한 객체의 경우 메티</li> <li>또한, 모니티핑 탭의 객체 수, 용량이 일치:</li> </ul>	라 데이터 수정 / 이름 바꾸기 / 복사 / 이동 기능을 사용할 수 없습니다. 하지 않을 수 있습니다.				
	객체 필터	Q				객체 수 : 4
	- 이름	최종 수	정일시	크기	유형	
	Choonsik.jpeg	2024.0	05.01 14:49	5.33 KB	jpeg	:
사용자 가이드 🖸	✔ 1개 파일이 선택됨		I	복사 이동	다운로드	삭제
					1	
	[그림 4.2.1] Obje	ct Storage 콘솔 메뉴	에서 이동	할 파일 선택		

iii kakao <b>cloud</b>		Q 서비스 <b>검</b> 비		kr-central-2 ~		) I E
Object Storage	Object Storage > Bucket >	ή em	×			
프로젝트	objerin v	파일 이동				
¢ ,	 타인	▲ 알티 파트 업로드된 파일을 복사 / 이동앞 경우, 하위 segment 파일이 노출될 수 있습니다.				
Bucket	STANDARD	이전 위치 새 위치 :test/				
	객체					
	Ed objerin		.		파인 언론드 [7	품더 생성
		₩ test				
	(i) 열티 파트 업로: 또한, 모니터링 '					
	객체 필터					객체 수 : 4
	- 이름		Р	ក	형	
	Cho		3	KB jp	eg	:
	🗌 🕒 larg		00	MB bi	n	:
-	n 🗖 stat	취소 이동		포	<del>с</del>	:
사용자 가이드 ②	🧭 1개 파일이		×.	사 이동	다운로드	4 <b>M</b>
	[그림 4.2.2	] Object Storage 콘솔 메뉴에서 피	임 (	이동 싴행		



iii kakao <b>cloud</b>	Q 서비스 검색		♥ kr-centr	al-2 - 🗂 📋	() I
Object Storage	Object Storage $\rightarrow$ Bucket $\rightarrow$ test				
프로젝트	test ~				
Bucket	부입 STANDARD	생성일 2024.06.12 10:49			
	객체 속성 권한 관리 모니터 G test	8		파일 업로드 [2]	플더 생성
	<ul> <li>법티 파트 업로드 전형한 객체의 경우 에타 데이터 수정 / 이름 바꾸기 / 북사 / 이동 기능을 사용할 수 입</li> <li>또한, 모니티킹 범의 객체 수, 용량이 일치하지 않을 수 있습니다.</li> </ul>	(습니다.			
	객체 월터 Q				객체 수 : 1
	이름	최종 수정일시	크기	유형	
	choonsik.jpeg	2024.06.18 16:35	5.33 KB	jpeg	:
사용자 가이드 🛛				페이지 당 행 수 : 10 🗸	< >
	[그림 4.2.3] Object Storage 콘솔	게뉴에서 파일	입 이동 환	<u> </u>	

# 4 참고 사항

▶ 카카오클라우드 Object Storage 〉 객체/파일 관리 가이드



# 4.3. 암호키 서비스 관리자 권한 통제

#### 1 기준

식별번호		기관	E E		내용
10	암호키	서비스	관리자	권한	· 클라우드 암호키 서비스 이용 시 관리자 권한은 최소인원
4.3	통제				에게 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 기능 없음
- ▶ 카카오클라우드 내부에서 사용하는 암호 키(File, Object Storage 암호화용)관리 시스템의 접근 인원은 최소한으로 권한을 부여하여 관리

## 4 참고 사항

► N/A



# 4.4. 암호키 호출 권한 관리

#### 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 기능 없음
- 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, 검토

#### 4 참고 사항

► N/A



# 4.5. 안전한 암호화 알고리즘 적용

## 1 기준

식별번호	기준	내용
4 5	아저하 아ㅎ히 아그리즈 저요	암호화 기능 이용 시 안전한 암호화 알고리즘을 적용하여야
4.0	인신인 암오와 철고니금 식용	한다.

## 2 설명

▶ 암호화 기능 이용 시 안전한 암호화 알고리즘을 적용하여야 한다.(또는 확인하여야 한다.)

- (예시)
  - 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 기능 없음
- ▶ 카카오클라우드 내부에서 사용하는 암호 키(File, Object Storage 암호화용)는 안전 암호화 알고리즘을 적용(256bit 이상)하여 암호화

# 4 참고 사항

► N/A



# 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, 호출일시등)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



로깅 및 모니터링 관리



# 5.1. 가상자원 이용(생성, 삭제, 변경 등)에 관한 행위추적성 확보

#### 1 기준

5

식별번호	기준	내용
Б 1	가상자원 이용(생성, 삭제, 변경	이용자의 가상자원(서버, 데이터베이스, 스토리지 등) 이용
5.1	등)에 관한 행위추적성 확보	관련 행위추적성(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
    - 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

#### 1) 가상자원 변경 사항에 관한 행위(생성, 변경, 삭제 등)

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

iii kakao <b>cloud</b>			۵	서비스 검색			Q kr-central-2 ~	1 9 .
Cloud Trail	Cloud Trail > Event						• 로그 X	장 중 로그 저장 관리
S chudhach-main >	는 속성 이름을 입력해 주/	네요.		조회 항목: 조	직 이벤트 🗸 1일 전	1	✓ 총 187 건 중 1-50	< 이전 다음 >
Dashboard	이벤트 발생 시간 💠	이벤트 구분	이벤트 이름	사용자	사용자 고유 ID	서비스 이름	자원 유형	자원 이름
Event	2024.06.04 (화) 1	조직	Console Login	jd.new@kakacen	Shec799388154.	IAM	Domain	kakaon/oud-r
	2024.06.04 (화) 1	조직	Console Logout	kanın orşcoroğik.	1antorfeete?(246.	IAM	Domain	kalkastististed r
	2024.06.04 (화) 1	조직	Console Login	henry inglikakaon.	706829/Dac/1641.	IAM	Domain	hahammined r
	2024.06.04 (화) 1	조직	Console Logout	kri-orgeorrafikak.	674adc5d7154142.	IAM	Domain	kakamon kaka
	2024.06.04 (화) 1	조직	Payment View	scloud r india@g.	08-05-75-05-53-41.	Billing	Payment	
	2024.06.04 (화) 1	조직	Free Credit View	utrud i indiaĝija.	0848-775476-5341 -	Billing	Credit	
	2024.06.04 (화) 1	조직	Billing Report View	icloud.cirdia@g.	084575455341	Billing	Billing Report	
	2024.06.04 (화) 1	조직	Billing Report View	clout reduips.	054575455341.	Billing	Billing Report	
	2024.06.04 (화) 1	조직	Cost Report View	scloud r india@g.	0848-775476-5341 -	Billing	Cost Report	
	2024.06.04 (화) 1	조직	Console Login	harry youngkaka.	9525e757437546.	IAM	Domain	kakasistinud r
	2024.06.04 (화) 1	조직	Console Login	andrew.changglà	40atas30049154.	IAM	Domain	kakacrichoud r
	2024.06.04 (화) 1	조직	Console Logout	andrew chang@k	40aba300d9754	IAM	Domain	kakacii:/inud-r
사용사 가이드 亿	2024.06.04 (화) 1	조직	Console Logout	harry prongitatia.	9625e757637546.	IAM	Domain	Rathanic/Inud-r

[그림 5.1.1] Cloud Trail 의 조직 이벤트 확인

iii kakao <b>cloud</b>			٩	서비스 검색		•	kr-central-2 ~	- 1 0 -
Cloud Trail	Cloud Trail > Event							
프로젝트	Event						• 로:	그 저장 중 로그 저장 관리
۵ · · · · · ·	~ 속성 이름을 입력해 주	세요.		조회 항목: 프	로젝트 이벤트 🖌 1일 (	4 .	~ 총 55 건 중 1-5	50 < 이전 다음 >
Dashboard	이벤트 발생 시간 💠	이벤트 구분	이벤트 이름	사용자	사용자 고유 ID	서비스 이름	자원 유형	자원 이름
Event	2024.06.04 (화) 1	프로젝트	Choose Project	ern-offiskaoert	653562xdx71543.	IAM	Project	chould ach main
	2024.06.04 (화) 1	프로젝트	Choose Project	erin oğlakasını.	653542+4x71443	IAM	Project	cloudlach-main
	2024.06.04 (화) 1	프로젝트	Choose Project	ern ogkakaoert.	65.5562mdx/1449.	IAM	Project	cloudlach-main
	2024.06.04 (화) 1	프로젝트	Choose Project	erin oğlubasert.	653562w3x75843.	IAM	Project	cloudlach-main
	2024.06.04 (화) 1	프로젝트	Choose Project	justin koolojjikak.	CEub-4259(517274).	IAM	Project	cloudbach-main
	2024.06.04 (화) 1	프로젝트	Choose Project	virrie pojikakane.	01172519895e4d.	IAM	Project	cloudtech-main
	2024.06.04 (화) 0	프로젝트	Public IP Update	poly hysorificati.	RabertStation.	VPC	Public IP	
	2024.06.04 (화) 0	프로젝트	Public IP Update	polity hymorofikak	Rabati Shalline .	VPC	Public IP	
	2024.06.04 (화) 0	프로젝트	Public IP Create	polity hyperrylikask.	Robertsteation.	VPC	Public IP	
	2024.06.04 (화) 0	프로젝트	Choose Project	polty hymorofikak.	GaberShallin.	IAM	Project	cloudinch-main
	2024.06.04 (화) 0	프로젝트	Target Group Cre	coudach-main@	6F5730bb-6031-48.	Load Balancing	Target Group	prof.1_kuba_am.
	2024.06.04 (화) 0	프로젝트	Target Group Cre	cloudlech-mamp.	499730564021-48.	Load Balancing	Target Group	pool, 1, Julie, per.
사용자 가이드 🖸	2024.06.04 (화) 0	프로젝트	Load Balancer Cr	cloudbach-main@	675730bb603148	Load Balancing	Load Balancer	habe, service, cla-

[그림 5.1.2] Cloud Trail의 프로젝트 이벤트 확인



▶ (Console) 프로젝트 선택 후 'Dashboard' → 'Cloud Trail' → 'Event' 에서 가상자원 이용에 관한 행위를 이벤트로 확인한다.

× kakao <b>cloud</b>	Q. 서비스 검색	🍳 kr-central-2 🗸 🗗 🗓 🕐 ၊ 匡				
④ 최근 사용	IAM 세분화된 리스스 접근 제어 및 권한 관리 기능을 제공합니다. 사용자의 역할에 맞는 리스스 접근					
\$\$ 전체 서비스	· 권한불 부여하고, 리소스를 인천하게 관리할 수 있습니다.					
즐겨찾기 Beta	Monitoring     메트릭, 로그 기반의 정책을 설정하여 컴퓨팅 리소스의 상태와 변화를 모니터링 할 수 있습니다.					
자주 사용하는 서비스를 목록에서 추가하세요.						
카테고리	관리합니다.					
Beyond Compute Service	Cloud Trail     사용자의 활동을 자동으로 수집, 기록하는 서비스입니다. 로그인, 리소스 생성, 변경, 삭제 등의 활동을     가려서게 조직 교리하 스 이슈니 IL	84 ×3+				
Beyond Networking Service	- 긴민야계 가역, 린미을 두 있습니다.	-				
Container Pack		2024.25.25				
Beyond Storage Service		2004.04.05				
Data Store		2014.05.08				
Developer Tools						
Analytics						
Management >						
Al Service		Â				
Billing		Bare Metal Server				
[그림 5.1.3] 카카오클라우드 곤솔에서 Cloud Irall 서비스로 이동						

Kakaocioad							·	
Cloud Trail	Cloud Trail > Event							
<u>E</u>	Event						• =	그 저장 중 로그 저장 관리
cloudlash-main	~ 속성 이름을 입력해 주	세요.		조회 항목: 전	체 조희 🗸 1일 7	2	~ 총 <b>117</b> 건 중 1-	50 < 이전 다음 >
hboard	이벤트 발생 시간 💠	이벤트 구분	이벤트 이름	사용자	사용자 고유 ID	서비스 이름	자원 유형	자원 이름
nt	2024.06.03 (월) 1	조직	Console Login	eupera.son@kak	12072-02845445	IAM	Domain	Rolling Chinades
	2024.06.03 (월) 1	프로젝트	Choose Project	erin oğluşkapert.	653582#dx75849.	IAM	Project	cloudbach-main
	2024.06.03 (월) 1	조직	Console Login	ern-ogkakapert	65.7542.wdx?%\$49	IAM	Domain	half-accorder.
	2024.06.03 (월) 1	조직	Console Logout	jure (22gRahare -	ef957871475346	IAM	Domain	kalkarrichted-r
	2024.06.03 (월) 1	조직	Domain Role Ass	vincent anycom	788023#575#944	IAM	User	vincent anycom.
	2024.06.03 (월) 1	조직	Console Login	hazəl orycorruğik	76591#75656640.	IAM	Domain	Robbarovichioud+
	2024.06.03 (월) 1	조직	Console Login	andrew chang@k	40aba300d91b4	IAM	Domain	hallanci (houd-r
	2024.06.03 (월) 1	조직	Console Login	vincent anycom.	788023x575x444.	IAM	Domain	National -
	2024.06.03 (월) 1	조직	Console Login	single 121 (propri-	212125e0bc504	IAM	Domain	Radiansis (Strad) -
	2024.06.03 (월) 1	조직	Console Login	chiomest's gyop	SaceEdcol40224e	IAM	Domain	National -
사용자 가이드 [2]	2024.06.03 (월) 1	조직	Console Logout	chioment's gauge.	haceblock0224e.	IAM	Domain	kakaciclinud-r

#### 2) 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 있다.



(예시)

- Ubuntu 계열 Linux 의 경우 /var/log/auth.log 파일을 확인한다.
- CentOS 계열 Linux 의 경우 /var/log/secure 파일을 확인한다.
- 카카오클라우드는 Data Store(MySQL, Redis), File Storage 서비스와 같은 Managed Service 의 경우 사용자가 직접 OS에 접근할 수 없다. 따라서, 해당 서비스들로 생성된 자원의 경우 접속 일시, 접속자, 접근기록을 필요로 하지 않는다.
- 3) 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 있다.

	kakao <b>cloud</b>		Q, 서비스 검색		• kr-central-2 ·	۵	i (?	•
4	Alert Center	Alert Center 〉 알림 정해 아그리 저 차비			아리 저희 미나요	사제		571
프로젝트		28 84		월일 양의 사용	월명 영의 비사용 · 구성	억제	28 3 4 D	
0	cloudtech-main >	👻 속성 이름을 입력해 주세요.			총 <b>2</b> 건 중 1-2	< 이전	다음 >	S
	[그림 5.1.5] Alert Center의 알림 정책 만들기							

1 알림 조건 설정	1단계: 알림 조건	1 설정 ☺		
<ol> <li>2 수신 채널 설정</li> <li>3 기본 정보 설정</li> </ol>	조건 유형	이 메트릭 이 로그 💿 이벤트		
4         검토	서비스	Virtual Machine 🗸		
	조건 설정	인스턴스 재시작 × 전체 삭제		
		이벤트 항목 선택		
		조건 #1 이벤트 항목		
		인스턴스 재시작		
		취소 다음		
[그림 5.1.6] 인스턴스 재시작 이벤트 설정				



Alert Center > 알림 정책 > 알림 정책 만들기							
알림 정책 만들기							
카카오클라우드 콘솔에서 제공하는 서비스의 이벤트 및 알림을 받기 위한 알림 정책을 생성합니다.							
1 알림 조건 설정	2단계: 수신 채널 설정						
조건 유형 : 이벤트 서비스 : Virtual Machine							
조건 : 1개	수신 채널	메인 채널 유형	수신 채널				
2 수신 채널 설정		이메일 🗸	~				
3 기본 정보 설정		十 채널 추가					
4 검토		<ul> <li>여러 개의 수신 채널을 추가히 장됩니다.</li> </ul>	면 각 채널마다 알림이 발생하며 중복되는 채널은 제거하여 1	개 항목으로 저			
			_				
이전 다음							

☆ [카카오클라우드] Instance Reboot (Virtual Machine) 알림				
✓ 보낸사람 옷 no-reply@kakaoenterprise.com ⊘		2024-06-26 15:36 (GMT +0900)		
	Virtual Machine 알림			
	설정된 알립 정책에 의한 메시지입니다. 자세한 내용은 카카오클라우드 콘솔의 Alert Center에서 확인해 주세요.			
	조건 유형 이벤트			
	알림			
	서비스 Virtual Machine			
	이벤트 인스턴스 재시작			
	리소스	= 44		
	리소스 유형 Instance	+ 더보기		
[그림	- 5.1.8] 인스턴스 재시작 이메일 알림			


▶ 카카오클라우드의 Cloud Trail 이벤트 목록에서 가상 자원의 이벤트 로그를 확인할 수 있다.

::: kakao <b>cloud</b>		[	۵	서비스 검색		•	r-central-2 v	di 🗎 🕐 📧
	2024.06.26 (0) 1.	24	Console Logout	peeps songipts.		0.00	Domain	kakaorotoud+r
	2024-08-26-(*) 1.	2.1	Console Logn	prosph.song@ka	76,85716344643	0.03	Domain	kaloactic/toud-r
프로젝트	2024-06-26 (*) 1.	2.5	Console Logn	andrew.chang@k	40aba000497541.	0.00	Domain	kakacit/trud+
	2024-06-25 (*) 1.	2.1	Console Logn	hazel onycomiĝik.	75521#5555643.	0.000	Domain	kalkanichud-r
대시보드	2024.06.26 (수) 1	프로젝트	Instance Reboot	erin.o@kakaoent	6b3b82eda7fd49	Virtual Machine	Instance	host-172-16-2-12
이벤트	2024-06-26 (*) 1.	0.0755	Alert Policy Create	erin sijikakasent.	653582wdx71545.	Allert Center	Alast Policy	entro-resultant
	2024-06-26-(*) 1.	2.11	Console Loge	em.s@sakapert.	65.3582mda.76643.	0.00	Duman	kakacit/isud-r
	2024-06-26 (*) 1.	2.4	Consolie Logout	kr. onycorreĝikak	674ad:52754142.	U104	Domain	hahaciclinadir
	2024-06-26 (4) 1	2.11	Console Logout	harry youngkaka	9525e707c37545.	0.004	Dumain	kakacic/loud+
	2024-06-26 (*) 1.	2.11	Console Logeut	hazəf.orycoroğk	76571#75608642	UNIX	Domain	haliant/foud-r
	2024-06-26-(*) 1	2.11	Console Logeut	andress changijik	40454300(91541	0.00	Domain	hallacrichtud-r
	2024-06-26-(+) 1.	2.4	Payment Value	whend r indiaging .	08457545550.	0.0mg	Payment	
	2024-06-26 (*) 1.	2.1	Free Credit View	icloud - india@g.	0845754756341.	Billing	Credit	
	2024-06-26 (†) 1	2.11	Billing Report View	eloud / indiaĝig.	054575455341.	Billing	Billing Report	
	2024-06-26 (*) 1.	2.11	Billing Report View	kloud rindsajby.	084575455341	0.0mg	Billing Report	
사용자 가이드 🖸	2024-06-26 (*) 1.	2.9	Cost Report View	eloud / india@g.	08467754755341.	Billing	Cost Report	
[]	1림 5.1.9]	Cloud	Trail에서	인스턴스	재시작 0	벤트 로그	1 확인	

▶ 카카오클라우드 Monitoring 서비스를 통해 생성된 가상 자원의 주요 메트릭 정보를 확인할 수 있다.

Monitoring	Monitoring > 대시보드					
15	대시보드				수정 복제 삭제	대시보드 만들기
) 1185	i Monitoring에서 제공 Grafana 등 써드파티	3하는 Metric Export 엔드포인트를 이용하여 I에서 Monitoring 데이터를 확인하실 수 있습니다. 자세	한 내용은 가이드를 확인해주세요. <del>사용자 가이</del> !	E 12		
색기	· · · 속성 이름 혹은 값을 입	력해 주세요.			총 7 건 중 1-7 < 이전	다음 > ( )
	유형 ≑	이름 수	설명	생성자 💠	생성 일시 💠	
	기분	Beyond Compute Service	Beyond Compute Se	-	-	:
	기본	MySQL	MySQL 기본 대시보드	-		:
	기본	Redis	Redis 기본 대시보드	-		:
	기본	Load Balancing	Load Balancing 기본	-	+	:
	기본	Kubernetes Engine	Kubernetes Engine	-	-	:
	커스텀	david, test		david emglikakasenterpri	2024.05.23 (목) 18:56:39	:
	커스텀		Tanat .	viteria joĝkakacertistorio.	2024.05.07 (화) 14:16:31	:
사용자 가이드 🖸						





[그림 5.1.11] Beyond Compute Service 기본 대시보드

ections (Counts)	MySQL - Slow Quer           4.71           3.71           2.71           1.71	y (Counts)
06.26 15.58 06.26 16:15	471 371 272 171	
06.26 15.58 06.26 16:15	3 21 2 21 1 21	
06.26 15:58 06.26 16:15	2.7i	
06.26 15:58 06.26 16:15	1 개	
06.26 15:58 06.26 16:15	0.78	
	06.26 16:32 06.26 15:41 0	5.26 15:58 06.26 16:15 06.26 16:32
Max Current Aver	age 🔽 범례	Max Current Average
onn680 680 680	Slow Query	0 0 0
.ock Wait (Counts)	MySQL - Binary Log	ı (Bytes)
	256 B	
	Max         Current         Aver           nn         680         680         680           nn         1         1         1	Max         Current         Average         ☑ 10           xm680         680         680         680           xmn1         1         1         1







	1시간전 3시간전 12시간전 1일전 7일전	사용자화 자동 새로고침 안 함 🗸
CPU 사용량 (millicores)	Memory 사용량 (Bytes)	Disk 사용량 (Bytes)
4000	16.764 GB	
3000	12.573 GB	
2000	8.382 GB	
1000	4.191 GB	
0 06.26 15:43 06.26 16:00 06.26 16:17 06.26 16:34	0 Bytes 06.26 15:43 06.26 16:00 06.26 16:17 06.26 16:34	
2 범레 Min Max Average	V 범레 Min Max Average	
- Limit 4000 4000 4000	🗹 — Limit 15.622 GB 15.622 GB 15.622 GB	표시할 데이너가 없습니다.
Request 250 250 250		
	TX Network (hyte/s)	예양되 CPI 컨프틱 유량 (%)

- 4) 가상자원내 전산자료의 처리 내용을 확인할 수 있는 사용자 로그인, 엑세스 로그 등 접근기록
- 금융회사에서는 가상자원으로 구성한 정보처리시스템 내 전산자료(소스코드, 고객정보, 회사정보 등)에 대한 처리 로그(전산자료의 수정 및 삭제, 접근 등)를 수집하여야 한다.

## 4 참고 사항

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



# 5.2. 가상자원 이용 행위추적성 증적 모니터링

### 1 기준

식별번호		기준		내용
F 0	가상자원	이용	행위추적성	가상자원 이용에 관한 행위추적성 증적에 대해 모니터링
5.Z	증적 모니	터링		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
  - 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 고객사 SIEM 연동 기능을 제공하여 행위추적성에
   대한 적극적인 모니터링 가능하도록 지원하고 있습니다
- KAKAOCLOUD CloudTrail 로그를 Pub/Sub 서비스를 활용하여 고객사에서 보유하고 있는 SIEM과 연동할 수 있는 가이드를 제공하며, 이용자가 능동적으로 행위추적성에 대해 모니터링 및 주기적으로 검토할 수 있는 기반 환경 지원
  - + 대상 SIEM : Logpresso, Splunk

### 1) 공통

- ▶ KAKAOCLOUD 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



::: kakao <b>cloud</b>			Q 서비스 검색		kr-central-2 🗸 🗗 🗓 🧷 🗉 🗉
Vub/Sub (Apha)	Pub/Sub > Topic			-	
프로젝트	Topic 💿	토픽 만들기		×	+ 토팩 만들기
Topic	토릭 필터	토픽 이름	test-topic		
Subscription	토픽 이름 👙	기본 서브스크립션 📀	<ul> <li>생성 실성 안함</li> </ul>		생성자 💠
	Default-Topic	메시지 보존 기간	0 일 0 시간 10 분		patite kantefördessertingelse som
			최소 10분에서 최대 7일까지 설정할 수 있습니다.		페이지당행수: 10    1-1    /1    >
		토픽 설명(선택)	100자 이내로 착성		
			취소 저장		
사용자 가이드 안					
		[그림	님 5.2.1] 토픽 만들 <u>기</u>		

::: kakao <b>cloud</b>		Q, 세비쇼 웹세
Pub/Sub (Alpha)	Pub/Sub $>$ Subscription $>$ $k$	(브스크립션 만들기
프로젝트	서브스크립션	만들기
Topic	기본 설정	서브스크립션 이름 pubsub-subscribtion
Subscription		토픽 선택 text topic
		restropic
	서브스크립션 타입	Pull 구독자가 전송을 요청해야 합니다
		Push     에시지가 게시되는 즉시 Pub/Sub에서 에시지를 전승입니다.     고프트로 사용     에디디디디드 UD 용 이런에 또 NO
		Image: Second
		IPu바음 선택한 경우, Ark를 활용한 에시지 요청과 용답 확인이 필요합니다. 자세한 내용은 가이드 문서 산품 참고매주세요.
사용자 가이드 🖸		취소 만들기
[=]	1림 5.2.2] 사	1브스크립션 타입을 Push로 하여 서브스크립션 만들기



III kakao <b>cloud</b>		Q 서비스 검색	• kr-central-2 ·	di 🛓 🕐 🗉
🕰 Alert Center	Alert Center > 수신 채널 > 수신	1 채널 만들기		
프로젝트	<b>수신 채널 만들기</b> Alert Center에서 알림 정책 생성 A	1 달림을 판송하기 위한 채널을 생성합니다.		
알림 정책 수신 채널	수신 채널 이름	pubsub		
발신 내역 조직	수신 채널 설명 (선택)	100자 이내로 작성		
말림 정책 (조직) 수신 채널 (조직)	메인 채널 유형	기본채널 슬랙 램흑 🖲 Pub/Sub		
발신 내역 (조직)				
		test-topic v		
사용자 가이드 안		취소 만들기		
		[그림 5.2.3] 수신 채널 만들기		

Alert	Center > 알림 정책 > 알림 정책 만들기				
<b>알</b> i 카카의	<b>림 정책 만들기</b> 오클라우드 콘솔에서 제공하는 서비스의 이	벤트 및 알림을 받기 위한 알림 정책을 생성합니다	ł.		
		이나라. 스시 테너 서저			
1	알림 조건 설정	2단계: 주신 새널 실성			
	조건 유형 : 이벤트 서비스 : Container Registry				
	조건 : 1개	수신 채널	메인 채널 유형	수신 채널	
2	수신 채널 설정		Pub/Sub ~	pubsub	
3	기본 정보 설정		十 채널 추가	pubsub 📀 사용중	
4	검토		<ul> <li>여러 개의 수신 채널을 추가하</li> <li>장됩니다.</li> </ul>	면 각 채널마다 알림이 발생하며 중복되는 채널은 제거하여 1개 §	방목으로 저
			/오 스시케너우	서태들(어 아리 저채은 마드	71
		기전에 민들이군 Pub	/Sub 구신세걸굴	신백이어 걸림 징색을 빈글	

## 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)



			<b>1</b>	♥ 보안정보	🕐 대시보드	<b>숙</b> 수	집 🛟 분석	므 대응	Q, 정책	(오) 계정	88 앱
수집	4	수집기 추가								<b>√</b> ₫	인 🗙 취소
수집 설정		공통 설정									
파서		이름		CLOUDTRAIL			자산 IP	선	택		
로그 스키마		실행 방식		주기			주기		5 초		
TUII		수집 노드		control			센트리	선	택 안 함		
		수집 모델		cloudtrail			테이블	CL	OUDTRAIL		
		설명		설명 입력 (최대 2,0	00자)						
		수집 설정									
		콜백 이름		cloudtrail			/log/콜백이름				
		필터 설정									
		정규식 패턴									
		대상 필드		미 입력시 기본값: li	ne						
		필터 방식		패턴 매칭된 로그만	수집						

▶ 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

		# *	🛡 보안정보	🏤 대시보드	< 수집	🖨 분석	묘대용	Q, 정책	😩 গন্ত	<b>:::</b> 앱	🔅 시스템	[
<	수집 모델 수정					-			v 1	4연 × 취소		
	설정											
	이름		cloudtrail									
	설명		설명 입력 (최대									parsejson overlay=t field=line
	유형		HTTP POST									l explode messages
	파서		선택 안 함									I parsemap overlay=t field=messages
	원본 × +										-	I parsemap overlay=t field=message
	정규화 규칙											I eval data=frombase64(data)
	이름		원분									l eval data=decode(data)
	로그 스키마		원분									I parseman overlay-t field-event
	스트림 취리		parsejson over   explode mess   parsemap ov   parsemap ov   eval data=fro   eval data=der   parsejson ov   parsemap ov   fields - mess	rlay=t field=line sages erlay=t field=messa mbase64(data) code(data) erlay=t field=data erlay=t field=data ages, - message, - c	ages age data, - event							I fields - messages, - message, - data, - event
	새로고침 주2		60 歳									
												L
				[그림	5.	2.61	Lo	apr	ess	0 1	딬드	값 Decode 석정 예시하면

▶ 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)

			12	10
ACTIVE		10 분		서브스크립션 시점 되돌리기
사용자 Topic!           i         카카오클라우!	의 <b>서브스크립션 타입이 Push</b> 인 경우, 시큐· 드 Public IP를 사용한 앤드포인트 URL로민	리티 그룹의 인바운드 정책 설정이 필요합니 Push가 가능합니다. Message Push 관련	니다. (Source IP : 61.109.238.137, 6 김 자세한 내용은 가이드 문서 [2를 참고	51.109.238.0, 61.109.237.249, 61.109.238.114, 61.109.238.74, 61.109.236. 2하세요.
세부 정보	메시지			
너브스크립션 ID	55c1	dc7f	서브스크립션 이름	cloudtrail
병성자	jı ii@k e.com		생성일시	2024.01.18 (목) 10:13:55
너브스크립션 타입	Push		엔드포인트 URL	http:// 8888
응답 대기 시간	20 초		미처리 메시지 개수	0 71
토픽 이름	cloudtrail-s t		토픽 메시지 보존 기간	10 분
너브스크립션 베시지 보존 기간	10 분		재처리 횟수	3회

- ▶ 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

t	able •:CLOUDTRAIL ields publish_time region resou	Irce_name service_r	name name subscription project_id project_name					실행 초
«	< 1 > » 27	<u>H</u>					ES .	초 ▼ III 표시 개수 (
#	A publish_time	A region	resource_name	A service_name	A name	Subscription	A project_id	project_name
1	2024-01-16T07:07:15Z	kr-central-2	host-10 156 (mart )	Virtual Machine	Instance Shelve	cloudtrail-	ca71 7271	kr2-
2	2024-01-16T06:44:14Z	kr-central-2	host-10228 (cloudtrail-: :)	Virtual Machine	Instance Reboot	cloudtrail	ca7 7271	kr2-
			[그림 5.2.8] SIEM	(Logpres	sso) 로그	1 수집 예시	화면	

### 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)



데이터 추가 <sub>원</sub>	● <b>○ ○ ○</b>	· [유] · · · · · · · · · · · · · · · · · · ·
<b>파일 및 디렉터리</b> 파일을 업로드하거나 로컬 파일을 인덱스하거나 전체 디렉터리를 모니터링합 니다.	HTTP를 통해 데이터를 수신하기	위한 새 토큰을 설정합니다. 자세히 알아보기 [건
HTTP Event Collector 클라이언트가 HTTP 또는 HTTPS를 통해 데이터를 보내기 위해 사용할 수 있는 토큰을 설정하십시오.	이름 Source 이름 재정의 ?	KC_cloudtrail 선택 사항
TCP / UDP 네트워크 포트에서 수신 대기하도록 Splunk 플랫폼을 설정합니다.	설명 ?	선택 사항
스크립트 스크립트를 사용하여 API, 서비스 또는 데이터베이스에서 데이터를 가져옵니	출력 그룹(선택 사항)	없음 ▼
ч.	인덱서 수신확인 기능 활성화	
[그림 5.2.9] SIEM(Sp	lunk) HTTP Even	t Collector 설정 예시화면

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

인덱스					
Splunk 플랫폼은 수신한 데이터의 source type 스를 만들어서 사용할 수 인덱스에 영향을 주지 않 든지 이 설정을 변경할 수	한 데이터를 선택된 을 파악하는 데 문제 〉 있습니다. 테스트 않고 설정 문제를 해 수 있습니다. 자세히	인덱스에 이벤트  가 있는 경우 "티 용 인덱스를 사용 결할 수 있습니디   알아보기 [건	트로 저장합니다. 테스트용" 인덱 용하면 프로덕션 다. 나중에 언제		
허용되는 인덱스 선	사용 가능항목	모두 추가 »	선택됨항목	« 모두 제거	
택	≣cim_modacti	ons	🗉 cloudtrail		
	© cloudtrail				
	≣ fortigate				
	Ehistory				클라이언트가 선택할 수 있는 인덱스를 선택합니다.
기본 인덱스	🗉 cloudtrail 🔻	새 인덱스	만들기		
	[그림 5.2	2.10] SIEN	/(Splunk) Ir	ndex 설정	예시화면

▶ 다음 구성을 검토하고 제출을 클릭하여 저장

금융분야 상용 클라우드컴퓨팅서비스 보안 관리 참고서 5. 로깅 및 모니터링 관리

	데이터 추가	원본 선택	입력 설정	검토	<b>O</b> 완료	< 뒤로	제출 >
검토							
입력 유형 이름	토큰 KC_cloudtrail						
Source 이름 재정의 설명	해당 사항 없음 해당 사항 없음						
 인덱서 수신확인 기능 활성화 출력 그룹	아니요 해당 사항 없음						
허용되는 인덱스	cloudtrail						
기본 인덱스	. cloudtrail 자도						
앱 컨텍스트	. search						
[그림 5.2.]	11] SIEM(Splunk) F	ITTP Eve	nt Colleo	ctor 설	정예시	니화면	

- 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

전역 설정 편집		×
모든 토큰	사용 가능	사용 불가능
기본 Source Type	Source	Type 선택 ▼
기본 인덱스	7	본값 -
기본 출력 그룹	Ê	었음 ▼
배포 서버 사용		
SSL 사용	$\checkmark$	
HTTP 포트 번호 <sup>?</sup>	8088 (기본 값 또는 사용자 임의로 변경	· 한 값 입력)
		취소 저장
	[그림 5.2.12] 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)



- ▶ 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



- ▶ 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 (<u>가이드</u>)



서브스크립션 상태		서브스크립션 메시지 보존	트 기간	기능	
ACTIVE		10 문		서브스크립션 시점 되돌리기	
사용자 Top	i <b>c의 서브스크립션 타입이 Push</b> 인 경우, 시큐	리티 그룹의 인바운드 정책 설정이 필요	합니다. (Source IP : 61.109.238.137, 6	1.109.238.0, 61.109.237.249, 61.109.238.114, 61.109.238.74, 61.109.23	6.65)
· 카카오클라	우드 Public IP를 사용한 엔드포인트 URL로민	Push가 가능합니다. Message Push	관련 자세한 내용은 가이드 문서 🖸 🖻 참고	:하세요.	
세부 정보	메시지				
서브스크립션 ID	55c1	dc7f	서브스크립션 이름	cloudtrail	
냉성자	ju ii@k e.com		생성일시	2024.01.18 (목) 10:13:55	
서브스크립션 타입	Push		엔드포인트 URL	http:// 8888 📋	
응답 대기 시간	20 초		미처리 메시지 개수	0 개	
토픽 이름	cloudtrail-s t		토픽 메시지 보존 기간	10 분	
서브스크립션 케시지 보존 기간	10 분		재처리 횟수	3회	
					_

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

index=cloudtr	ail				
<b>4개의 이벤트</b> (24/0 <sup>-</sup>	1/18 13:00:00.000	0 ~ 24/01/19 1	3:32:17.000)	이벤트 샘플링 없	음 ▼
벤트 <b>(4)</b> 패턴	통계 시그	화			
시간 표시줄 형식 지정	형 ▼ - 축소	+ 선택 항	목 확대/축소	X 선택 취소	
필드 표시 테	이블 ▼	식 페이지	당 20개 ▼		
_time	host ‡	source ‡	sourcetype	index ‡	messages().message.data ‡
24/01/19 1:00:15.000	210.109.2.80	cloudtrail	httpevent	cl	eyJhbGFybV92ZXJzaW9uljogInYxLjAuMCIsICJhbGFybV9uYW1lljogImN
24/01/18 19:23:55.000	210.109.2.80	cloudtrail	httpevent	cloudtrail	eyJhbGFybV92ZXJzaW9uljogInYxLjAuMCIsICJhbGFybV9uYW1lijogImN
24/01/18 19:23:45.000	210.109.2.80	cloudtrail	httpevent	clearly "	eyJhbGFybV92ZXJzaW9uljogInYxLjAuMCIsICJhbGFybV9uYW1lljogImN
24/01/18 18:34:15.000	210.109.2.80	cloudtrail	httpevent	cleadauil	eyJhbGFybV92ZXJzaW9uljogInYxLjAuMCIsICJhbGFybV9uYW1lljogImN
		[그림 !	5.2.16] <u>S</u>	EM Splu	nk 로그 조회 예시화면



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

앱							
개 항목 중 11-1 표시							
decrypt	Q						
이름 •		폴더 이름 🗲	버전 🕈	업데이트 확인 ♥	표시 여부 🕈	공유 중 🕈	상태 🕈
DecryptCommands		decrypt2	2.4.1	Yes	No	전역   권한	사용 가능   비활성화
		[그림	5.2.17] SI	EM Splunk	앱 설치 예시화[	<u>.</u>	

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

1 index=cloudtrail 2   rename "messages() message.data" as data 3   decrypt field=data atob() emit('decode')	최근 24시간 ▼ Q
√ <b>4개의 이벤트</b> (24/01/18 13:00:00.000 ~ 24/01/19 13:30:28.000) 이벤트 샘플링 읍	음▼ 작업▼ !! ■ ☆ 총 ± ■ 상세모드▼
이벤트(4) 패턴 통계 시각화	
시간 표시줄 형식 지정 ▼ - 축소 + 선택 항목 확대/축소 × 선택 취소	컬림당 1시간
> 필드 표시 테이블 ▼ / 형식 페이지당 20개 ▼	
i _time host \$ source \$ sourcetype \$ index \$	decode \$
> 24/01/19 210.109.2.80 cloudtrail httpevent cloudtrail 1:00-15.000	<pre>("alarm_version": 'v1.0.0", "alarm_name": "cloudtra t', "alarm_id": "f7d722e59435451ab9de5b3234f3tcc5", "service_name": 'Virtual Machine", "alarm_type": "EVENT", "event_time": "2024-01-19101:00:309:00", "project_id": "ce "," "domain_id": "region="," reg", "link": "https://console.kakaolio/alert-center/alert-policies/f7d722e59435451ab9de5b3234f3tcc5? "geion="," resource_name": "," "resource_type": "Snapshot Create"; "source_type": "Snapshot Create"; "source_type": "Snapshot", "une: ": "2024-01- 19101:00:03+09:00"; "domain_id": "32737ac52974577a79a5e26b26c27e9"; "domain_name": "*"project_id": "ca7" "1"project_iname": "kc":setup-default"; "region": "kr-central-2"; user_id": "b2"b2")</pre>
> 24/01/18 210.109.2.80 cloudtrail httpevent cloudtrail 19:23:55.000	(*alarm_version*: 'v10.00*, *alarm_name*: *cloudtrail
	이 이디자 아내네는 티코드 코그 에너티머

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



발신 내역 필터		Q		조회 기간: 2024.01.13 - 2024.01.19
반일시 ≑	알림 정책 🍦	서비스 🗢	알림 조건	발신 상태
2024.01.19 01:00:08	cloudtrail- t 🖸	াখ্রছ Virtual Machine	이벤트: 스냅샷 생성	● 성공 1 🛛 💙
2024.01.18 19:23:53	cloudtrai 🗾 🛂	<u>াখ্য≡</u> Virtual Machine	이벤트: 인스턴스 시작	● 성공 1 V
2024.01.18 19:23:43	cloudtrail 2	<u>াখ≡</u> Virtual Machine	이벤트: 인스턴스 중지	● 성공 1   ❤
2024.01.18 18:34:13	cloudtrail-	াল্ল Virtual Machine	이벤트: 인스턴스 재시작	● 성공 1   ❤
2024.01.18	cloudtrail- t 🖸	이벤트 Virtual Machine	이벤트: 인스턴스 재시작	● 성공 1 🛛 💙

# 4 참고 사항

- ▶ 카카오클라우드 〉 AlertCenter 가이드 참고
- ▶ 카카오클라우드 〉 Pub/Sub 가이드 참고
- 카카오클라우드에서 연동 제공하는 SIEM은 Logpresso, Splunk 대상이며, 이 외의 SIEM은 추가적인 검토 필요



#### 5.3. 이용자 가상자원 모니터링 기능 확보

#### 기준 1

식별번호	기준	내용
Б <b>2</b>	이용자 가상자원 모니터링 기능	이용자 가상자원 운용에 관한 모니터링 기능을 확보하여야
0.0	확보	한다.

#### 설명 2

▶ 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

### 1) 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 가능하다.

	✔ 신작 정지 재사작 경제·제사작 종료 인스탠스 삭제 인스탠스 작업 +
프로젝트	
△ doutleth man	
인스턴스	세우 정보 데트웨크 보안 2 출급 이 적김 도그 보니버형
볼륨	기본 모니터링 상세 <b>모니터링</b>
스냅샷	
스냅샷 일정	1시간전 3시간전 12시간전 1일전 7월전 오
0[0]X]	
키페어	CPU - 총 사용량 (%)
	0.09%
	06.03 1/21/ 06.03 1/22/ 06.03 1/244 06.03 1801
사용자 가이드 안	



모니터링 에이전트가 설치된 상태에서 Alert Center 서비스의 수신 채널 설정 및 알림 정책 설정 후 메트릭, 로그, 이벤트를 트리거로 알림을 수신할 수있도록 설정 가능하다.

🗳 Alert Center	Alert Center > 알림 정책 > 알림 정최	비만들기			
프로젝트	알림 정책 만들기				
۵ (میرامی) ،	카카오클라우드 끈들에서 제공하는 서비	스피 이벤트 및 알림을 받기 위한 알림 정치	1을 생성합니다.		
알림 정책					
수신 채널	1 알림 조건 설정	1단계: 알림 조건	1 설정 💿		
발신 내역	2 수신 채널 설정				
조직		조건 유형	🔹 메트릭 🔷 로그 🔷 이벤트		
turkanis fraukt	3 기본 정보 설정				
알린 전책 (조직)	4 검토	서비스	Beyond Compute Service	~	
수신 채널 (조직)					
발신 내역 (조직)			고니터링 조건을 설정하기 위해서는 인스턴 사용자 가이드를 확인 후 모니터링 에이전트	-에 모니터링 에이전트 설치가 필요합니다. 설치를 진행해 주세요.	
		조건 설정	④ 설정한 조건들은 개별 동작하며, 논리합(OR) 조건으	로 동작합니다.	
			조건 #1	<b></b>	
			메트릭 항목 ⊚		
			Cpu Usage	~	
			자원 💿	예상 알림 : 1	
			인스턴스	~ ]	
			with manifest about Salida Made with a		
			0.701±1	コをリアームアロ	
			☆XI- % ~	이상 수자 문 후기금 수	
			취소 다음		

- ▶ 그 외 Managed 형태의 서비스 중 일부(Load Balancing, MySQL, Redis)는 기본 대시보드를 통해 모니터링 정보 제공
  - (Console) 'Dashboard' → 'Monitoring' → '대시보드' 목록에서 기본으로 제공되는 Load
     Balancing, MySQL, Redis 대시보드 확인 가능

④ 최근 사용	IAM 세분화된 리소스 접근 제어 및 권한 관리 기능을 제공합니다. 사용자의 역할에 맞는 리소스 접근	
🚼 전체 서비스	권한을 부여하고, 리소스를 안전하게 관리할 수 있습니다.	
즐겨찾기 Beta	Monitoring     에트릭, 로그 기반의 정책을 실정하여 컴퓨팅 리소스의 상태와 변화를 모니터링 할 수 있습니다.	
자주 사용하는 서비스를 목록에서 추가하세요.	Alert Center	**
	가가오늘려누느 끈들 시미스에서 끈들 사용사에게 날림을 보내기 위한 말림 정석 및 주신 세달을 통합 관리합니다.	
Beyond Compute Service	Cloud Trail     사용자의 활동을 자동으로 수집, 기록하는 서비스입니다. 로그인, 리소스 생성, 변경, 삭제 등의 활동을	
Beyond Networking Service	간편하게 추적, 관리할 수 있습니다.	
Container Pack	CERTIFICATION CONTRACTOR CONTRACTOR	2024.00.00
Beyond Storage Service	CONTRACTOR CONTRACTOR CONTRACTOR CONTRACTOR	2024.01.21
Data Store	Name and States and States and an	2004.01.00
Developer Tools		
Analytics		
Management >		
Al Service		
Billing		Bare Metal Server
	A16 A164	Regard Compute Service
	Malak and Bila	해야나 방도의 인정으로 해당해 관계할 수 있습니다. 물론 사가로 물론적으로 환경해 관계할 수 있습니다.



iii kakao <b>cloud</b>		Q 서비스 검색			♥ kr-central-2 ~	1 🤊 - 🖪
프로젝트	Monitoring > 대시보드 대시보드				수정 복제 삭제	대시보드 만들기
C · · ·	<ul> <li>Monitoring에서 제공하는 Metric</li> <li>Grafana 등 써드파티에서 Monito</li> </ul>	Export 엔드포인트를 이용하여 ring 데이터를 확인하실 수 있습니다. 자세한 내용은 기	이드를 확인해주세요. <del>사용자 가</del> 이	5 B		
탐색기	속성 이름 혹은 값을 입력해 주세요.				총 6건 중 1-6 < 이전	다음→   <b>3</b>
	유형 💠 이름 🗧	)	설명	생성자 💠	생성 일시 💠	
	기본 Beyor	nd Compute Service	Beyond Compute S	-	-	:
	기문 MySC	L	MySQL 기본 대시보	-	-	:
	기분 Redis		Redis 기본 대시보드		-	:
	기문 Load	Balancing	Load Balancing 7	-	-	:
	커스범	land .		david am@kakacenterpri	2024.05.23 (목) 18:56:39	:
	커스텀		1002	einna jojikakaoenterpro	2024.05.07 (화) 14:16:31	:
사용자 가이드 亿						
1 I						

### [그림 5.3.4] 기본 대시보드 확인

	3시간전 12시간전 1일전 7일전 사람	자화 자동 새로고침 안 함 🗸
인바운드 트래픽 (bytes/sec)	아읏바운드 트래픽 (bytes/sec)	CPS (Counts/sec)
4 B/s	4 B/s	4
3 B/s	3 B/s	3
2 B/s	2 B/s	2
1 B/s	1 B/s	1
0 B/s	0 B/s	0
06.03 17:36 06.03 17:53 06.03 18:10 06.03 18:27		
06.03 17:36 06.03 17:53 06.03 18:10 06.03 18:27	에 관심되어 Min Max Average	2 러스테 ID Min Max Average
06.03 17:36 06.03 17:53 06.03 18:10 06.03 18:27 같 리스닉 ID Min Max Average 같 — listener_a7_0 B/s 0 B/s 0 B/s Concurrent Session (Counts)	같으며 Hall Dollar Hall Color Hall	같스너 ID Min Max Average 같스너 ID Min Max Average 같 → listener_a7_0 0 0
06.03 17:36 06.03 17:53 06.03 18:10 06.03 18:27 오리스니 ID Min Max Average 오 — listener_a7_D B/s D B/s D B/s Concurrent Session (Counts)	로 리스니 ID Min Max Average ☑ — listener_s708/s 08/s 08/s	Id⇒l (10     Min     Max     Average       Image: Source of the second state of
06.03 17:36 06.03 17:53 06.03 18:10 06.03 18:27	같으며 Fills 같스니 ID Min Max Average 같 — listener_a7_0 8/s 0 8/s 0 8/s	Image: State of the state



<ul> <li>✓ 전체 조회항목 (6) ↓</li> </ul>	시간 천 3시간 전 1일 전 7일 전	사용자화 자동 새로그침 안 함 🗸
lySQL - 초당 수행 쿼리 (QPS)	MySQL - Connections (Counts)	MySQL - Slow Query (Counts)
3/s	800 7#	4.74
25/s	600 개	3 개
1.5/s	400 개	2.78
75/s	200 개	1 개
0/s	0.78	0 71
6.03 17:43 06.03 18:00 06.03 18:17 06.03 18:34	06.03 17:43 06.03 18:00 06.03 18:17 06.03 18:34	06.03 17:43 06.03 18:00 06.03 18:17 06.03 18:34
6.03 17:43 06.03 18:00 06.03 18:17 06.03 18:34 같 범죄 Max Current Average 같 — QPS 2.8518518519 2.811111111 2.8225865209	06.03 17:43 06.03 18:00 06.03 18:17 06.03 18:34 전 범래 Max Current Average       ····································	06.03 17.43 06.03 18:00 06:03 18:17 06:03 18:34 전 번역 Max Current Average 준 — Slow Query 0 0 0
6.03 17:43 06.03 18:00 06.03 18:17 06.03 18:34 양 범력 Max Current Average 양 — QPS 2.8518519 2.8111111111 2.8225865209 ySQL - 유형별 5분간 쿼리 횟수 (Counts)	06.03 17:43 06.03 18:00 06.03 18:17 06.03 18:34 오 병례 Max Current Average 오 취태 Conn 680 680 680 오 위험 Conn 1 1 1 MySQL - Row Lock Wait (Counts)	06.03 17.43         06.03 18:00         06:03 18:17         06:03 18:04           Image: The state of the stat
A CO 317.43 06.03 18:00 06.03 18:17 06.03 18:34 같 범택 Max Current Average 같 - QPS 2.8518519 2.8111111111 2.8225865209 YSQL - 유형별 5분간 쿼리 횟수 (Counts)	06.03 17:43 06.03 18:00 06.03 18:17 06.03 18:34	06.03 17:43 06.03 18:00 06.03 18:17 06.03 18:34
06.03 17:43 06.03 18:00 06.03 18:17 06.03 18:34 같 편책 Max Current Average 같 -	06.03 17:43 06.03 18:00 06.03 18:17 06.03 18:34	06.03 17:43         06.03 18:00         06.03 18:17         06.03 18:14           값         Max         Current         Average           값         —         Slow Query 0         0         0

### [그림 5.3.6] MySQL 기본 대시보드

	전:	녜 조회항목 (4) 🗸 14	시간 전 12시간 전 1일 전	7일 전 사용자화 자동 새로고침 안	함 ~
edis - 명령 별 호출 (Count/	sec)		Redis - Connections (Counts)	Redis - Cache hit Ratio (%)	
18			10000 개	4%	
75\$			7500 개	3%	
0.5念			5000 78	2%	
25회			2500 78	1%	
0.2			0.21	0%	
auth 0.4	0.4 0.2	0.4	<ul> <li>✓ — 활성 Conn 1</li> <li>1</li> <li>✓ — 최대 Conn 10000</li> <li>10000</li> </ul>	🕑 — Hit ratio 0 0	0
🗹 — info 0.3	0.3	0.3			
♥ — info 0.3 edis - 만료 및 제거된 키 (Co	0.3 Dunts)	0.3	CPU - 총 사용량 (%)	Memory - 총 사용량 (%)	
✔ — imfo 0.3 edis - 만료 및 제거된 키 (Ca	0.3 Dunts)	0.3	CPU - 총 사용량 (%)	Memory - 총 사용량 (%) 8%	
Image: symplectic symplecti symplecti symplectic symplectic symplectic symplectic symplecti	0.3 Dunts)	0.3	СРU - Š + 88 (%) 1% 0.75%	Memory - 총 사용량 (%)	
edis - 만료 및 제거된 키 (Cd           4개           3개           2개	0.3 punts)	0.3	СРU - 층 사용량 (%) 1% 0.75%	Memory - 총 사용량 (%)           0%           0%           4%	

### 2) 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 가능하다.





### [그림 5.3.8] 모니터링 에이전트 설치

III kakao <b>cloud</b>		Q, 서비스 주	뷥쎅			<b>Q</b> Global	() 1
④ 계정 설정		kapitaconcinoued +					
		이름					
계정 정보		242			0		
IAM 역할		닉네임 (선택) 💿					
액세스 키		win.o			O		
비밀번호 변경		사용자 아이디 📀					
언어 설정		erin oğlukaserterprise com					
		사용자 고유 아이디					
		45.3582eds/10494351cad3d556625964			Ē		
	연락처 정보	연락용 이메일 주소					
		erin ağlılakaserterprisa.com		인증변	번호 발송		
		인증번호 입력	유효 시간 05:00	취소	저장		
		휴대폰 번호 (선택)					
		+82 ~		인증법	번호 발송		
		인증번호 입력	유효 시간 05:00	취소	저장		
	IAM 사용자 등록일	2023.12.22 (금) 14:55:46					
	[그림 539	) 사용자 계정정보0	에서 연란처	정부	인증	및 섭정	



ert Center > 수신 채널 > 수신 채널	만들기				
<b>누신 채널 만들기</b> ert Center에서 알림 정책 생성 시 알림	을 전송하기 위한 채널을 생성합니다.				
신 채널 이름	한글, 영문 대·소문자, 숫자, '-', '-'만 입력 (4~50자	)			
-신 채널 설명 (선택)	100자 이내로 작성				
인 채널 유형	<ul> <li>● 기본채널 슬랙 웹축 Pu</li> </ul>	b/Sub			
	• 🗹 이메일	○ 📮 문자	이 🔎 알림톡		
	③ 문자, 알림쪽은 신백한 수신자의 ID를 통해 IAM에서 휴대폰 번호를 조회하여 발신합니다.				
	등록 가능한 수신자 목록 10	선택한 :	수신자 목록 0	전체 삭제	
	이메일 또는 이름으로 사용자 격색	이 지수 전들기 지수 전들기 이 지수 전들기 지수 전들이 지수 전들이 지수 전들기 지수 전들기 지수 전들이 지수 전들이 지수 전들이 지수 전들기 지수 전들이 지수			
	e <b>t Center ) 수상재료 ) 수신재료</b> > <b>신 채널 만들기</b> ert Center에서 일립 정책 생성 시 일립 신 채널 이름 신 채널 설명 (신택) 인 채널 유형				

[그림 5.3.10] 수신 채널 생성

iii kakao <b>cloud</b>		Q 세비스:	검색	• kr-central-2 ·	_ ≞	() I
🕰 Alert Center	Alert Center > 알림 정책 > 알림 정책 만들기					
프로젝트	<b>알림 정책 만들기</b> 카카오클라주드 콘솔에서 제공하는 서비스의 이민 	<sup>#트</sup> 및 알림을 받기 위한 알림 정책을 생성합니	<b>ц</b> .			
알림 정책 수신 채널 발신 내역	1 알림 조건 설정 2 스시 채너 성제	1단계: 알림 조건 설정	D			
조직	2 구년 세골 물망 3 기본 정보 설정	조건 유형	• 메트릭 🤇 로그 🔵 이벤트			
알림 정책 (조직)	4 검토	서비스	Beyond Compute Service		~	
수신 채널 (조직) 발신 내역 (조직)			고니타링 조건을 설정하기 위해서는 인스턴스에 모니터링 에 사용자 가이드를 확인 후 모니터링 에이전트 설치를 진행해 주	기전트 설치가 필요합니다. 세요.		
		조건 설정	① 설정한 조건들은 개별 동작하며, 논리할(OR) 조건으로 동작합니다.			
			조건 #1 메트릭 향목 ⊚	Ŧ		
			메트릭 항목 선택		~	
사용자 가이드 건			취소 다음			
[]	그림 5.3.11] 메트	릭, 로그, 이벤	트를 트리거로 한 알림	정책 생성		

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

kakao <b>cloud</b>		Q, 서비스 검색		♥ kr-central-2 ~ 世 1
작업 중인 프로젝트 🛛				
프로젝트 이름:				변경
공지사항				전체 보기 (
<mark>안내</mark> 'Data Catalog' 업데이트 인	반내 (06/03)			2024.06.03
안내 'Kubernetes Engine' 업데이	이트 안내 (5/31)			2024.05.31
안내 'Monitoring' 서비스, endpo	oint, path 변경 사전 안내 (6/13, k	r-central-2)		2024.05.28
서비스 목록 22 (Wirtual Machin Beyond Compute Servit	ne œ	GPU Beyand Compute Service		Earn Mathal Sequer
Instance	33 EA	Instance	1 EA	Beyond Compute Service
VCPU	130 EA	VCPU	24 EA	뛰어난 성능과 안정성을 제공하는 물리 서버를 클라우드 환경에 구축할 수 있습니다.

kakao <b>cloud</b>	소개	서비스	마켓플레이스	파트너	리소스	고객지원	기술문서	공공기관용 🦻	(	Console	회원가입
	카카오클리 안전하고 신	ት우드는 신속한 고?	객 지원 서	비스를 :	제공합니	니다					
	<b>전체</b> 안내	점검 보인	ŀ					Q, 검색어를 입력	해주세요.		
	유형				제목				등록일		
	안내	NEW 'Data	i Catalog' 업데이트	안내 (06/03)					2024. 6. 3		
	안내	NEW 'Kube	ernetes Engine' 업대	헤이트 안내 (5/	31)				2024. 5. 31	1 I	요금계산기
	안내	NEW 'Mon	itoring' 서비스, end	point, path 변	경 사전 안내 (6	/13, kr-central-2	)		2024. 5. 25	🖍 상담 및	도입 문의
	점검	NEW 카카스	오클라우드 서비스 {	반정화를 위한 점	범검 작업 예정 (	한내(6/4)			2024. 5. 28		$(\uparrow)$
	[그림 !	5.3.13]	카카오클	라우드	- 포털	에서 혹	인할 수	> 있는 공지	시항		

### 3) 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 가능하다.



### [그림 5.3.14] 모니터링 에이전트 설치

::: kakao <b>cloud</b>		Q, 서비스 검색			<b>Q</b> Global	di 1 ? 🛛 E
④ 계정 설정		kakant foud -				
		이름				
계정 정보		242		Ø		
IAM 역할		닉네임 (선택) 💿				
액세스 키		arin.a		Ø		
비밀번호 변경		사용자 아이디 💿				
언어 설정		erin official acenterprise.com				
		사용자 고유 아이디				
		653b82m3x76494381cmd3db56657964		6		
	연락처 정보	연락용 이메일 주소			1	
		erin sijikakaoenterprise.com		인증번호 발송		
		인증번호 입력	유효 시간 05:00	<b>취소</b> 저장		
		휴대폰 번호 (선택)				
		+82 ~		인증번호 발송		
		인증번호 입력	유효 시간 05:00	<b>취소</b> 저장		
	IAM 사용자 등록일	2023.12.22 (己) 14:55:46			-	
	[그림 5.3.1	5] 사용자 계정정보에	서 연락처	정보 인령	등 및 설정	

iii kakao <b>cloud</b>		Q 서비스 검색		♀ kr-central-2 ~						
🕰 Alert Center	Alert Center > 수신 채널 > 수신 채널	d 만들기								
프로젝트	수신 채널 만들기 Alert Center에서 얄립 정책 생성 시 얄럽	김을 전송하기 위한 채널을 생성합니다.								
알림 정책 수신 채널	수신 채널 이름	<b>수신 채널 이름</b> 한글, 영문 대·소문자, 숫자, <sup>-1</sup> , <sup>-1</sup> 만 입력 (4~50자)								
발신 내역 조직	수신 채널 설명 (선택)	100자 이내로 작성								
말림 정책 (조직) 소시 채널 (조직)	메인 채널 유형	● 기본채널 _ 슬랙 _ 웹혹 _ P	Pub/Sub							
발신 내역 (조직)		<ul> <li>이메일</li> </ul>	- 문자	🔷 🕮 알림톡						
		(i) 문자, 알림톡은 선택한 수신자의 ID를 통해 IAMG	에서 휴대폰 번호를 조회하여 발신합니다.							
		등록 가능한 수신자 목록 10	0	선택한 수신자 목록 0	전체 삭제					
사용자 가이트 건		이메일 또는 아름으로 사용자 검색	취소 만들기							

[그림 5.3.16] 수신 채널 생성

iii kakao <b>cloud</b>		Q, 서비스 3	ৰূপ 🗘 kr-central-2 - d	I I 🤊 - E
🕰 Alert Center	Alert Center > 알림 정책 > 알림 정책 만들기			
프로젝트	<b>알림 정책 만들기</b> 카카오클라우드 콘솔에서 제공하는 서비스의 이벤	트 및 알림을 받기 위한 알림 정책을 생성합니	9.	
알림 정책 수신 채널 발신 내역	1 알림 조건 설정 2 수신 채널 성정	1단계: 알림 조건 설정 🛛		
조직	3 기본 정보 설정	조건 유형	<ul> <li>● 메트릭 ○ 로그 ○ 이벤트</li> </ul>	
알림 정책 (조직) 수신 채널 (조직)	4 검토	서비스	Beyond Compute Service	•
발신 내역 (조직)			<ul> <li>소나타킹 조건물 불명야가 체력시는 전츠인드에 조나타킹 에너인드 불소가 참보합니다.</li> <li>사용자 가이드를 확인 후 모나타킹 에이전트 철치를 진행해 주세요.</li> </ul>	
		조건 설정	<ul> <li>○ 설정한 조건들은 개별 등직하며, 논리법(OR) 조건으로 등직합니다.</li> <li>조건 #1</li> <li>● ①</li> <li>····································</li></ul>	
사용자 가이드 강			에트리 항목 선택 · · · · · · · · · · · · · · · · · ·	
[	그림 5.3.17] 메트	릭, 로그, 이벤	트를 트리거로 한 알림 정책 생성	

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

kakao <b>cloud</b>		Q, 서비스 검색		Q kr-central-2 ∽			
작업 중인 프로젝트 🛛							
프로젝트 이름:					변경		
공지사항					전체 보기 @		
안내 'Data Catalog' 업데이트 안내 (06/03) 안내 'Kubernetes Engine' 업데이트 안내 (5	안내         'Data Catalog'업데이트 안내 (06/03)         2024.06.03           안내         Kubernetes Engine'업데이트 안내 (5/31)         2024.05.31						
안내 Monitoring 서비스, endpoint, path 면	1경 사전 안내 (6/13, kr-central-2)				2024.05.28		
저미스 폭독 22		_					
Virtual Machine Beyond Compute Service	(	Beyond Compute Service		Bare Metal Server			
Instance	33 EA In	stance	1 EA	Beyond Compute Service 뛰어난 성능과 안정성을 제공하는			
	IJUEA	7FV	24 EA	물리 서버를 클라오드 화경에 구추할 수 있습	L IFL		

kakao <b>cloud</b>	소개	서비스 마켓플레이스	파트너 리소스	고객지원	기술문서	공공기관용 🗷	Co	nsole 회원가입
	카카오클라 안전하고 신	우드는 l속한 고객 지원 서	비스를 제공합니	니다				
	<b>전체</b> 안내	점검 보안				Q 검색어를 입력해주세요.		
	유형		제목			등록일		
	안내	NEW 'Data Catalog' 업데이트	안내 (06/03)			2024.	6. 3	
	안내	NEW 'Kubernetes Engine' 업	데이트 안내 (5/31)			2024. 5	. 31	🖩 요금계산기
	안내	NEW 'Monitoring' 서비스, en	dpoint, path 변경 사전 안내 (6	/13, kr-central-2)		2024. 5	· 25	상담 및 도입 문의
	점검	NEW 카카오클라우드 서비스	안정화를 위한 점검 작업 예정	안내(6/4)		2024. 5	. 28	$\uparrow$

▶ 사용자는 알림과 공지를 참조하여 장애상황기록를 작성한다.

### 4) 가상자원 네트워크 정책 변경(삭제 등) 모니터링

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



iii kakao <b>cloud</b>	Q. 세비.	스 경색	♥ kr-central-2 · 🗍 🛓 ?	) ' 🗉
Cloud Trail	Cloud Trell > Deshboard Dashboard			
프로젝트 C · ·	프로젝트 이벤트 현황		15.74	
Dashboard	조회 기간   2024.05.28 ~ 2024.06.03 ● Block Storage Instance Project Public IP Security Group 1 ● VPC Snapshot 2024.05.28 2024.05.29 2 최근 프로젝트 이벤트 목록	Listener Backup Keypair Alert Policy Load Balancer	· Target Group • Health Check • Bucket • Image 9 2024.06.02 2024.06.03 전체 이벤트 기록 보기	→
	이벤트 발생 시간 이벤트 이름 사용자	사용자 고유 ID 서비스 이를	자원 유형 자원 이를	
	2024.06.03 (절) 19: Shapshot Create 2024.06.03 (월) 18: Public IP Delete	VPC	Public IP -	
사용자 가이드 亿	2024.06.03 (월) 17: Public IP Update	VPC	Public IP -	
	2024.06.03 (월) 17: Choose Project	IAM	Project	
	[그림 5.3.20] Cloud T	rail 서비스의 Dashboar	rd	

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

iii kakao <b>cloud</b>		Q 서비스 김	냄석	🗣 kr-central-2 🗸 📑 🕄 🛛 E
Cloud Trail	Cloud Trail > Event			<ul> <li>로그 사장 중</li> <li>로그 처장 권리</li> </ul>
۵ ,	~ 속성 이름을 입력해 주세요.		조회 항목: 전체 조회 ^ 1일 전	★ 총 223 건 중 1-50 < 이전 다음 →
Dashboard	이벤트 발생 시간 ≑ 이벤트 구분	이벤트 이름 사용:	· 전체 선택 서비:	스 이름 자원 유형 자원 이름
Event	2024.06.03 (월) 1 프로젝트	Snapshot Create -	▼ 조직 이벤트 :d4 Virte	ual Machine Snapshot
	2024.06.03 (월) 1 프로젝트	Snapshot Create -	☑ 프로젝트 이벤트 cd4 Virte	ual Machine Snapshot
	2024.06.03 (월) 1 조직	Payment View	Billin	ng Payment -
	2024.06.03 (월) 1 조직	Free Credit View	Billin	ng Credit -
	2024.06.03 (월) 1 조직	Billing Report View	Billi	ng Billing Report -
	2024.06.03 (월) 1 조직	Billing Report View	Billin	ng Billing Report -
	2024.06.03 (월) 1 조직	Cost Report View	Billi	ng Cost Report -
	2024.06.03 (월) 1 조직	Console Login	IAM	Domain
	2024.06.03 (월) 1 조직	Console Login	IAM	Domain
	2024.06.03 (월) 1 조직	Console Logout	IAM	Domain
	2024.06.03 (월) 1 조직	Console Login	IAM	Domain
	2024.06.03 (월) 1 조직	Console Login	IAM	Domain
사용사 가이는 년	2024.06.03 (월) 1 조직	Console Login	IAM	Domain
[그림 5.	.3.21] 조직 이벤트	와 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 한다.



iii kakao <b>cloud</b>			(	Q, 서비스 검색		_	Q kr	-central-2 ~	
Cloud Trail	Cloud Trail > Event								
프로젝트	Event							• 로그?	해장 중 로그 저장 관리
<u>ہ</u>	· · · 속성 이름을 입력해					×	~	총 <b>223</b> 건 중 1-50	< 이전 다음 >   ;
Dashboard	이벤트 발생 시간 💠	로그 저장 관	리				기름	자원 유형	자원 이름
Event	2024.06.03 (월) 1		<b>•••</b>	용			Machine	Snapshot	
	2024.06.03 (월) 1	로그 저장 옵션	로그 저장어 한 시간마디	l 3회 연속 실패 시, 자동으로 미시 h 저장소 버킷에 저장됩니다.	·용으로 변경됩니다. 생성된 로그는		Machine	Snapshot	
	2024.06.03 (월) 1		✓ 조직	이벤트 포함				Payment	•
	2024.06.03 (월) 1	이벤트 저장 범위	범위 프로젝트 이벤트는 기본적으로 저장됩니다. 해당 옵션을 체크하면 조직 지 포함하여 저장합니다.		해당 옵션을 체크하면 조직 이벤트	까		Credit	•
	2024.06.03 (월) 1		- and the second	Lizzef 1				Billing Report	-
	2024.06.03 (월) 1	저장소 버킷	로그 저장 8	용량에 따라 요금이 부과됩니다. <b>C</b>	Dbject Storage 요금 정책 보기 큰			Billing Report	-
	2024.06.03 (월) 1		저장소의 비 로그는 복구	킷을 삭제할 경우, 정상적으로 로 "할 수 없습니다. Object Storage	:그가 저장되지 않으며 삭제된 : C			Cost Report	
	2024.06.03 (월) 1			지수 전용				Domain	
	2024.06.03 (월) 1							Domain	
	2024.06.03 (월) 1	조직	Console Logout	forder progler.	Roberts, Service,	IAM		Domain	
	2024.06.03 (월) 1	조직	Console Login			IAM		Domain	
	2024.06.03 (월) 1	조직	Console Login			IAM		Domain	
사용사가이드 전	2024.06.03 (월) 1	조직	Console Login	ante orgenerative.	and the second second	IAM		Domain	Summer Courts

# 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



#### API 사용(호출대상, 호출자, 호출일시등)에 관한 행위추적성 확보 5.4.

#### 기준 1

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

### 2 설명

▶ API 사용 이력에 대한 행위추적성을 확보하여야 한다.

- (예시)

1) API 호출에 관한 정보(호출대상, 호출자, 호출일시 등)

# 3 우수 사례

▶ 카카오엔터프라이즈에서는 현재 API 행위추적성 확보에 대한 기능이 제공되지 않아, 이용 고객(금융 회사 등)은 API 사용 이력에 대한 별도 행위추적성 확보 필요

## 4 참고 사항

► N/A



# 5.5. 네트워크 관련 서비스(VPC, 보안그룹, ACL 등)에 관한 행위추적성 확보

### 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 제공한다.

Cloud Trail	Cloud Trail > Dashboard	
프로젝트	Dashboard	
۵ · · · ·		
Dashboard	<b>프로젝트 이벤트 현황</b> 조희 기간   2024.05.28 ~ 2024.06.03	1주전 🗸
Event	Block Borage Instance Project Public IP Security Group Listener Backup Keyair Alert Policy Load Balance Target Group H	20 2022.06.03
	최근 프로젝트 이벤트 목록	전체 이벤트 기록 보기 →
	이벤트 발생 시간 이벤트 이를 사용자 사용자 고유 ID 서비스 이를 자원 유형	자원 이를
	2024.06.03 (1) 19: Snapshot Create Virtual Machine Snapshot	
	2024.06.03 (월) 18: Public IP Delete VPC Public IP	-
	2024.06.03 (월) 17: Public IP Update VPC Public IP	
사용자 가이드 🖸		



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

iii kakao <b>cloud</b>		Q. 서비스 검색		• kr-central-2 ·	
Cloud Trail	Cloud Trail > Event			• =	저장 중 로그 저장 관리
프로젝트	속성 이름을 입력해 주세요.		조희 항목: 전체 조희 ^ 1일 전	✓ 총 223 건 중 1-50	이 < 이전 다음 >   2
Dashboard	이벤트 발생 시간 💠 이벤트 구분	이벤트 이름 사용자	☑ 전체 선택	너비스 이름 자원 유형	자원 이름
Event	2024.06.03 (월) 1 프로젝트	Snapshot Create -	🗹 조직 이벤트 🛛 :d4 🗸	/irtual Machine Snapshot	
	2024.06.03 (월) 1 프로젝트	Snapshot Create -	☑ 프로젝트 이벤트 ;d4 V	/irtual Machine Snapshot	
	2024.06.03 (월) 1 조직	Payment View	and the second second	tilling Payment	
	2024.06.03 (월) 1 조직	Free Credit View	and all the second second	Silling Credit	-
	2024.06.03 (월) 1 조직	Billing Report View	entrajo, manifestore e	Billing Billing Report	
	2024.06.03 (월) 1 조직	Billing Report View	and the second second	Billing Billing Report	
[그림 5	5.2] 조직 이벤트	와 프로젝트 0	벤트로 구분되는	Cloud Trail 이번	<u> </u>

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

iii kakao <b>cloud</b>			Q, 서비스 검색		<b>♀</b> kr-	-central-2 ~ [	
Cloud Trail	Cloud Trail > Event						
프로젝트	Event					• 로그기	해장 중 로그 저장 관리
۰ ،	· · · 속성 이름을 입력해			×	~	총 <b>223</b> 건 중 1-50	< 이전 <b>다음 &gt;</b>   C
Dashboard	이벤트 발생 시간 💠	로그 저장 관리			기름	자원 유형	자원 이름
Event	2024.06.03 (월) 1		사용		Machine	Snapshot	
	2024.06.03 (월) 1	로그 저장 옵션	로그 저장에 3회 연속 실패 시, 자동으로 미사용으로 변경됩니다. 생성된 로그는 한 시간마다 저장소 버킷에 저장됩니다.		Machine	Snapshot	
	2024.06.03 (월) 1		✔ 조직 이벤트 포함			Payment	•
	2024.06.03 (월) 1	이벤트 저장 범위	프로젝트 이벤트는 기본적으로 저장됩니다. 해당 옵션을 체크하면 조직 이벤트/ 지 포함하여 저장합니다.	ŀ		Credit	•
	2024.06.03 (월) 1					Billing Report	•
	2024.06.03 (월) 1	저장소 버킷	로그 저장 용량에 따라 요금이 부과됩니다. Object Storage 요금 정책 보기 간			Billing Report	•
	2024.06.03 (월) 1		저장소의 버킷을 삭제할 경우, 정상적으로 로그가 저장되지 않으며 삭제된 로그는 북구할 수 없습니다. Object Storage [2			Cost Report	•
	2024.06.03 (월) 1		취소 적용			Domain	Same and Same
	2024.06.03 (월) 1					Domain	
	2024.06.03 (월) 1	조직 Cons	iole Logout	IAM		Domain	
				_			
		[그림 5.5.:	3] 로그 저장 관리 설정 모	달			

## 4 참고 사항

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



# 5.6. 계정 변동사항에 대한 행위추적성 확보

### 1 기준

식별번호	기준	내용
БG	계정 변동사항에 대한 형	위 클라우드 계정 변동사항에 대한 행위추적성(로그 등)을 확보
5.0	추적성 확보	하여야 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

- 1) 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 제공한다.

::: Kakaocloud			م	、서비스 검색		•	r-central-2 ~	II U ()   []
Cloud Trail	Cloud Trail > Event						• 로그 자	1장 중 로그 저장 관리
	· 속성 이름을 입력해 주시	비요.		조회 항목: 전	체조희 🗸 3일 ?	9 ×		
Dashboard	서비스 이름 : IAM × )	필터 초기화					총 209 건 중 1-50	< 이전 <b>다음</b> > [2
Event	이벤트 발생 시간 💠	이벤트 구분	이벤트 이름	사용자	사용자 고유 ID	서비스 이름	자원 유형	자원 이름
	2024.06.03 (월) 1	조직	Console Login	0<0.000, y<0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.000, 0.0	$((x_1,x_2,x_3,x_3,x_3,x_3,x_3,x_3,x_3,x_3,x_3,x_3$	IAM	Domain	10000000000000000000000000000000000000
	2024.06.03 (월) 1	조직	Console Login	pringe hyperse (files).	Gaga_011111_0111100	IAM	Domain	4.445 (1997)
	2024.06.03 (월) 1	조직	Console Logout	6111/1000-00000-0000-0000-0000-0000-0000	$\sum_{i=1}^{n} (i-1)^{-1} \sum_{i=1}^{n} (i-1)^{-1} (i-1)^{$	IAM	Domain	Number 2017
	2024.06.03 (월) 1	조직	Console Login	14000-0010-001000	1.000 cm/s100 cm/s1000	IAM	Domain	
	2024.06.03 (월) 1	조직	Console Login	1070-000-00003264	e-,05,000-0,0	IAM	Domain	4 and 1 and 1 (1 and 1 -
	2024.06.03 (월) 1	조직	Console Login	6172-1121-1119[Ris.	<ul> <li></li></ul>	IAM	Domain	1.450 Control 1.100 Control 1.1000 Control 1.1000 Control 1.1000 Control 1.1000 Control 1.100 Contro
	2024.06.03 (월) 1	조직	Console Login	electrol any con-	100000000000000000000000000000000000000	IAM	Domain	Applicant Character
	2024.06.03 (월) 1	조직	Console Logout	proceeding and a second second	$g_{i}(t) \in [0,1]^{-1} \cup [1,1] \cup [1,1] \cup [1,1]$	IAM	Domain	10000000000000000000000000000000000000
	2024.06.03 (월) 1	조직	Console Logout	ense-segurig.		IAM	Domain	1
	2024.06.03 (웗) 1	조직	Console Logout	4-10-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1	4748-1772-114	IAM	Domain	
	2024.06.03 (월) 1	조직	Console Logout		10.000 (10.000 (10.000))	IAM	Domain	
사용자 가이드 🖸	2024.06.03 (월) 1	조직	Console Logout	10	4779-1471-1471-1471-1471	IAM	Domain	And the second of the second of

### [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 한다.

() Cloud Trail Clour 프로젝트	l Trail → Event ent								
프로젝트	ent								
								● 로그 제	장 중 로그 저장 관리
<u>ح</u> , Ξ	속성 이름을 입력해					×	~	총 <b>223</b> 건 중 1-50	< 이전 다음 >   오
Dashboard	벤트 발생 시간 💠	로그 저장 관리				^	비름	자원 유형	자원 이름
Event 20	024.06.03 (월) 1			· ee			Machine	Snapshot	
20	024.06.03 (월) 1	로그 저장 옵션	로그 저장어 한 시간마디	il 3회 연속 실패 시, 자동으로 미사+ i 저장소 버킷에 저장됩니다.	용으로 변경됩니다. 생성된 로그는		Machine	Snapshot	
20	024.06.03 (월) 1		🗸 조직	이벤트 포함				Payment	•
20	024.06.03 (월) 1	이벤트 저장 범위	프로젝트 이벤트는 기본적으로 저장됩니다. 해당 옵션을 체크하면 조직 이벤트끼 지 포함하여 저장합니다.			ŀ		Credit	
20	024.06.03 (월) 1							Billing Report	
20	024.06.03 (월) 1	저장소 버킷	로그 지장 용량에 따라 요금이 부과됩니다. Object Storage 요금 정책 보기 [					Billing Report	
20	024.06.03 (월) 1		저장소의 버킷을 삭제할 경우, 정상적으로 로그가 저장되지 않으며 삭제된 로그는 복구할 수 없습니다. Object Storage [2					Cost Report	
20	024.06.03 (월) 1							Domain	
20	024.06.03 (월) 1			n= 48				Domain	
20	024.06.03 (월) 1	조직 Co	onsole Logout	tolia projin.	Research	IAM		Domain	
20	024.06.03 (월) 1	조직 Co	onsole Login			IAM		Domain	
20	024.06.03 (월) 1	조직 Co	onsole Login			IAM		Domain	
사용자 가이드 선 20	024.06.03 (월) 1	조직 Co	onsole Login	and a sequence of the second	anaman'ny se	IAM		Domain	Same Provide State
	ſ	그리 토승	_ງ] ⊒	그 퍼지는 고난	기 서저 미	다			

- 2) 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 있다

kakao <b>cloud</b>	소개	서비스	마켓플레이스	파트너	리소스	고객지원	기술문서	공공기관용 🦻	Console 회원가입
j t	<b>Market</b> 카카오클라우드와 8 빠르게 비즈니스를	<b>plac</b> 함께하는 다 시작하세요.	<b>건</b> 양한 서비스를 활동	용하여					
	마켓플레이스 서비스	제휴 신청							
(	전체 (108)	~						Q 검색어를 입력해주서	표 요금계산기 II요. 27. 상담 및 도입 문의
		[기린	563]7	<b>ŀ</b> 7ŀQ≣	라우드	- - 코속(	이 마케	프레이스	

# 4 참고 사항

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



# 5.7. 계정 변경사항에 관한 모니터링 수행

### 1 기준

식별번호	기준	내용
Б <b>7</b>	계정 변경시항에 관한 모니터링	클라우드 서비스 이용 계정 변경사항(생성, 삭제 등)에 관한
5.7	수행	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 내부규정등에 수립된 주기에 맞추어 주기적 검토 수행
  - 3) 관리자 계정에 대해서는 이중확인 수행 등

### 3 우수 사례

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

Cloud Trail	Cloud Trail > Event							
	Event						• 23	지장 중 로그 저장 관리
프로젝트								
۵	는 속성 이름을 입력해 주.	세요.		조회 항목: 전	체 조희 🗸 3일 전	1	~	
Dashboard	서비스 이름 : IAM × *	필터 초기화					송 209 건 중 1-50	이 적 다음 ·
Event	이벤트 발생 시간 单	이벤트 구분	이벤트 이름	사용자	사용자 고유 ID	서비스 이름	자원 유형	자원 이름
	2024.06.03 (월) 1	조직	Console Login	10110/1011-00111-00111-00110-0011-0011-	622,-104120,-104-104.	IAM	Domain	
	2024.06.03 (월) 1	조직	Console Login			IAM	Domain	100000000000000000000000000000000000000
	2024.06.03 (월) 1	조직	Console Logout			IAM	Domain	Statistican St. Threads -
	2024.06.03 (월) 1	조직	Console Login		1 particular (* 1 1 1 1 1 1 1 1.	IAM	Domain	****
	2024.06.03 (월) 1	조직	Console Login			IAM	Domain	- Condition (C. 1999)
	2024.06.03 (월) 1	조직	Console Login		41-14750,00077-100400	IAM	Domain	
	2024.06.03 (월) 1	조직	Console Login			IAM	Domain	10.000 constant ( 10.0.000
	2024.06.03 (월) 1	조직	Console Logout			IAM	Domain	****
	2024.06.03 (월) 1	조직	Console Logout			IAM	Domain	10.000 million and 10.000 million
	2024.06.03 (월) 1	조직	Console Logout		40.000	IAM	Domain	*****************
	2024.06.03 (월) 1	조직	Console Logout			IAM	Domain	10.000 cm
사용자 가이드 [2]	2024 06 03 (別) 1	조직	Console Logout			IAM	Domain	

[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 한다.

iii kakao <b>cloud</b>				Q, 서비스 검색			<b>Q</b> kr	central-2 ~ [	
Cloud Trail	Cloud Trail > Event								
프로젝트	Event							• 로크 x	i장 중 로그 저장 관리
۵ · · ·	· 속성 이름을 입력해					×	~	총 223 건 중 1-50	< 이전 다음 >   3
Dashboard	이벤트 발생 시간 💠	로그 저장 괸	리				비름	자원 유형	자원 이름
Event	2024.06.03 (월) 1			사용			Machine	Snapshot	Second Second
	2024.06.03 (월) 1	로그 저장 옵션	로그 저 한 시간!	장에 3회 연속 실패 시, 자동으로 미사! 마다 저장소 버킷에 저장됩니다.	으로 변경됩니다. 생성된 로그는		Machine	Snapshot	
	2024.06.03 (월) 1		✓ 조	즉 이벤트 포함				Payment	
	2024.06.03 (월) 1	이벤트 저장 범위	프로젝트 지 포함:	트 이벤트는 기본적으로 저장됩니다. 히 하여 저장합니다.	당 옵션을 체크하면 조직 이벤트지	ŀ		Credit	
	2024.06.03 (월) 1			inf incl	~			Billing Report	
	2024.06.03 (월) 1	저장소 버킷	지장소 버킷 로그 저장 용량에 따라 요금이 부과됩니다. Object Storage 요금 정책 보기 [2					Billing Report	
	2024.06.03 (월) 1		저장소의 로그는 ·	리 버킷을 삭제할 경우, 정상적으로 로그 복구할 수 없습니다. Object Storage (	가 저장되지 않으며 삭제된			Cost Report	
	2024.06.03 (월) 1			취소 적용				Domain	
	2024.06.03 (월) 1		-					Domain	
	2024.06.03 (월) 1	조직	Console Logout	and the second sec	Roberts Cont.	IAM		Domain	
	2024.06.03 (월) 1	조직	Console Login			IAM		Domain	
11811 2015 12	2024.06.03 (월) 1	조직	Console Login			IAM		Domain	
	2024.06.03 (월) 1	조직	Console Login	and a sequence of the second s	automotion.	IAM		Domain	Salesting -
		[그림 5.	7.2] <u></u>	르그 저장 <u>관</u>	의 설정 <u>모</u>	달			

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

iii kakao <b>cloud</b>		Q, 서비스 강	색	♥ Global	] ⑦ + 🗉
🗳 Alert Center	Alert Center > 알림 정책				
프로젝트	알림 정책 만들기				
	카카오클라우드 콘솔에서 제공하는 서비스의 이벤! 	트 및 알림을 받기 위한 알림 정책을 생성합니!	ł.		
수신 채널	1 알림 조건 설정	1단계: 알림 조건 설정 🕻			
발신 내역	2 수신 채널 설정				
조직 <b>1</b> 1	3 기본 정보 설정	소선 유형	<ul> <li>이벤트</li> </ul>		
알림 정책 (조직)	4 검토	서비스	IAM	~	
수신 채널 (조직) 방신 내역 (조직)		조건 설정	선택된 이벤트 항목이 없습니다.		
			이벤트 항목 선택	^	
			사용자 추가 조직 권한 부여		
			조직 권한 해제		
사용자 가이드 亿			끈딸 로그바웃 콘솔 로그인		
	[그리 6	· · · · · · · · · · · · · · · · · · ·	베이 아리 저채 새서		
		5.7.5] 쪼씩 데	걸기 걸림 경색 생성		



# 2) 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 제공한다.

kakao <b>cloud</b>			۵	、서비스 검색			• kr-central-2 ·	
) Cloud Trail	Cloud Trail > Event						• 2:	1 저장 중 로그 저장 관리
젝트								
	· 속성 이름을 입력해 주세	요. Ini + nim		소의 양복: 선기	제 소의 🗸 3일 전		* 200 건 주 1.0	
ashboard	서비스 이동: IAM X 5 월	1너 소기와					5 209 2 8 14	
rent	이벤트 발생 시간 💠	이벤트 구분	이벤트 이름	사용자	사용자 고유 ID	서비스 이름	자원 유형	자원 이름
	2024.06.03 (월) 1	조직	Console Login	deciliar provigilar.	Colombar (1) - 1.	IAM	Domain	***********
	2024.06.03 (월) 1	조직	Console Login	pringrigeners@ingh.	6145440000000000000000000000000000000000	IAM	Domain	***
	2024.06.03 (월) 1	조직	Console Logout	decolution, proceeding the set of the set	$\ f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1}(x)-f_{n+1}^{-1$	IAM	Domain	10000000000000000
	2024.06.03 (월) 1	조직	Console Login	taran separatigh.	140000000000000000000000000000000000000	IAM	Domain	
	2024.06.03 (월) 1	조직	Console Login	1079-019101113ffa.	e-100000-0040	IAM	Domain	And report Clinical P
	2024.06.03 (월) 1	조직	Console Login	4172-1121-112264	4-275,00710240	IAM	Domain	100000000000000000000000000000000000000
	2024.06.03 (월) 1	조직	Console Login	attempts any com-	100000000000000000000000000000000000000	IAM	Domain	Subsection and s
	2024.06.03 (월) 1	조직	Console Logout	processing the state of the second se	470200-14702-004	IAM	Domain	10000000000000
	2024.06.03 (월) 1	조직	Console Logout	ense organity.		IAM	Domain	1.11.11.11.11.11.1
	2024.06.03 (월) 1	조직	Console Logout	entres during the	4748-017037-144	IAM	Domain	10201020111111111111
	2024.06.03 (월) 1	조직	Console Logout	parties in configuration.	60ap+67ap+17%	IAM	Domain	100000000000000000000000000000000000000
사용자 가이드 🖸	2024.06.03 (월) 1	조직	Console Logout	en	479aanda/1071-001	IAM	Domain	Aug Disso Collins of Co

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

iii kakao <b>cloud</b>									
Cloud Trail	Cloud Trail > Event								
I로젝트	Event							• 2	로 저장 중 로그 저장 관리
s ,	· · · 속성 이름을 입력해					×	~	총 223 건 중 1-5	0 < 이전 다음 >
Dashboard	이벤트 발생 시간 💠	로그 저장 관리	4				기름	자원 유형	자원 이름
Event	2024.06.03 (월) 1			나용			Machine	Snapshot	
	2024.06.03 (월) 1		로그 저장 옵션 로그 저장에 3회 연속 실패 시, 자동으로 미사용으로 변경됩니다. 생성된 로그는 한 시간마다 저장소 비킷에 저장됩니다.					Snapshot	
	2024.06.03 (월) 1		🗹 조직	이벤트 포함				Payment	•
	2024.06.03 (월) 1		이벤트 저장 범위 프로젝트 이벤트는 기본적으로 저장됩니다. 해당 옵션을 체크하면 조 지 포함하여 저장합니다.					Credit	
	2024.06.03 (월) 1		-	i iun 7	v			Billing Report	
	2024.06.03 (월) 1	저장소 버킷	로그 저장	로그 저장 용량에 따라 요금이 부과됩니다. Object Storage 요금 정책 보기 간				Billing Report	
	2024.06.03 (월) 1		1짓을 삭제할 경우, 정상적으로 로 7할 수 없습니다. Object Storage	그가 서상되지 않으며 삭제된 같			Cost Report		
	2024.06.03 (월) 1			취소 적용				Domain	
	2024.06.03 (월) 1							Domain	
	2024.06.03 (월) 1	조직	Console Logout	polar, proglar,	Schengelsens,	IAM		Domain	
	2024.06.03 (월) 1	조직	Console Login			IAM		Domain	
	2024.06.03 (월) 1	조직	Console Login			IAM		Domain	
사용자 가이드 亿	2024.06.03 (월) 1	조직	Console Login			IAM		Domain	

[그림 5.7.5] 로그 저장 관리 설정 모달


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

iii kakao <b>cloud</b>			Q, 서비스 검색			kr-central-2	
Cloud Trail	Cloud Trail > Dashboard						
Dashboard	<b>프로젝트 이벤트 현</b> 황 조회 기간   2024.05	<b>B</b> .28 ~ 2024.06.03					1주전 ~
Event	Block Storage In     VPC Snapshot     VPC Snapshot     VPC 30     VPC 20     VPC	223 724.05.28 202 트 목록	49 19 405 29 2024 05.3	rr Backup Keypair Al	ert Policy E Load Balancer	Target Group      Healt     2024.06.02	Check ■ Bucket ■ Image 20 2024.06.03 전체 이벤트 기록 보기 →
	이벤트 발생 시간	이벤트 이름	사용자	사용자 고유 ID	서비스 이름	자원 유형	자원 이름
	2024.06.03 (월) 19:	Snapshot Create		Conversion and	Virtual Machine	Snapshot	
	2024.06.03 (월) 18:	Public IP Delete	$e^{-i\omega_{-}} \sim \int_{0}^{\infty} \int_{0}^{\infty} df  dg  dg  dg  dg  dg  dg  dg $	0.000.04/1010.0	VPC	Public IP	-
	2024.06.03 (월) 17:	Public IP Update		0.000.000.0000.000	VPC	Public IP	

- 3) 관리자 계정에 대해서는 이중확인 수행 등
- ▶ 카카오클라우드에서는 Cloud Trail의 조직 이벤트에서 User Add, Delete, Group Assign 등 계정 변경사항에 대한 이벤트 기록을 제공한다.

::: kakao <b>cloud</b>		c	↓ 서비스 검색			Q kr-central-2 →	₫ ₫ ⑦ ⊨
Cloud Trail	Cloud Trail > Event					• ==	저장 중 로그 저장 관리
프로젝트	😇 속성 이름을 입력해 주세요.		조희 항목: 전	체 조희 🗸 3일 전		~	
Dashboard	서비스 이름 : IAM × 'O 필터 초기화					총 209 건 중 1-50	) < 이전 <b>다음</b> →   C
Event	이벤트 발생 시간 💠 이벤트 구	분 이벤트 이름	사용자	사용자 고유 ID	서비스 이름	자원 유형	자원 이름
	2024.06.03 (월) 1 조직	Console Login	decilias proviĝita.	$((\gamma_1,(\gamma_2)))_{1\leq i\leq j\leq n},(\gamma_1,(\gamma_1))_{1\leq i\leq j\leq n})$	IAM	Domain	
	2024.06.03 (월) 1 조직	Console Login	princharanginat.	4555-cc1000-cg1000a.	IAM	Domain	
	2024.06.03 (월) 1 조직	Console Logout	41000000.000000000000000000000000000000	$\ f_{n+1}^{-1}(x,t)-f_{n+1}^{-1}(x)\ _{L^{\infty}(\Omega)} \leq \ f_{n+1}^{-1}-f_{n}\ _{L^{\infty}(\Omega)} \leq \ f_{n}\ _{L^{\infty}(\Omega)} \leq \ f$	IAM	Domain	
	2024.06.03 (월) 1 조직	Console Login	1	1.94000/0010/71-2240.	IAM	Domain	
	2024.06.03 (월) 1 조직	Console Login	and proproving the	e-470207-0440.	IAM	Domain	And and a first state of the
	2024.06.03 (월) 1 조직	Console Login	any my ungles.	4.475,00710,000	IAM	Domain	
	2024.06.03 (월) 1 조직	Console Login	etropolitic ampositio.	100000000000000000000000000000000000000	IAM	Domain	4 mail: 10 million and 10
	2024.06.03 (월) 1 조직	Console Logout	pro-Coglication.		IAM	Domain	
	2024.06.03 (월) 1 조직	Console Logout	ernen ungenengt.	024000000000000000000000000000000000000	IAM	Domain	4 mail: 1 mail: 1 mail: -
	2024.06.03 (월) 1 조직	Console Logout	1.000 million - 1.000 million -	4748-1777-114	IAM	Domain	
	2024.06.03 (월) 1 조직	Console Logout	partite insult (finale.	10.40 × 10.70 × 10.70.	IAM	Domain	
사용자 가이드 🗅	2024.06.03 (월) 1 조직	Console Logout	60-2010-00-000 (2010)	479auto 1027 1027 102	IAM	Domain	
· · ·	[72]	ᄃᄀᄀ <b>게저</b>	과려 이~	ud Trail-E	vont		

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

iii kakao <b>cloud</b>				Q, 서비스 검색			<b>Q</b> k	r-central-2 ~	
Cloud Trail	Cloud Trail > Event								
프로젝트	Event							• 로그;	여장 중 로그 저장 관리
۰ · ·	· 속성 이름을 입력해					×	~	총 <b>223</b> 건 중 1-50	< 이전 다음 >
Dashboard	이벤트 발생 시간 💠	로그 저장 괸	리			~	기름	자원 유형	자원 이름
Event	2024.06.03 (월) 1			사용 로그 저장에 3회 면속 실패 시, 자동으로 미사용으로 변경됩니다. 생성된 로그는 한 시간마다 저장소 버킷에 저장됩니다.			Machine	Snapshot	
	2024.06.03 (월) 1	로그 저장 옵션	로그 저 한 시간!				Machine	Snapshot	
	2024.06.03 (월) 1		✓ 조	✓ 조직 이벤트 포함				Payment	•
	2024.06.03 (월) 1	이벤트 저장 범위	프로젝트 지 포함:					Credit	•
	2024.06.03 (월) 1							Billing Report	•
	2024.06.03 (월) 1	저장소 버킷	◆ 로그 저장 용량에 따라 요금이 부과됩니다. Object Storage 요금 정책 보기 간					Billing Report	•
	2024.06.03 (월) 1		저장소의 로그는 ·	이 버킷을 삭제할 경우, 정상적으로 로 복구할 수 없습니다. Object Storage	그가 저장되지 않으며 삭제된 같			Cost Report	-
	2024.06.03 (월) 1			취소 적용				Domain	
	2024.06.03 (월) 1							Domain	
	2024.06.03 (월) 1	조직	Console Logout	Robin progin.	Rentwood Contraction of Contractiono	IAM		Domain	
	2024.06.03 (월) 1	조직	Console Login			IAM		Domain	
	2024.06.03 (월) 1	조직	Console Login			IAM		Domain	
사용사 가이드 년	2024.06.03 (월) 1	조직	Console Login	aption or generalities.	anaman mant.	IAM		Domain	Summer State
		[기리 도	7 81 .=	<u></u>	리 선저 모	다			

▶ 관리자는 관리자 권한을 가진 계정에 대해서는 Cloud Trail 로그를 이중으로 확인한다.

iii kakao <b>cloud</b>		Q, 서비스 검색			• kr-central-2 ~	
Cloud Trail	Cloud Trail > Dashboard					
C > C > C > C > C > C > C > C > C > C >	<b>프로젝트 이벤트 현황</b> 조회 기간   2024.05.28 ~ 2024.06.0 ■ Bicck Storage = Instance = Project = ♥ VPC = Snapshot	3 Public IP  Security Group  Listener	r 🛛 Backup 🗮 Keypair 🖷 Ale	ert Policy 📕 Load Balancer	🗕 Target Group 📕 Health	1주전 ~ Check Bucket Image
	240 223 180 120 60 0 2024.05.28	49 19 2024.05.29 2024.05.30	56	4 2024.06.01	9 2024.06.02	20 2024.06.03
	최근 프로젝트 이벤트 목록					전체 이벤트 기록 보기 →
	이벤트 발생 시간 이벤트 이름	사용자	사용자 고유 ID	서비스 이름	자원 유형	자원 이를
	2024.06.03 (월) 19: Snapshot Creat	e		Virtual Machine	Snapshot	
	2024.06.03 (월) 18: Public IP Delete	ert	Gelleticular/Spitter.	VPC	Public IP	-
	2024.06.03 (월) 17: Public IP Updat	e	$(1,1)(1,1)(1,1)(1,1)^{1/2}(1,1)(1,1)(1,1)(1,1)(1,1)(1,1)(1,1)(1,1$	VPC	Public IP	-
484 1VIE 0	2024.06.03 (월) 17: Choose Project		ended and respectively.	IAM	Project	disculture to reaso
	[그림 5.7.9]	Cloud Trail	서비스의 C	ashboard		



## 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



본 안내서 내용의 무단전재를 금하며, 가공 인용할 때에는 반드시 금융보안원 「금융분야 상용 클라우드컴퓨팅서비스 보안 관리 참고서」라고 밝혀 주시기 바랍니다.

〈비 매 품〉

참 여 자 DT대응지원부 클라우드보안팀	부장 이수미 팀장 장지현 차장 장기헌 과장 김용규 과장 유희만 대리 이성덕 대리 김상후 대리 최주섭 주임 송창석				
발 행 인	김철웅				
공 동 발 행 인	카카오엔터프라이즈				
발 행 처	금융보안원				
주 소	경기도 용인시 수지구 대지로 132				

금융분야 상용 클라우드컴퓨팅서비스 보안 관리 참고서 (카카오엔터프라이즈)



본 참고서는 금융회사 등에서 클라우드컴퓨팅서비스 이용 시 보안관리 및 기술 활용 지원이 목적이며, 금융회사의 의무 준수사항이 아닙니다.