2026 - 비정기 - AGR - 클라우드평가 -705

금융분야 상용 클라우드컴퓨팅서비스 보안 안내서

KT Cloud

금융보안원
FINANCIAL SECURITY INSTITUTE

kt cloud

CONTENTS

1. 가상자원 관리 ····· 1
1.1. 가상자원 생성 시 최초 계정에 대한 비밀번호 규칙 수립 ····· 2
1.2. 이용자 가상자원 접근 시 로그인 규칙 적용 ····· 7
1.3. 가상자원 루트 계정 접근시 추가인증수단 제공 ····· 10
1.4. 가상자원 생성 시 네트워크 설정 적용 ····· 13
1.5. 가상자원 접속 시 보안 방안 수립 ····· 19
1.6. 이용자 가상자원별 권한 설정 ····· 23
1.7. 이용자 가상자원내 악성코드 통제방안 수립 ····· 27

2. 네트워크 관리 ····· 29
2.1. 업무 목적에 따른 네트워크 구성 ····· 30
2.2. 내부망 네트워크 보안 통제 ····· 34
2.3. 네트워크 보안 관제 수행 ····· 37
2.4. 공개용 웹서버 네트워크 분리 ····· 44
2.5. 네트워크 사설 IP주소 할당 및 관리 ····· 47
2.6. 네트워크(방화벽 등) 정책 주기적 검토 ····· 50

3. 계정 및 권한 관리 ····· 51
3.1. 클라우드 계정 권한 관리 ····· 52
3.2. 이용자별 계정 부여 ····· 58
3.3. 인사변경 사항 발생 시 계정 관리 ····· 62
3.4. 클라우드 가상자원 관리 시스템 관리자 권한 추가인증 적용 ····· 65
3.5. 클라우드 가상자원 관리 시스템 로그인 규칙 수립 ····· 68
3.6. 계정 비밀번호 규칙 수립 ····· 70
3.7. 공개용 웹서버 접근 계정 제한 ····· 72

4. 암호키 관리 ····· 74
4.1. 암호화 적용 가능 여부 확인 ····· 75
4.2. 암호키 관리 방안 수립 ····· 78
4.3. 암호키 서비스 관리자 권한 통제 ····· 82
4.4. 암호키 호출 권한 관리 ····· 84
4.5. 안전한 암호화 알고리즘 적용 ····· 87

5. 로깅 및 모니터링 관리 ····· 89

5.1. 가상자원 이용(생성, 삭제, 변경 등)에 관한 행위추적성 확보 ····· 90
5.2. 가상자원 이용 행위추적성 증적 모니터링 ····· 93
5.3. 이용자 가상자원 모니터링 기능 확보 ····· 95
5.4. API 사용(호출대상, 호출자, 호출일시 등)에 관한 행위추적성 확보 ····· 102
5.5. 네트워크 관련 서비스(VPC, 보안그룹, ACL 등)에 관한 행위추적성 확보 ····· 104
5.6. 계정 변동사항에 대한 행위추적성 확보 ····· 107
5.7. 계정 변경사항에 대한 모니터링 수행 ····· 109

6. API 관리 ····· 111

6.1. API 호출 시 인증수단 적용 ····· 112
6.2. API 호출 시 무결성 검증 ····· 118
6.3. API 호출 시 인증 키 보호대책 수립 ····· 120
6.4. API 이용 관련 유니크값 유효기간 적용 ····· 122
6.5. API 호출 구간 암호화 적용 ····· 125

7. 스토리지 관리 ····· 126

7.1. 스토리지 접근 관리 ····· 127
7.2. 스토리지 권한 관리 ····· 130
7.3. 스토리지 업로드 파일 제한 ····· 133

8. 백업 및 이중화 관리 ····· 135

8.1. 클라우드 이용에 관한 행위추적성 증적(로그 등) 백업 ····· 136
8.2. 행위추적성 증적 (로그 등) 백업 파일 무결성 검증 ····· 139
8.3. 금융회사 전산자료 백업 ····· 141
8.4. 금융회사 전산자료 백업 파일 무결성 검증 ····· 156
8.5. 행위추적성 증적 및 전산자료등 백업에 관한 기록 및 관리 ····· 158
8.6. 백업파일 원격 안전지역 보관 ····· 161
8.7. 주요 전산장비 이중화 ····· 163

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 접근시 추가인증수단 제공
1.4. 가상자원 생성 시 네트워크 설정 적용
1.5. 가상자원 접속 시 보안 방안 수립
1.6. 이용자 가상자원별 권한 설정
1.7. 이용자 가상자원내 악성코드 통제방안 수립

1 가상자원 관리

1 기준

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

2 설명

- 이용자 가상자원에 접근하는 계정에 대한 비밀번호 규칙 등 보안통제 방안을 수립하여야 한다.
  - 예시
    1) 비밀번호는 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설정
    2) 분기별 1회 이상 변경
    3) 가상자원 마다 관리자(root, administrator) 계정은 비밀번호를 다르게 설정

3 우수 사례

(G플랫폼) 가상자원에 접근하는 계정에 대한 비밀번호는 가상자원 생성 시 대/소문자 영어와 숫자를 혼합한 12자 암호로 랜덤 설정됩니다.

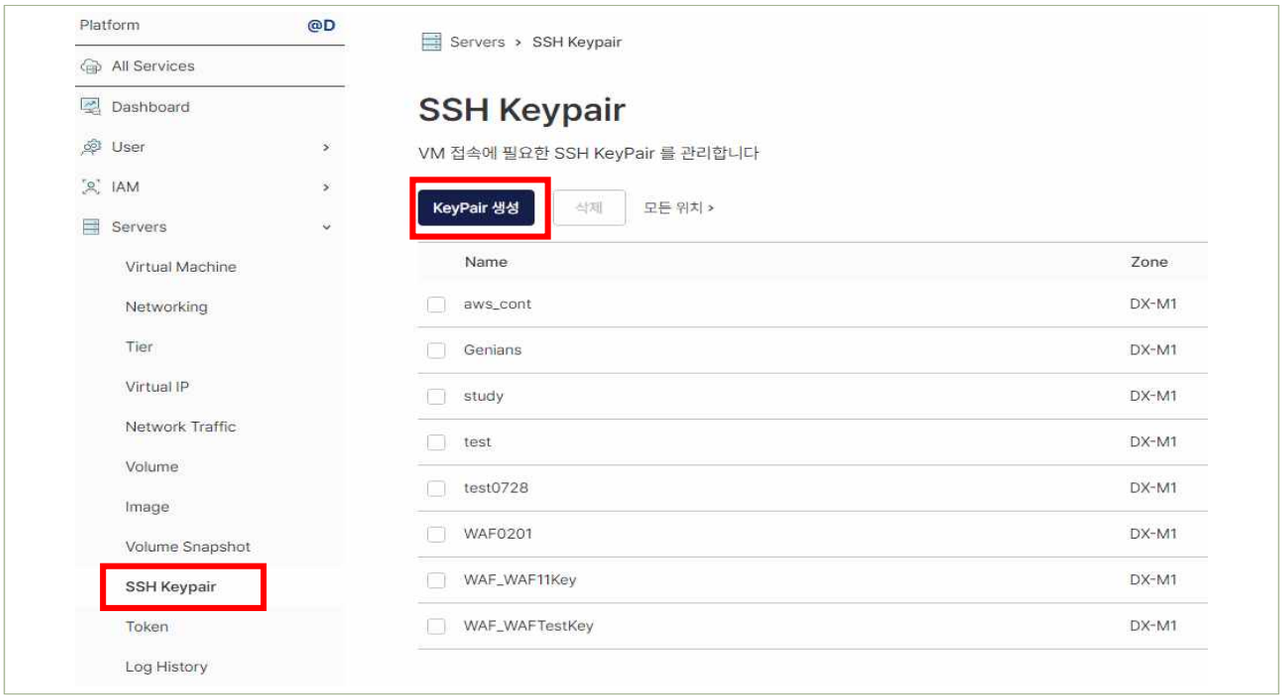
관리자 암호는 가상자원 생성 직후 콘솔 알림 창에 1회 안내되고 이메일로 발송됩니다. 초기 암호는 최초 로그인 이후 변경하여 사용하시는 것이 보안적으로 안전합니다.

| 그림 1-1-1 | 콘솔 알림 창을 통해 관리자 암호 확인

(D플랫폼) 가상자원에 접근하는 계정에 대한 비밀번호는 가상자원 생성 시 단방향 암호화된 암호로 랜덤 설정됩니다.

관리자 암호는 확인 불가하며, D플랫폼의 경우 보안적으로 보다 강화된 방식으로 서버 접속 시 Key Pair를 사용합니다. 반드시 Key Pair를 사용하여 가상자원을 생성해야 하고 해당 Key Pair를 사용하여 일반 계정으로 SSH 접속해야 합니다.

1) Keypair 파일 생성 (Servers 〉 SSH Keypair)



| 그림 1-1-2 | SSH Keypair 생성

2) 생성한 Keypair파일 다운로드(.pem 파일)

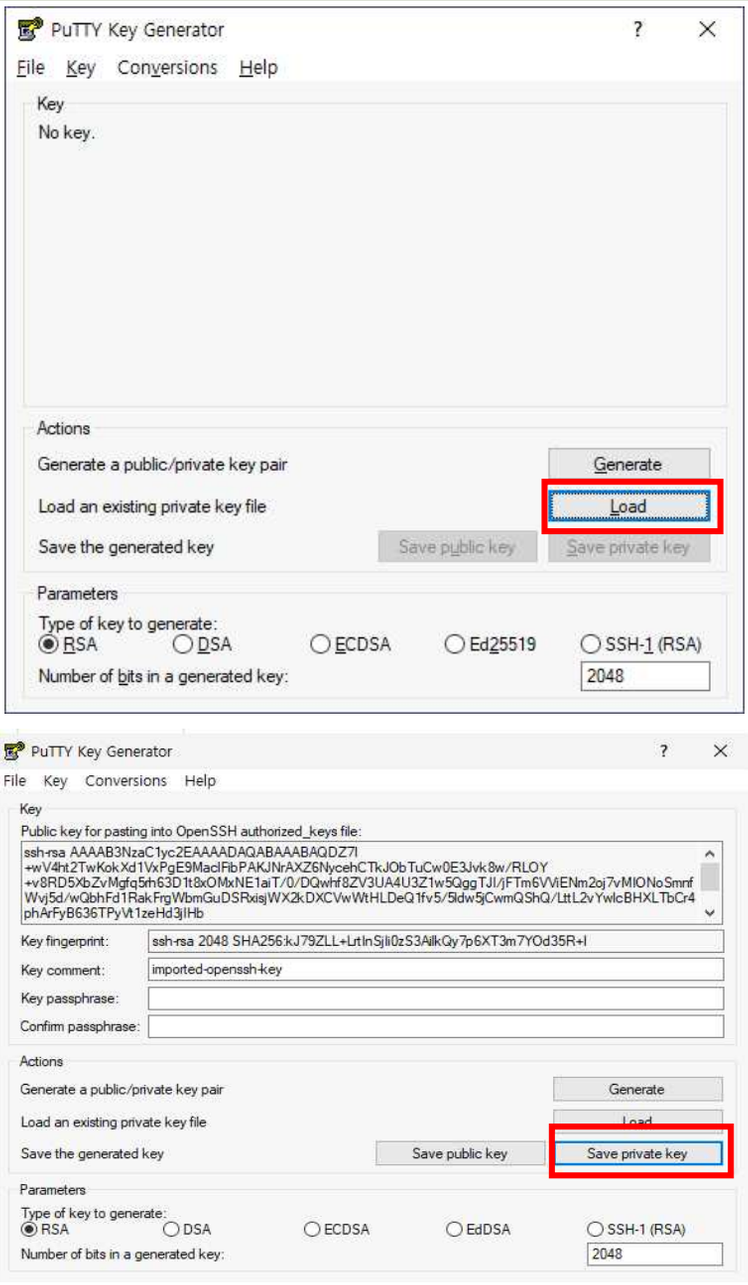
생성된 SSH Keypair는 1회만 제공하므로 다운로드 후 별도 보관합니다(메일로도 전송)

| 그림 1-1-3 | SSH Keypair 생성 결과

3) .pem 파일을 이용해 .ppk 파일 생성

Putty를 통해 서버에 접속하려면 다운받은 pem 파일을 ppk 파일로 변경하여야 합니다. 파일 변경은 Puttygen등을 통해 가능하며 Puttygen은 Putty 설치시 자동 설치됩니다.

Puttygen 실행 후 pem 파일을 불러온 후 Save Private Key 버튼을 통해 변경된 형식으로 저장합니다.



| 그림 1-1-4 | Keypair를 이용한 SSH 접속 설정

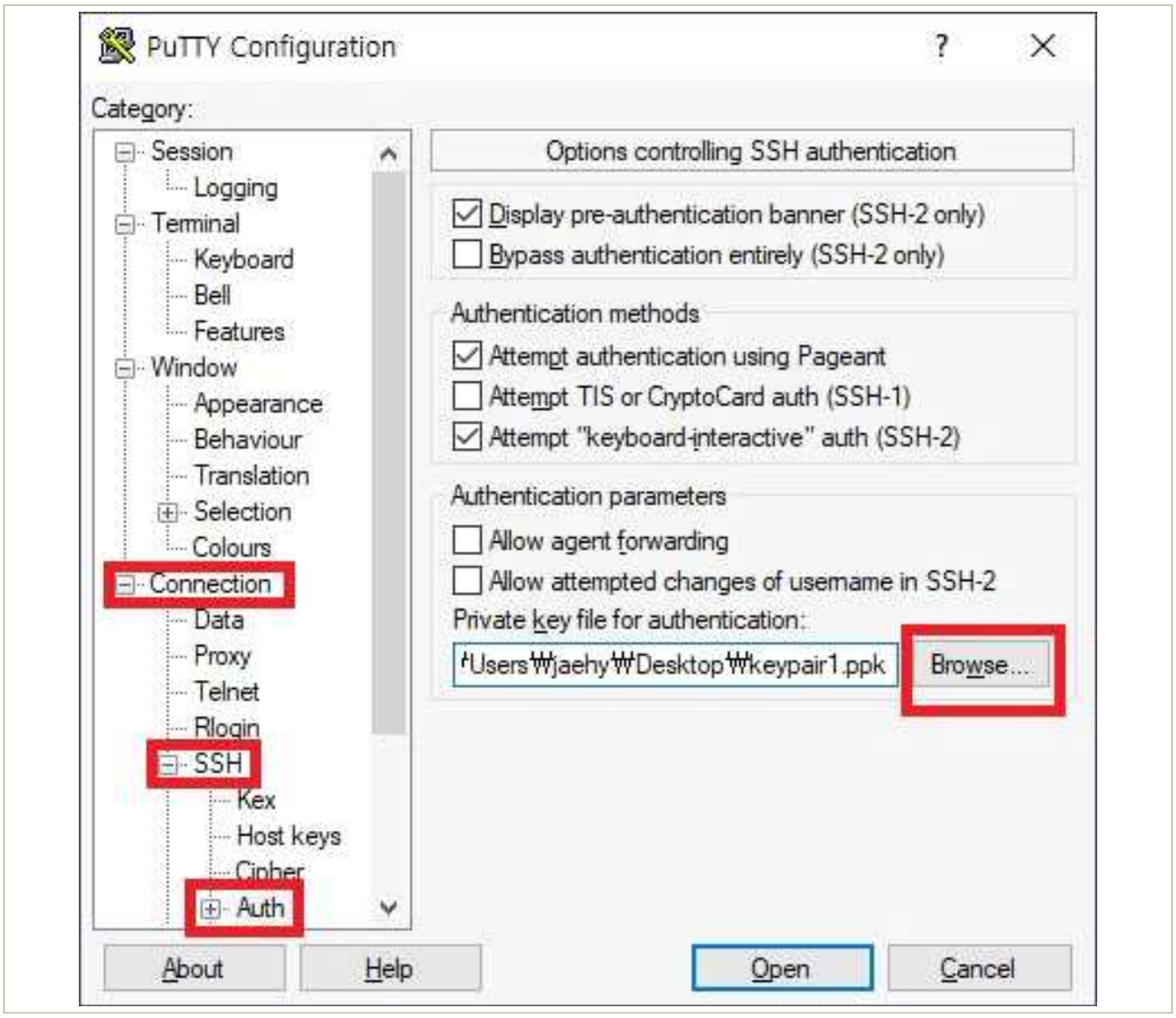
4) 가상 자원 생성 시 반드시 SSH 접속용 Keypair 지정

SSH Keypair는 VM 생성시에 지정하여 생성하는 것도 가능합니다.

| 그림 1-1-5 | VM 생성시 SSH Keypair 생성 방법

5) SSH 접속 시 Keypair 파일을 활용해 접속

Putty에서 서버 접속시에는 'Connection-SSH-Auth-Browse'를 통해 변경한 ppk 파일을 선택합니다.



| 그림 1-1-6 | SSH 접속 시 Keypair를 이용 방법

4 참고 사항

- **플랫폼 용어 안내**
  - D 플랫폼 : Openstack 기반의 3세대 플랫폼입니다.
  - G 플랫폼 : Cloudstack 기반의 서비스입니다.

  서비스를 이용하는 존(DX-M1, 금융존 등)에 따라 해당되는 플랫폼은 달라지며 플랫폼에 따라 일부 서비스의 차이가 있으며 세부 서비스 차이는 포탈 서버 상품 안내를 참고해 주시기 바랍니다.

  ➔ 포탈 서버 상품 안내 페이지 : kt cloud

- 서버 이용/접속 방법 포탈 매뉴얼 : Cloud 매뉴얼 (kt.com)
- SSH Keypair 관리 포탈 매뉴얼 : Cloud 매뉴얼 (kt.com)

1 기준

식별번호	기준	내용
1.2.	**이용자 가상자원 접근 시 로그인 규칙 적용**	**이용자 가상자원 접근 계정에 대한 로그인 규칙(오류횟수 지정 등) 등을 수립하여야 한다.**

2 설명

- 이용자 가상자원에 접근하는 계정에 대한 로그인 규칙을 수립하여야 한다.
  - 예시
    1) 로그인 오류에 따른 보안통제 방안 수립(5회이상 로그인 실패 시 계정 잠김 등)

3 우수 사례

① 서버 OS 설정 방법

서버 접속 시 보안강화를 위한 계정 잠금 임계 값 설정은 서버내 관련 OS 파일 설정 값 변경을 통해 가능합니다.

CentOS의 /etc/pam.d/system-auth 파일은 Console 접근 시, password-auth 파일은 SSH 원격접근 시 영향 받으므로 2가지 파일 모두 설정해야 합니다.(RHEL 계열 기준)

- pam_tally2.so.deny = 실패 시 잠금 횟수(예, 5) unlock_time = 잠금시간(예, 60)

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        required      pam_faildelay.so delay=2000000
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        required      pam_deny.so
auth        required      pam_tally2.so deny=5  unlock_time=60

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     required      pam_permit.so
account     required      pam_tally2.so

password    requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
~
```

| 그림 1-2-1 | /etc/pam.d/system-auth 파일 내 설정 값 변경

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        required      pam_faildelay.so delay=2000000
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        required      pam_deny.so
auth        required      pam_tally2.so deny=3 unlock_time=60

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     required      pam_permit.so
account     required      pam_tally2.so

password    requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok


password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
~
```

| 그림 1-2-2 | /etc/pam.d/password-auth 파일내 설정 값 변경

② Fail2Ban 프로그램(프리웨어) 이용 방법

Fail2ban은 python(2.4 Ver 이상)으로 만들어진 SW로 로그인을 몇 회 이상 실패할 경우, logfiles을 읽어서 일정 기간 동안 접속을 차단하는 툴로 ssh, ftp 등에 무작위로 로그인하는 brute force attack에 대응하기 위한 모듈입니다.

iptables, tcpwrapper 등에 해당 host를 등록하여 특정 host의 접속을 차단하는 기능을 가지고 있으며, ssh, apache, ftp 등을 이용한 접속 방어에 사용됩니다.

Fail2Ban의 활용 순서는 다음과 같습니다.

1) yum install fail2ban 등의 명령어를 통해 Fail2Ban을 설치합니다.
2) /etc/fail2ban 경로에 Fail2ban 설정 파일이 위치하게 됩니다.
3) 설정파일인 jail.conf 파일을 열어 [default] section에서 bantime(차단시간)과 maxretry(실패 시 접근 제한할 횟수)를 적절한 값으로 변경합니다.

```
[DEFAULT]

# "ignoreip" can be an IP address, a CIDR mask or a DNS host. Fail2ban will not
# ban a host which matches an address in this list. Several addresses can be
# defined using space separator.
ignoreip = 127.0.0.1

# "bantime" is the number of seconds that a host is banned.
bantime  = 600

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime  = 600

# "maxretry" is the number of failures before a host get banned.
maxretry = 3
```

| 그림 1-2-3 | Fail2Ban config 설정 화면

4 참고 사항

- 서버 이용방법 포탈 매뉴얼 : Cloud 매뉴얼 (kt.com)
- Fail2Ban 이용방법 포탈 매뉴얼 참조 : Cloud 매뉴얼 (kt.com)
- Fail2Ban 다운로드 링크 : https://github.com/fail2ban/fail2ban

1 기준

식별번호	기준	내용
1.3.	**가상자원 루트 계정 접근시 추가인증수단 제공**	**이용자 가상자원 루트 계정(root, administrator 등) 접근 시 추가인증 수단을 확보하여야 한다.**

2 설명

- 이용자 가상자원 루트 계정 접근 시 추가인증 수단이 확보되어야 한다(단, 기능이 제공되지 않는 경우 안전한 로그인 수단을 확보하여야 한다.)

  - 예시

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

3 우수 사례

① SSH PEM Key 이용 방법

가상자원의 SSH 접속 시 루트 계정으로의 직접 로그인은 차단되어 있으며, 반드시 일반 계정으로 로그인 후 루트계정으로 전환하여 사용 가능합니다.

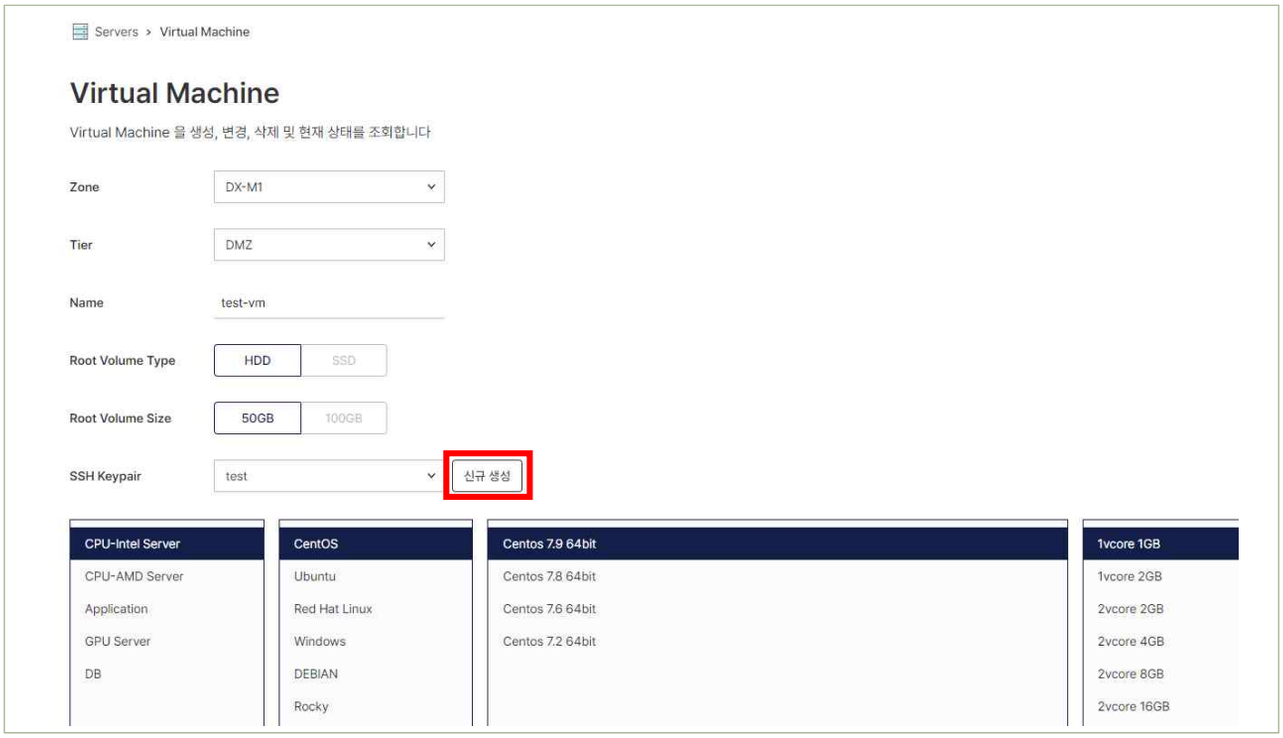
```
Please login as the user "centos" rather than the user "root".
```

| 그림 1-3-1 | SSH 접속 시 관리자 계정으로 로그인 불가 확인

| 표 1-3-1 | OS별 일반 계정

OS Type	일반 계정명
CentOS	centos
Ubuntu	ubuntu
Rhel	cloud-user
Debian	debian
Rocky	cloud-user
Windows	Admin

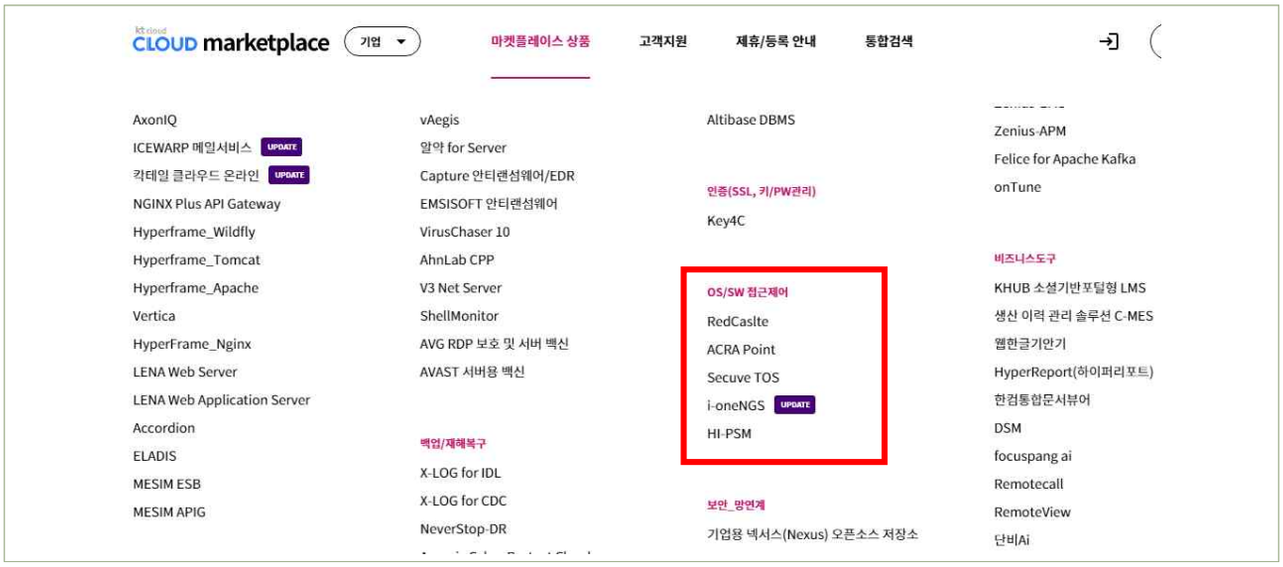
(콘솔) Servers 〉 Virtual Machine 〉 VM 생성 시 SSH Keypair를 사용하여 가상자원을 생성하면 해당 Keypair를 통해서 SSH 접속이 가능합니다.



| 그림 1-3-2 | VM 생성 시 SSH Keypair 신규 생성

② 외부 솔루션 이용

가상자원 접속 시 이메일 인증 등 추가적인 보안통제 강화를 위해서는 외부 보안솔루션을 활용할 수 있습니다. (마켓플레이스 상품내 OS/SW 접근제어 분야 솔루션 참조)



| 그림 1-3-3 | 마켓플레이스 접근제어 솔루션

4 참고 사항

- 서버 이용방법 포탈 매뉴얼 : Cloud 매뉴얼 (kt.com)
- kt cloud 마켓플레이스 : 마켓플레이스 (kt.com)

1 기준

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

2 설명

- 외부에서 직접 접속이 불필요한 경우 내부IP 또는 대역대에서만 접근할 수 있도록 설정하여야 한다.
  - 예시
    1) 가상자원 접속 가능한 공인IP(외부) 대역 점검 및 제거
    2) 접근가능한 IP 또는 IP 대역대 설정
    3) VPC 및 보안그룹을 통한 내부 네트워크 대역대 접근 설정

3 우수 사례

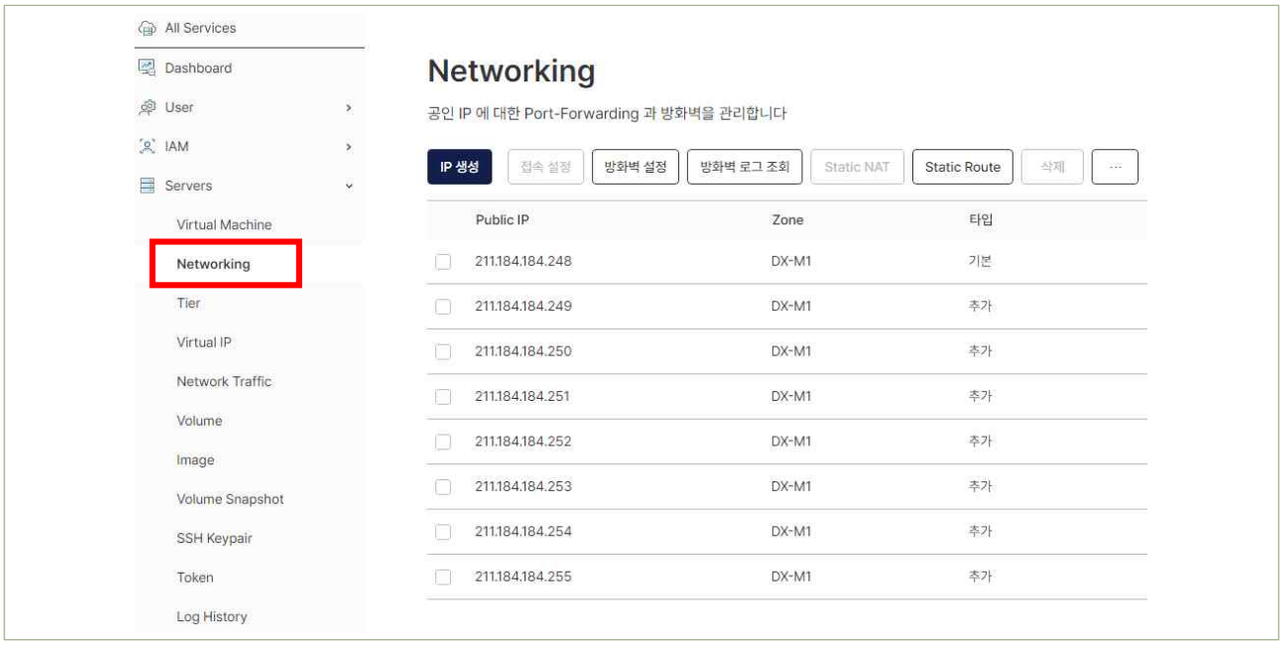
가상자원 생성 초기에는 방화벽에 의해 외부와 통신이 차단되어 있으며, Tier 내부에서 사설IP 기반으로 통신이 가능합니다.
가상자원의 외부 네트워크에서 접속 허용/차단을 위한 NAT 설정은 아래 두 가지 방식으로 가능하며 결과는 동일합니다.

1) 가상자원(Virtual Machine) 메뉴에서 가상자원 선택 후 접속 설정 기능 이용
2) Networking 메뉴에서 공인IP 선택 후 접속 설정 기능 이용

① 가상자원 외부 네트워크 접속 설정 및 설정 확인

콘솔의 Networking 메뉴의 접속설정 기능을 통해 가상자원별 NAT 설정을 추가하거나 기존에 등록된 NAT 설정을 확인할 수 있습니다.

1) (웹 콘솔) Servers 〉 Networking

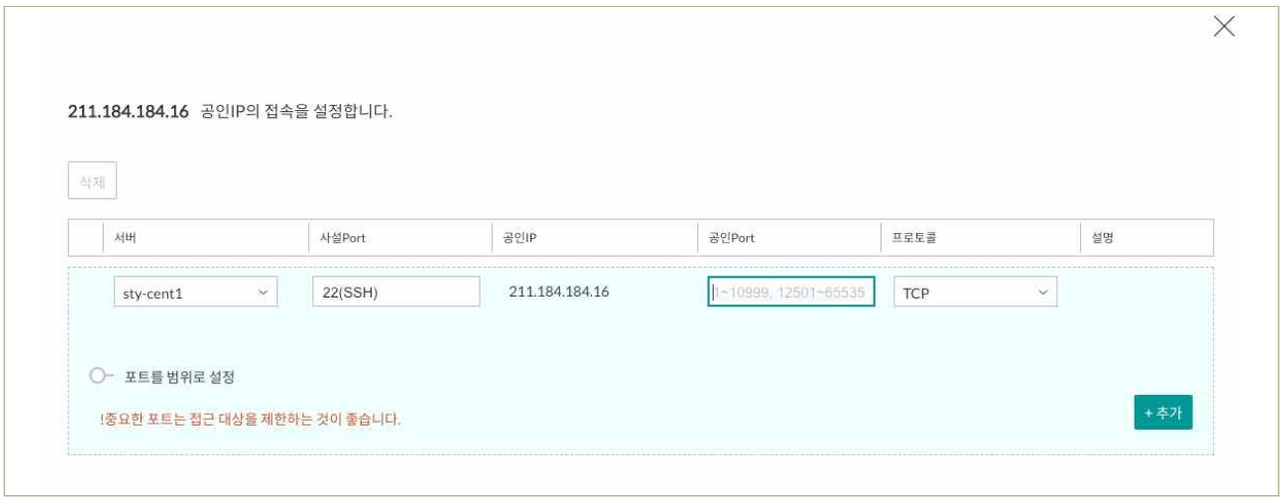


| 그림 1-4-1 | Network 설정 화면

2) 공인 IP 선택 후 접속 설정

3) VM 접속을 위한 접속 설정(Port-Forwarding 혹은 1:1 NAT)

(접속 설정) (콘솔) Servers 〉 Networking 메뉴에서 접속 설정에 사용할 공인 IP를 선택한 후 '접속 설정'을 클릭하면 Port-Forwarding 설정을 할 수 있습니다.



| 그림 1-4-2 | Port-Forwarding 설정 확인

- 서버: 접속 설정을 할 서버를 선택합니다.
- 사설Port: 서버의 어떤 Port로 접근할 것인지 선택합니다. OS 접근을 위해서는 리눅스는 22(SSH), 윈도우는 3389(RDP)를 사용합니다. 선택한 서버의 OS에 따라 자동으로 나타납니다. 이 외에 웹 서비스 80(HTTP), 443(HTTPS), FTP(21) 등이 있습니다.
- 공인IP: 앞서 선택했던 공인IP입니다.
- 공인Port: 외부에서 접근할 때 사용할 공인Port를 지정합니다. 사설Port와 같은 번호를 써도 되고, 다른 번호를 써도 됩니다.
- 프로토콜: 사용할 프로토콜을 설정합니다.

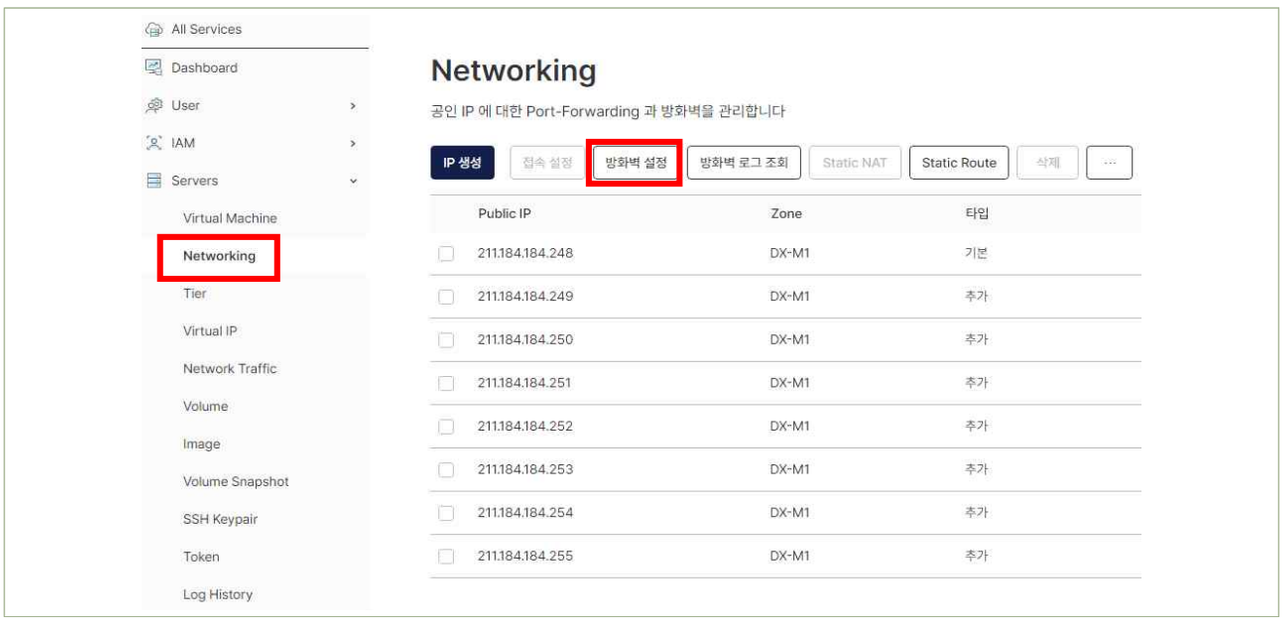
이와 같이 Port를 1:1로 연결할 수도 있고, 아래 '포트를 범위로 설정' 옵션을 사용하여 N:N개로 연결할 수도 있습니다.

| 그림 1-4-3 | 포트를 범위로 설정 가능

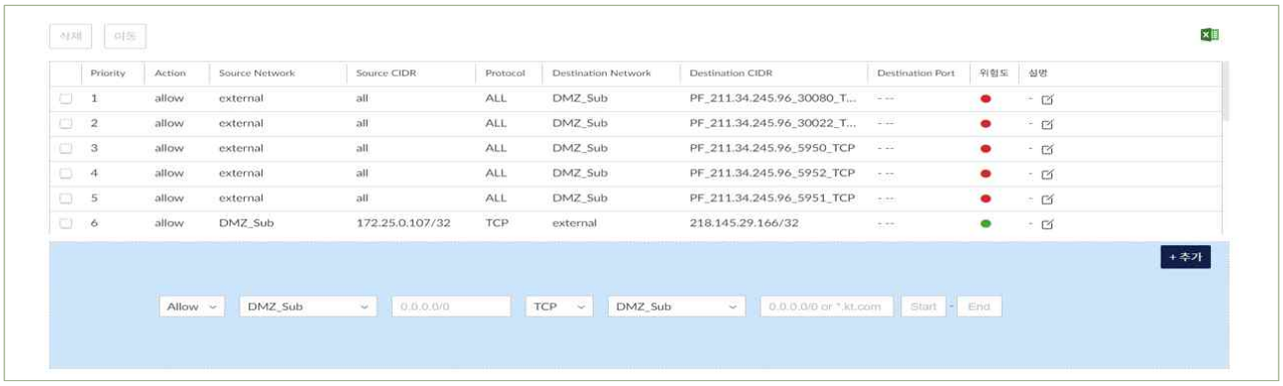
② 방화벽기반 가상자원 접근 대역 설정

서버 생성 후, 아무 설정을 하지 않은 상태에서 서버는 외부로의 통신이 방화벽으로 막혀 있습니다. 서버는 같은 Tier 안에서 사설 통신만 가능합니다. Tier 외부와 통신을 위해서는 방화벽 설정이 필요합니다.

1) 방화벽 허용 정책 설정(기본 Deny 정책 적용 중)



| 그림 1-4-4 | Network-방화벽 설정 화면



| 그림 1-4-5 | 방화벽 설정내역 확인 (IP or URL)

- Priority: 방화벽 규칙의 우선 순위입니다. 입력한 순서대로 우선 순위를 받습니다.
- Source Network: 출발지 네트워크를 입력합니다.
- Source CIDR: 출발지로 허용할 CIDR을 입력합니다.
- Protocol: 사용할 프로토콜을 입력합니다.
- Destination Network: 목적지 네트워크를 선택합니다.
- Destination CIDR: 목적지로 허용할 CIDR을 입력합니다. (IP or 도메인)
- Destination Port: 목적지로 허용할 Port를 입력합니다. 범위로 입력하며 단일 Port는 같은 숫자를 입력합니다.

네트워크의 종류는 다음과 같습니다.

- External: 외부망(공인망)
- DMZ_sub: 기본으로 제공되는 Tier
- Private_sub: 기본으로 제공되는 Tier

1) 상황별 방화벽 정책

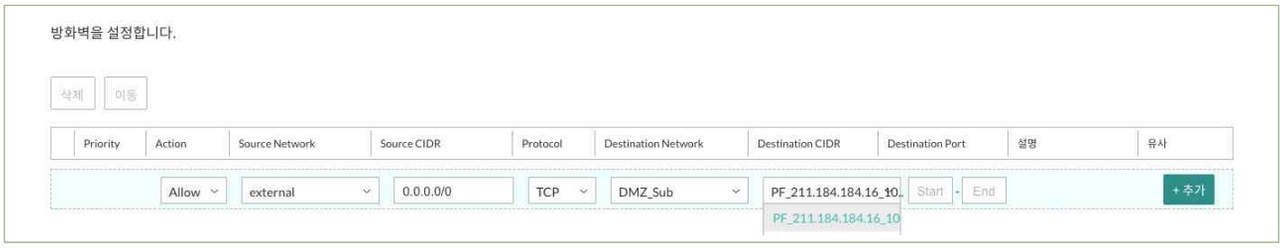
외부에서 접속 설정 시 출발지는 External로 설정합니다.

허용할 외부의 IP를 CIDR로 제어할 수 있습니다. Any로 접근을 허용하려면 0.0.0.0/0을 입력합니다. Destination은 서버가 위치한 Tier를 선택합니다.

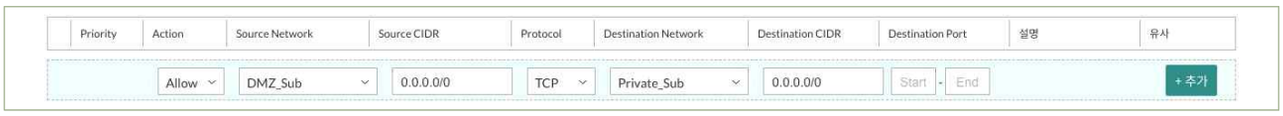
접속 설정을 이미 한 경우, Destination CIDR 대상으로 고를 수 있도록 보이게 됩니다.

예. PF_211.184.184.16_22_22_TCP

(포트포워딩_공인IP_공인포트_프로토콜)



서로 다른 Tier의 서버끼리 통신이 필요한 경우 Source와 Destination을 각각 Tier로 설정합니다.

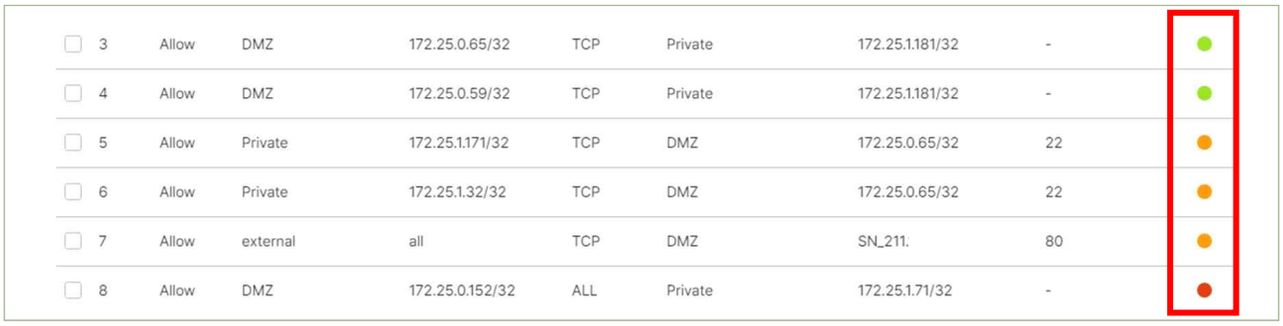


서버에서 외부로 나가는 Outbound 통신이 필요한 경우 Source에 서버의 Tier와 CIDR를 입력하고 Destination은 External로 설정합니다.

2) 방화벽 정책 위험도 가이드

방화벽 정책을 보안적으로 안전하게 관리하기 위해서 방화벽 정책 조회 시 정책 별 위험도를 시각적으로 제공합니다.

Servers 〉 Networking 〉 방화벽 설정 메뉴를 통해 등록된 방화벽 정책을 조회 시 각 정책별로 위험도가 맨 우측 컬럼에 자동으로 표시됩니다.



| 그림 1-4-6 | 방화벽 정책 별 위험도 표시

방화벽 정책 위험도 가이드는 아래 내용을 기준으로 위험을 판별하여 표기됩니다.

위험도 표시	방향	설명	예시		
			Sorce	Destination	Port
🔴	In	출발지 Any Open 정책 *사용량이 많은 TCP 80, 443 정책 제외	0.0.0.0/0	10.0.0.1/32	TCP 8443
	Out	목적지 Any Open 정책	10.0.0.1/32	0.0.0.0/0	TCP 80
	In/Out	포트 Any Open 정책	14.63.3.1/32	10.0.0.1/32	ALL(0-65535)
🟡	In	출발지 대역 Open 정책(16비트 이하 Subnet) *사용량이 많은 TCP 80, 443 정책 제외	14.63.0.0/16	10.0.0.1/32	TCP 6443
	Out	목적지 대역 Open 정책(16비트 이하 Subnet)	10.0.0.1/32	14.63.0.0/16	TCP 80
	In/out	평문 전송 정책 - FTP : TCP 20,21 - Telnet : TCP 23 - HTTP : TCP 80	14.63.3.1/32	10.0.0.1/32	TCP 23
	In	원격 터미널 접속 정책 - SSH : TCP 22 - RDP : TCP 3389	14.63.3.1/32	10.0.0.1/32	TCP 22
🟢	In/out	이 외 일반 정책			

| 그림 1-4-7 | 방화벽 정책 위험도 안내 기준

4 참고 사항

- Server/Networking 포탈 매뉴얼 참조 : Cloud 매뉴얼 (kt.com)

1 기준

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

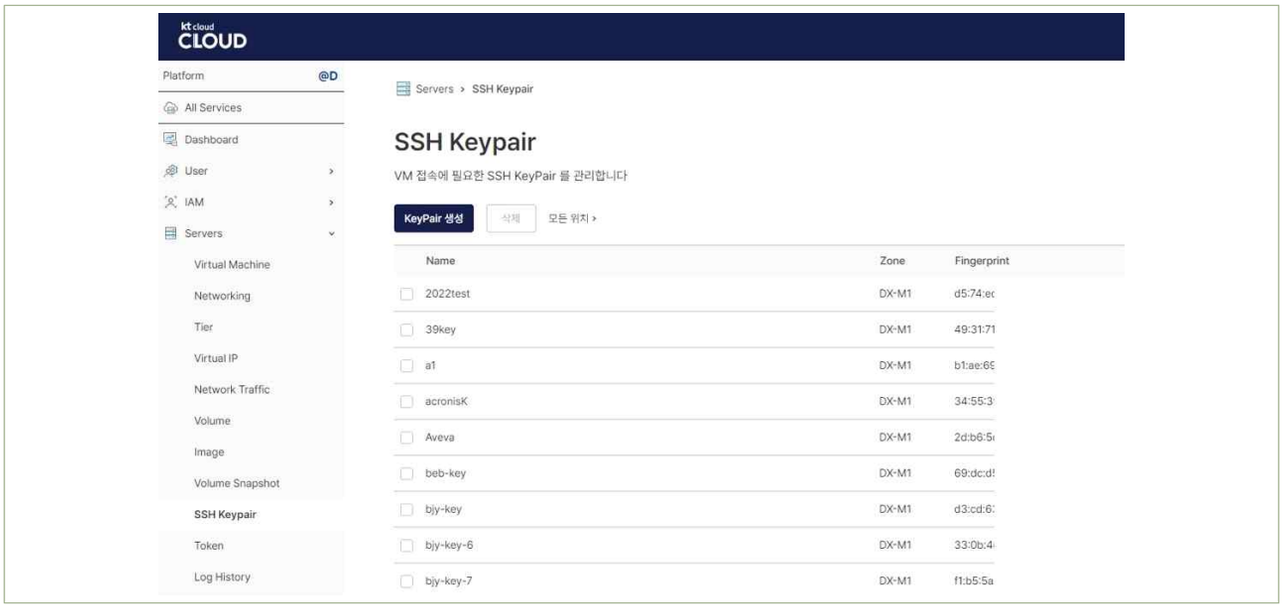
2 설명

- 이용자의 가상자원(인스턴스) 접속 시 안전한 방식을 통해 접근하여야 한다.
  - 예시
    1) SSH를 통한 접속 시 안전한 계정관리 수행(ex, ID/PW 기반이 아닌 Certificate 기반 인증 방식 적용 등)
    2) 클라우드 웹 콘솔에서 직접 실행 시 안전한 인증 방식 적용(해당 인스턴스를 호출할 수 있는 권한을 지닌 이용자인지 검증 등)

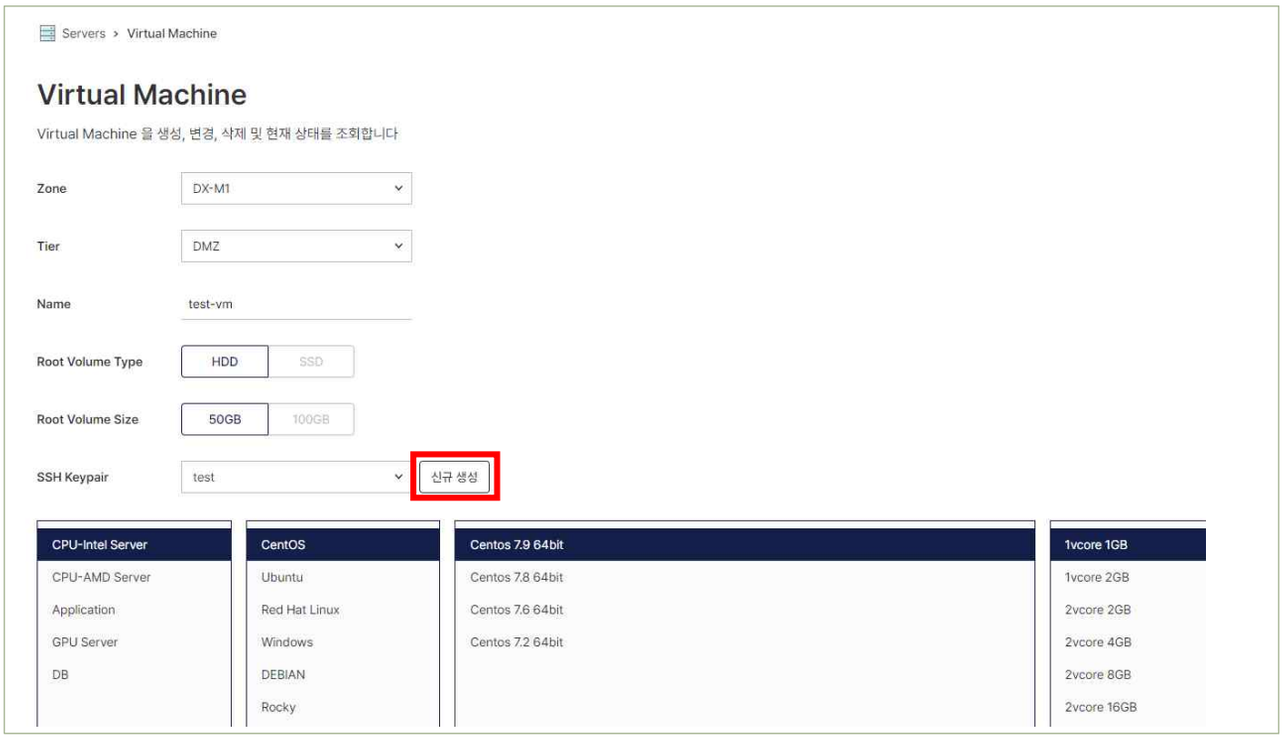
3 우수 사례

kt cloud의 경우 기본적으로 VM 접속 시 Certificate 기반 인증 방식을 지원하며, VM 생성 시 SSH Keypair를 사용하면 Keypair를 통해 안전한 방식으로 SSH 접속이 가능합니다.

1) SSH Keypair는 Servers 〉 SSH Keypair 메뉴에서 생성/관리할 수 있고, 서버 생성 시에 SSH Keypair를 동시에 간단하게 생성하는 방법도 가능합니다.



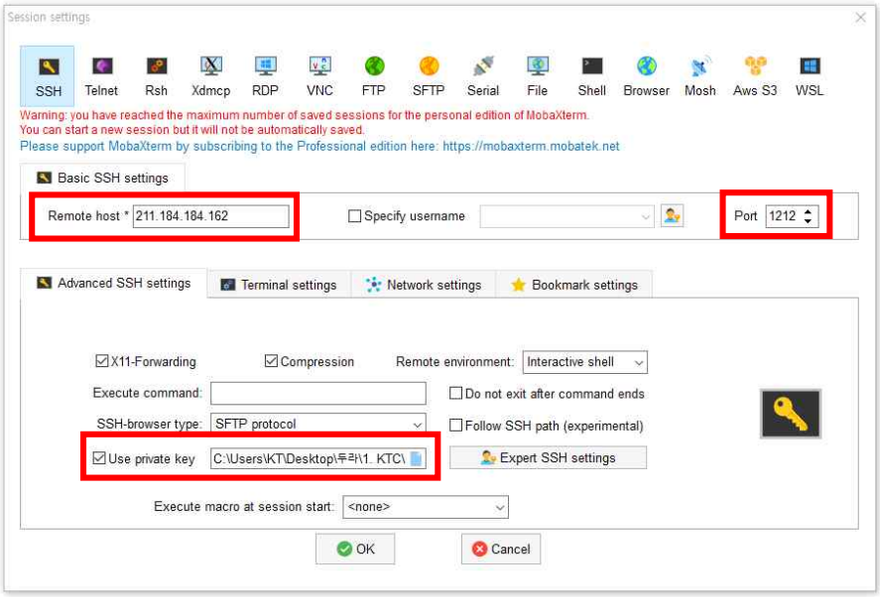
| 그림 1-5-1 | SSH Keypair 관리 화면



| 그림 1-5-2 | VM 생성 시 SSH Keypair 신규 생성 가능

2) Linux OS의 경우 SSH 원격 접속 Tool을 사용하여 접속합니다. 본 예시에서는 MobaXterm을 이용하여 원격 접속하였습니다.

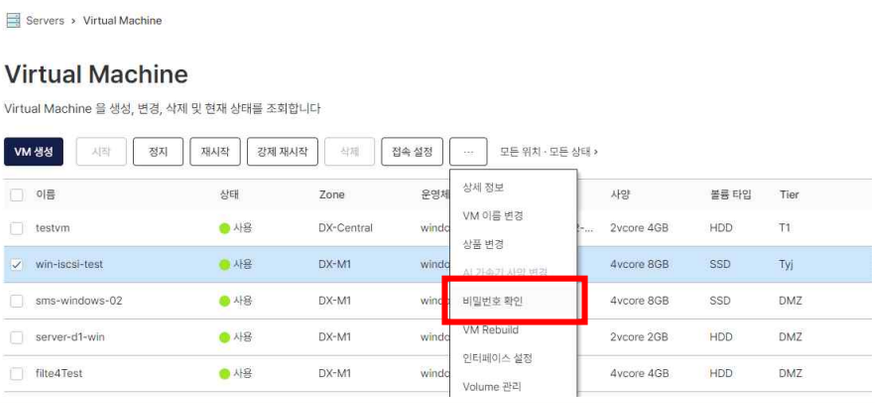
새로운 SSH Session을 생성하여 이전에 설정한 포트포워딩 정보를 입력합니다.



| 그림 1-5-3 | MobaXterm SSH 접속 설정 화면

- Remote host: 공인 IP
- Port : 공인 Port
- Use private key: SSH Keypair PPK 파일

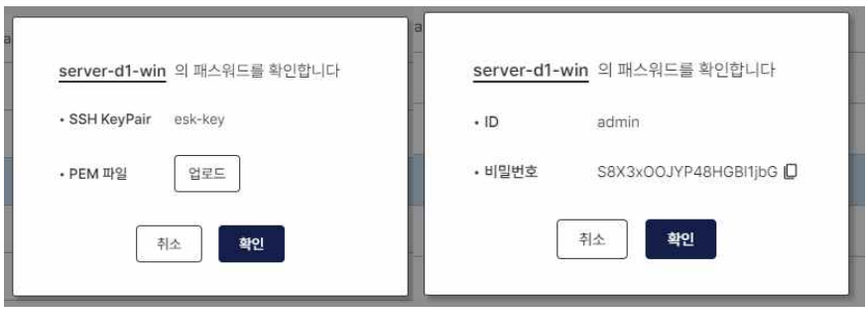
3) Windows OS의 경우 Admin PW를 확인한 후 '원격 접속 데스크탑'을 통해 접속합니다. Servers 〉 Virtual Machine 메뉴에서 Windows VM선택 후 드롭다운 메뉴에서 '비밀번호 확인'을 클릭합니다.



| 그림 1-5-4 | VM 조회 화면

서버를 만들 때 사용했던 SSH Keypair PEM파일을 업로드하면 Admin 계정의 패스워드를 확인할 수 있습니다. 해당 패스워드는 VM 부팅 시 설정된 초기 비밀번호입니다.
이후 가상자원에 접속하시어 관리자 계정의 비밀번호를 변경하시는 것을 권고 드리며, kt

cloud에서는 고객 VM의 패스워드를 임의로 알 수 없으므로 패스워드 관리에 유의 부탁드립니다.



| 그림 1-5-5 | Windows VM 패스워드 확인 화면

4 참고 사항

- Server/Networking 포탈 매뉴얼 참조: Cloud 매뉴얼 (kt.com)
- SSH Key Pair 관리 포탈 매뉴얼 참조 : Cloud 매뉴얼 (kt.com)

1 기준

식별번호	기준	내용
1.6.	**이용자 가상자원별 권한 설정**	**이용자 직무 및 권한에 따른 가상자원 별 최소권한 할당 원칙에 따른 접근통제 방안을 수립하여야 한다.**

2 설명

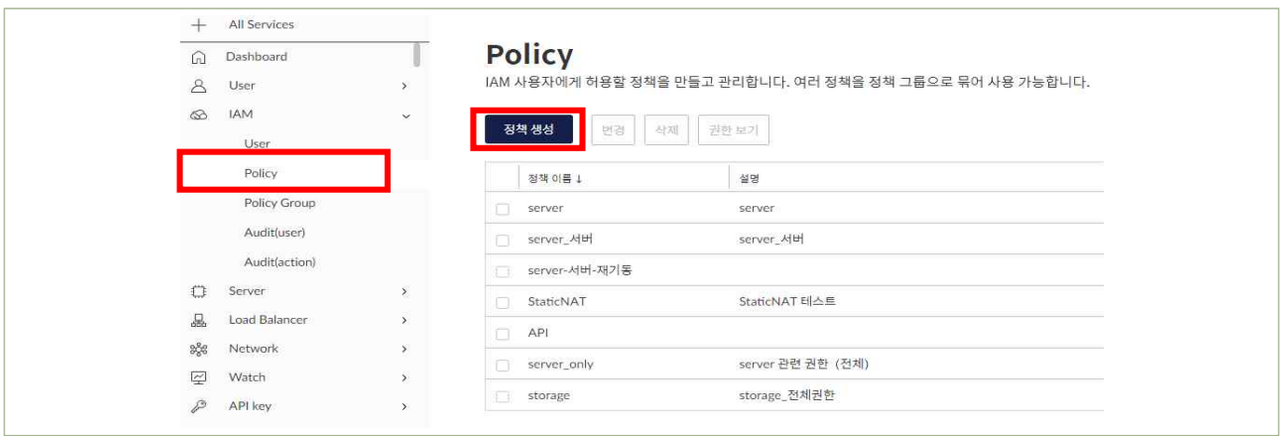
- 이용자 직무 및 권한에 따른 가상자원 별 접근통제 방안을 수립하여야 한다.
  - 예시
    1) 가상자원 종류 별 접근통제 방안 수립(ex. IAM을 통한 접근권한 관리)
    - 모든 가상자원에 접근 가능한 Role에 대해서는 최소한에 인원에 대해서만 부여

3 우수 사례

가상자원 종류 별 접근통제 방안을 수립하기 위해 IAM 서비스를 사용할 수 있습니다. IAM의 Policy 기능을 이용하여 IAM user별 영역별 필요한 권한만 선택하여 부여할 수 있습니다.

(콘솔) IAM 〉 Policy 메뉴에서 '정책 생성' 버튼을 통해 생성할 서비스 접근제어 권한에 대한 정책을 생성합니다. 서비스는 루트 계정에 청약 되어 있는 모든 서비스 목록 중에 추가 가능하며, 복수의 권한을 가질 수 있습니다.
예시로 모든 Server의 시작 권한을 갖지만 일부 서버에게만 정지 권한을 부여하려면, 아래와 같이 Policy를 생성합니다.

1) 웹 콘솔 접속 후 IAM 〉 Policy 〉 정책 생성

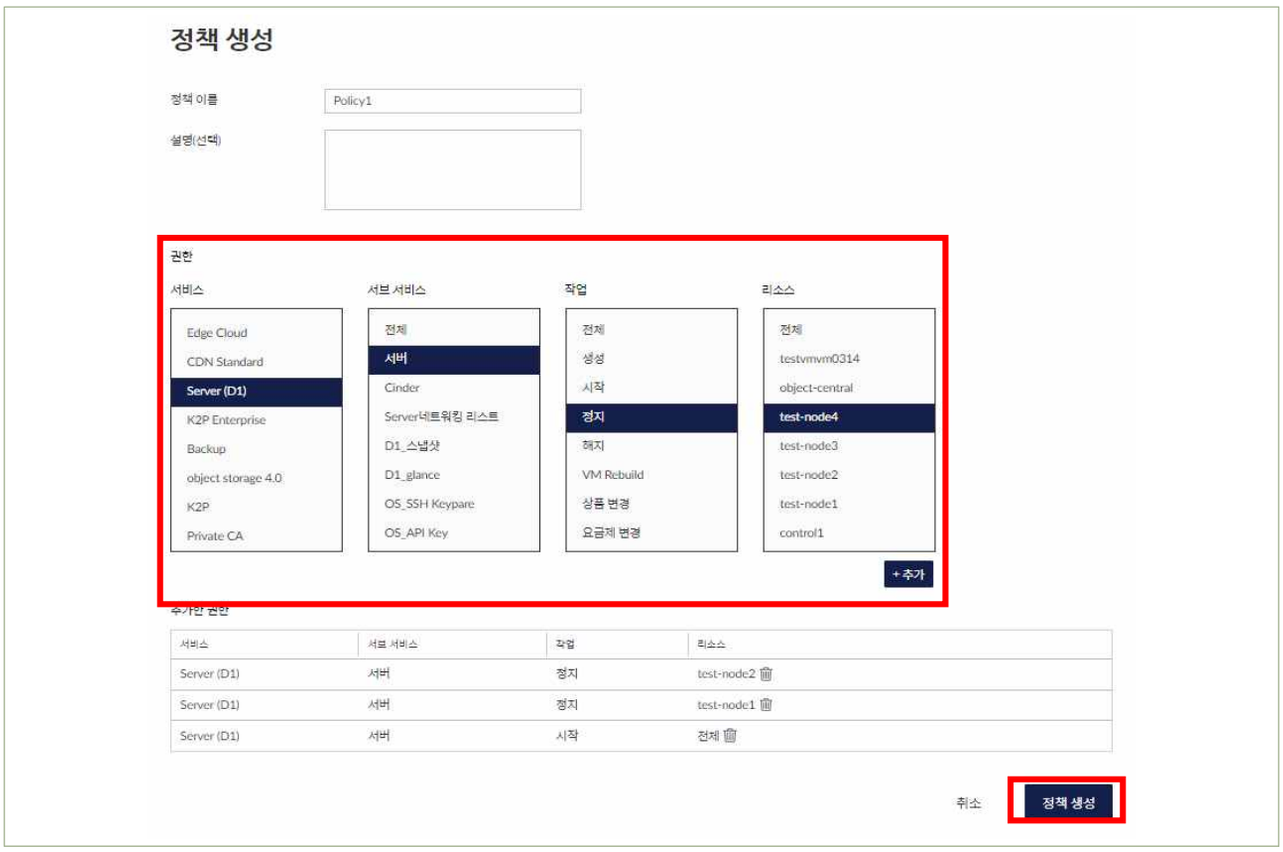


| 그림 1-6-1 | 이용자 권한 설정

2) 정책 명, 필요 권한 추가 후 정책 생성

서비스, 서브 서비스에서 Server(G1/G2), 서버를 각각 선택합니다.

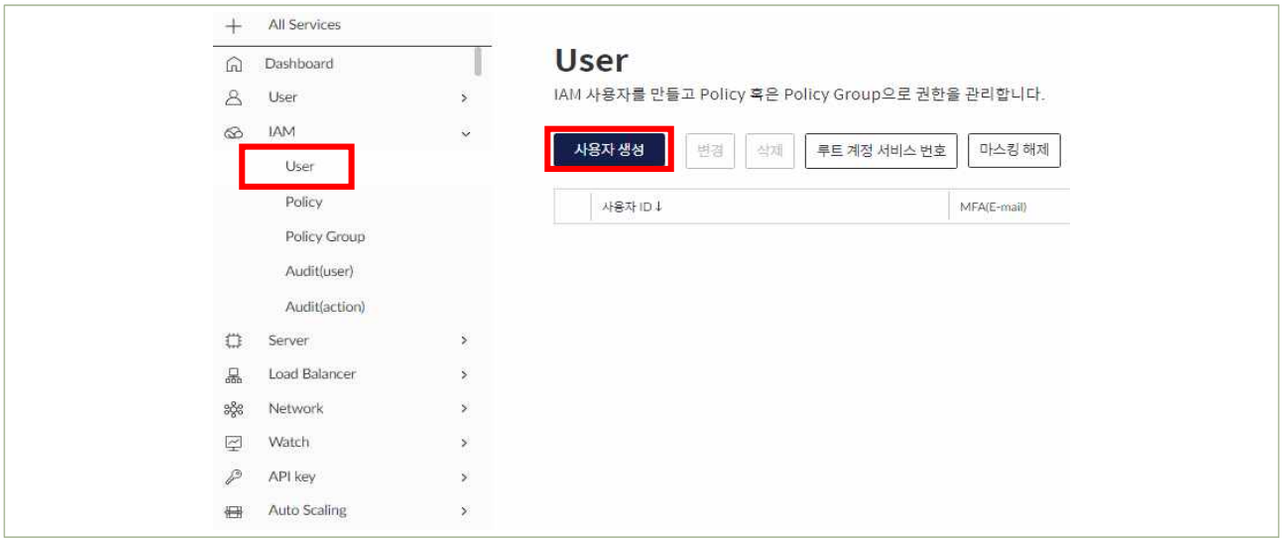
리소스에서 권한부여 대상 서버를 선택하여 서버별 정지, 시작 권한을 부여합니다.



| 그림 1-6-2 | 이용자 권한관리를 위한 정책(Policy) 설정

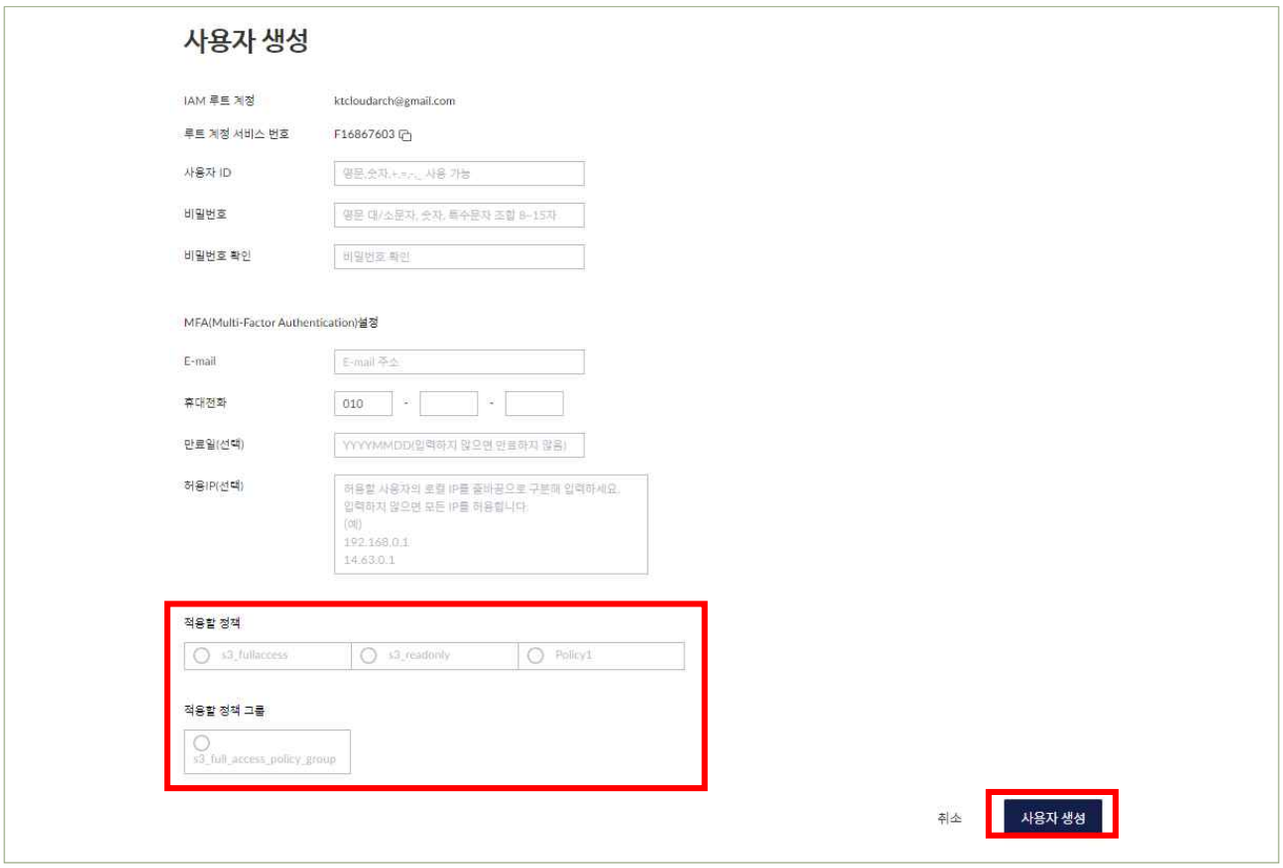
3) IAM 〉 User 〉 사용자 생성

사용자 생성 단계에서 Policy에서 생성한 권한 정책에 대한 부여가 가능합니다.



| 그림 1-6-3 | IAM 사용자 생성

4) 사용자 생성 시 적용할 권한 정책 적용



| 그림 1-6-4 | IAM 사용자 생성시 정책 선택

여러 Policy를 Policy Group으로 묶어서 사용하는 것 또한 가능합니다.

IAM 〉 Policy Group 메뉴에서 기존에 생성된 정책 중 필요한 부분을 선택하여 정책 그룹으로 생성/관리가 가능합니다.

| 그림 1-6-5 | 정책 그룹 생성 예시

4 참고 사항

- kt cloud IAM 서비스 이용방법 포탈 매뉴얼 참조 : Cloud 매뉴얼 (kt.com)

1 기준

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

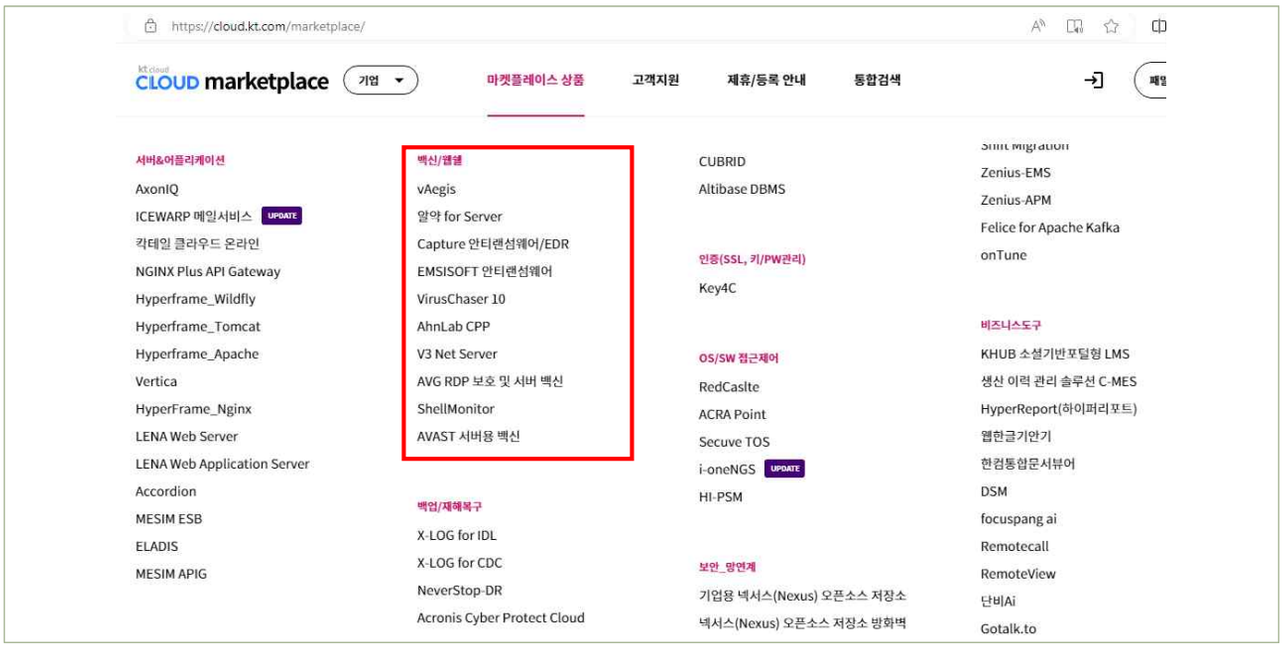
2 설명

- 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

가상자원내 악성코드 통제 관련, 마켓플레이스 내 등록된 다양한 솔루션을 통해 악성코드 대응이 가능합니다.

kt cloud 마켓플레이스 내 백신/웹쉘 카테고리 솔루션을 참고해 주시기 바랍니다.



| 그림 1-7-1 | 마켓플레이스 관련 솔루션 예시

4 참고 사항

- 마켓플레이스 링크 : https://cloud.kt.com/marketplace/

2. 네트워크 관리

2.1. 업무 목적에 따른 네트워크 구성
2.2. 내부망 네트워크 보안 통제
2.3. 네트워크 보안관제 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 네트워크 관리

1 기준

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

2 설명

- 클라우드 환경 내 업무 목적(개발, 운영, 업무 등)에 따른 네트워크 구성 및 네트워크간 접근 통제 방안을 수립하여야 한다
  - 예시
    1) VPC등 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

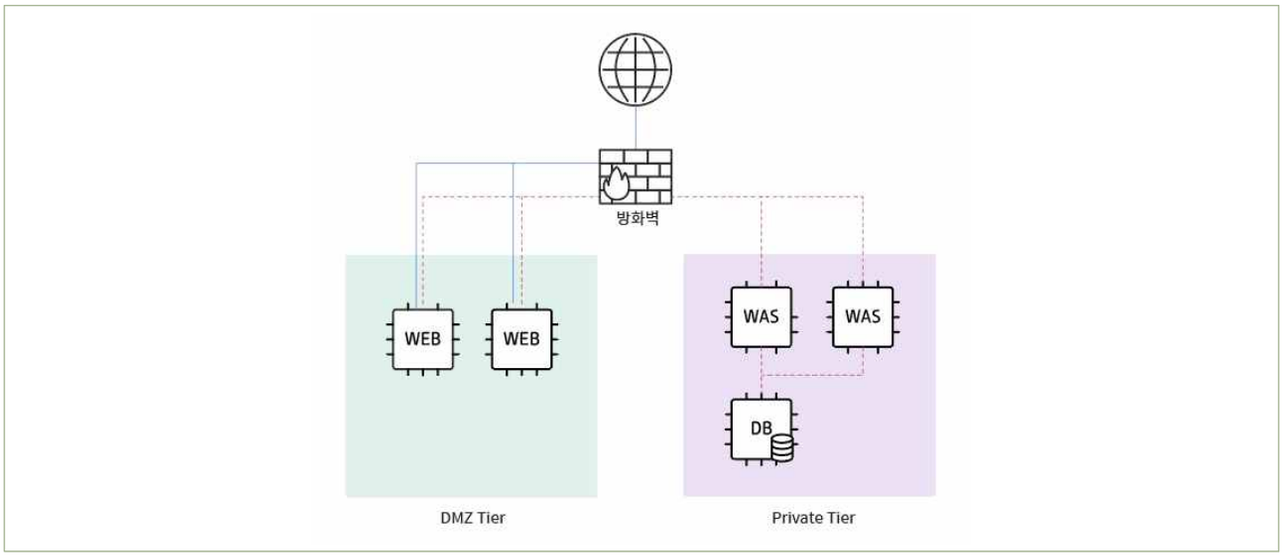
방화벽 기반의 네트워크 분리를 위한 기능을 제공하며, Tier 기능을 통해 업무목적에 따른 네트워크 분리가 가능합니다(DMZ/Private/Dev등).
서버 최초 생성 후 외부로의 통신이 방화벽으로 막혀 있습니다. 서버는 같은 Tier 안에서 서로 사설IP로 통신만 가능합니다. Tier 외부와 통신을 위해서는 방화벽 설정이 필요 합니다(1.4 참조).

Tier는 계정안에서 사용할 수 있는 가상 네트워크 서브넷입니다.

- 기본적으로 Tier안의 서버들은 외부와 격리되어 보호받습니다.
- 하나의 Tier는 /24bit IP대역을 제공하여 약 170개의 사설IP를 사용할 수 있습니다.
- 사용자는 여러 개의 Tier를 만들고 각 Tier들의 방화벽 정책을 원하는 대로 허용하거나 거부하여 다양한 토폴리지를 구현할 수 있습니다.
- 최초 DMZ, Private 두 개의 Tier를 기본 제공합니다.

콘솔의 Tier 생성 기능을 통해 목적에 따른 Tier 생성이 가능하며 필요시 Tier별 사설IP 대역 지정이 가능합니다.

Tier생성 기능을 통해 DMZ, Private Tier등으로 네트워크를 구분하고 내부서버를 외부접근으로부터 통제할 수 있습니다.

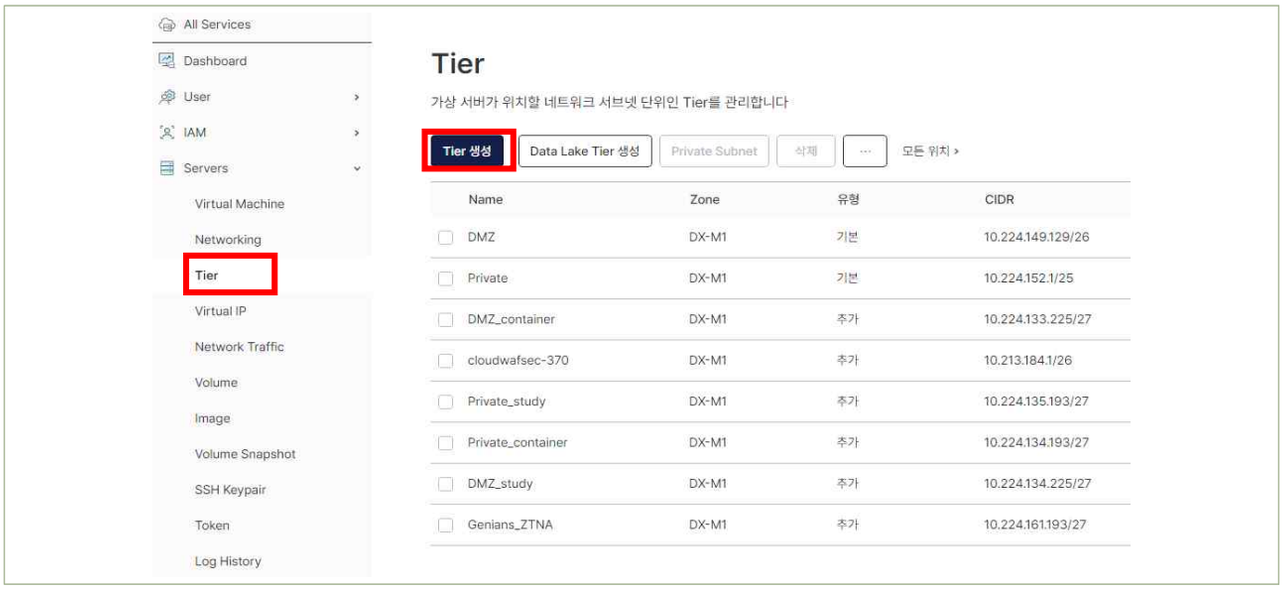


| 그림 2-1-1 | 기본적인 2 Tier Web-WAS-DB 구조

기본으로 제공되는 Tier(DMZ, Private)외 추가 Tier가 필요한 경우 생성 가능합니다.

1) 웹 콘솔 접속 후 Servers 〉 Tier 〉 Tier 생성

콘솔의 Tier 화면의 상단 메뉴바에서 Tier 생성 버튼을 클릭합니다.



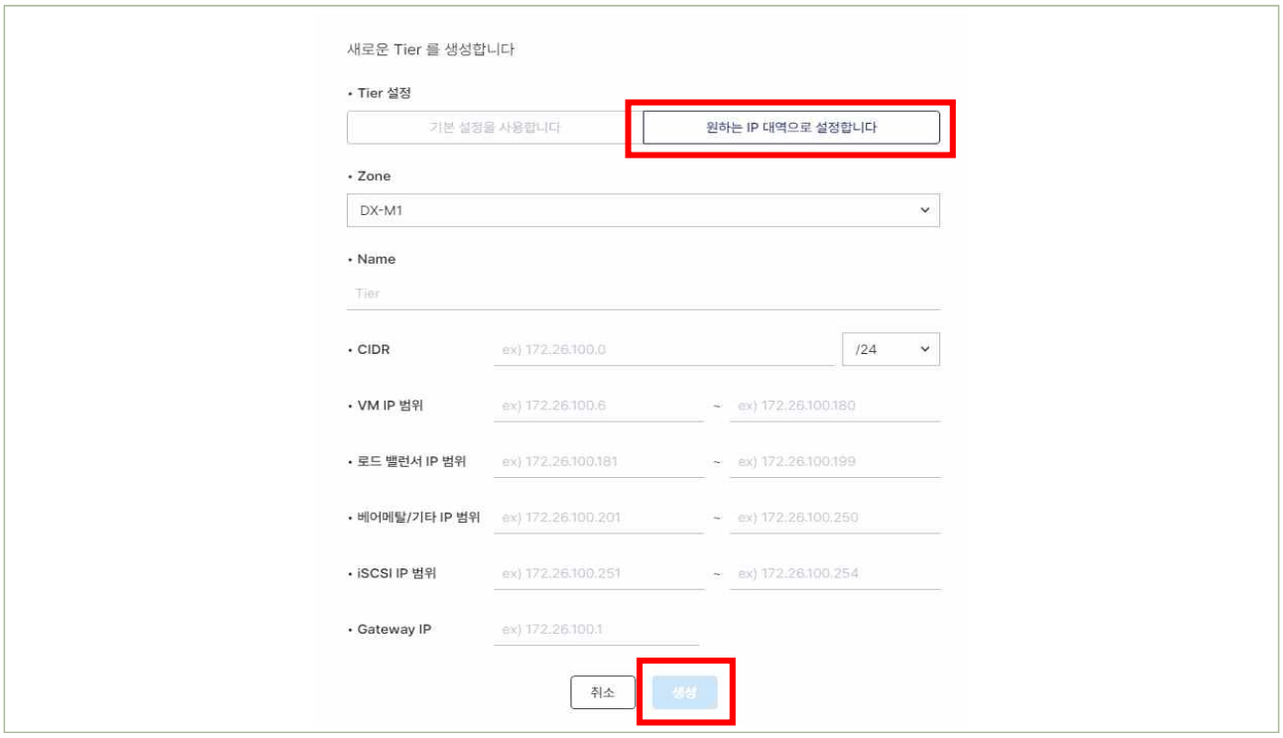
| 그림 2-1-2 | Tier 생성/관리

2) Tier 생성

Tier 생성 팝업화면에서 Tier명과 CIDR을 입력합니다. CIDR은 기존 Tier에서 사용하지 않는 대역을 입력합니다.

| 그림 2-1-3 | Tier 생성(기본)

Tier 생성시 세부 IP 대역을 지정하고자 할 경우 Tier생성 화면 상단의 Tier 설정에서 '원하는 IP 대역으로 설정합니다'버튼을 클릭하면 화면이 다음과 같이 전환됩니다. VM IP대역, 로드 밸런서 IP 대역등 대상 영역별 세부 IP대역을 입력 후 확인버튼을 클릭합니다.



| 그림 2-1-4 | Tier 생성(IP대역 지정)

3) Tier 생성 결과 조회

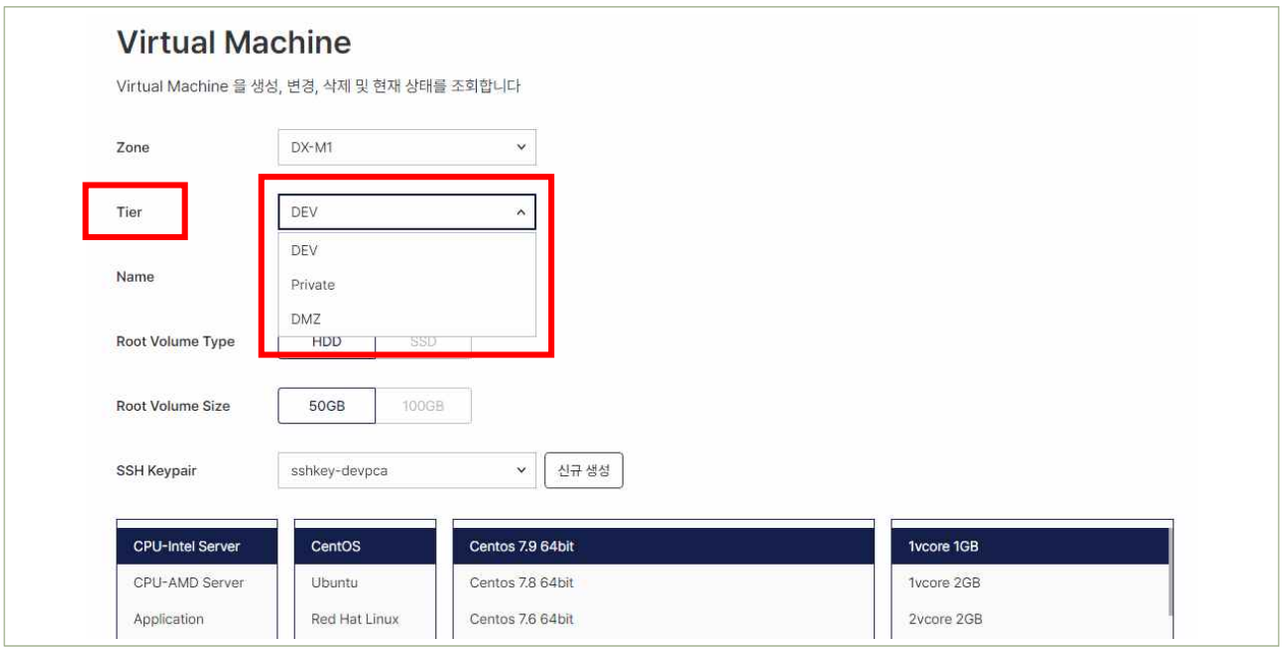
Tier를 생성하고 나면 생성한 Tier의 목록이 조회됩니다.

| 그림 2-1-5 | Tier 현황 조회

4) 서버 생성시 Tier 지정

앞서 생성한 Tier는 서버 생성시 서버가 위치할 Tier(DMZ/Private등)를 지정하여 서버의 배치 위치를 지정합니다.

Servers 〉 Virtual Machine 〉 VM 생성 메뉴 선택 〉 VM 생성 화면에서 Tier 선택



| 그림 2-1-6 | VM 생성시 Tier 선택

4 참고 사항

- Tier 관리 포탈 매뉴얼 참조 : Cloud 매뉴얼 (kt.com)

1 기준

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

2 설명

- 클라우드 환경 내 내부망을 구성하는 경우 외부 침입, 비인가 접근 등으로 보호될 수 있도록 보안 통제 방안을 수립하고 적용하여야 한다

  - 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/아웃바운드 통제 등)
    3) 내부망으로 구현한 가상자원(서버, 데이터베이스 등)에 공인IP 미 할당
    4) 방화벽 서비스를 통한 IP 통제 등

3 우수 사례

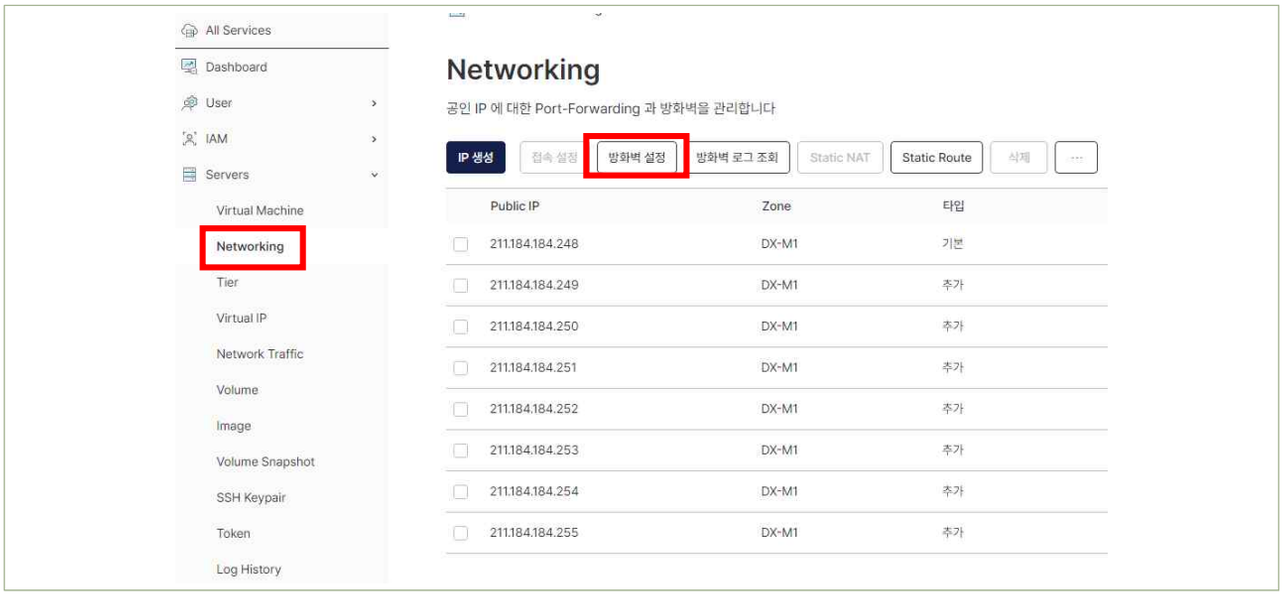
kt cloud는 기본적으로 방화벽 기반의 네트워크 분리/통제를 위한 제반 기능을 제공하며, Tier 기능을 통해 업무목적에 따른 네트워크 분리가 가능합니다(DMZ/Private/Dev등).

① 방화벽/Tier 기반 네트워크 구성 및 통제

서버 생성 후, 기본 상태는 Tier 외부로의 통신이 방화벽으로 막혀 있으며, Tier 외부와 통신을 위해서는 방화벽 설정이 필요합니다(1.4 항목 참조).

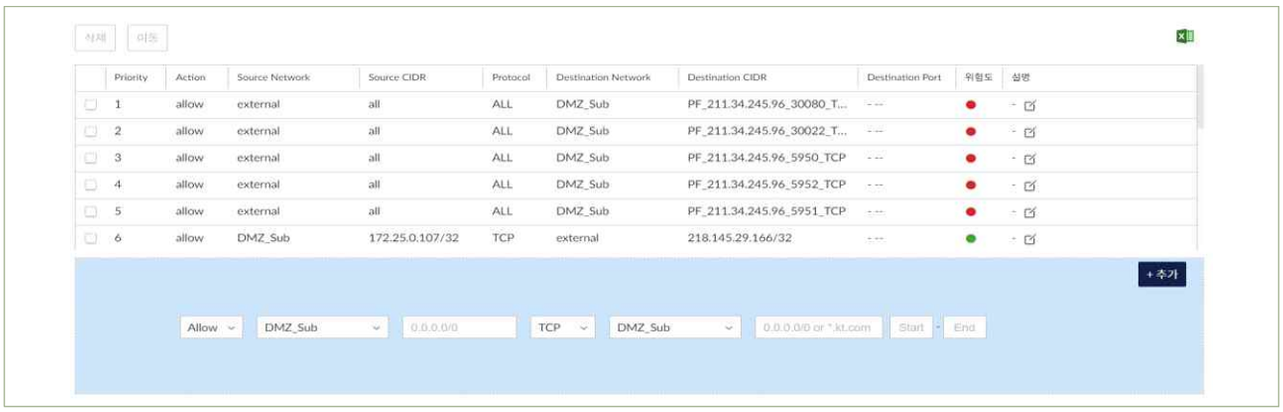
1) 웹 콘솔 접속 후 Servers 〉 Networking 〉 방화벽 설정

Networking 매뉴의 방화벽 정책 관리 기능을 통해 서버의 통신 대상 IP/port 지정을 통해 통신구간 지정할 수 있습니다.



| 그림 2-2-1 | 방화벽 설정 화면

2) 방화벽 정책 설정



| 그림 2-2-2 | 방화벽 정책 확인, 신규 등록

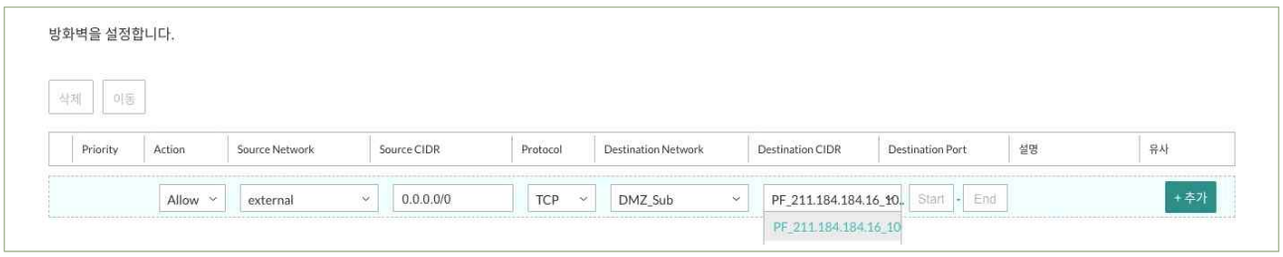
(상황별 방화벽 정책) 외부에서 접속 설정 시 출발지는 External로 설정합니다.

허용할 외부의 IP를 CIDR로 제어할 수 있습니다. Any로 접근을 허용하려면 0.0.0.0/0을 입력합니다.

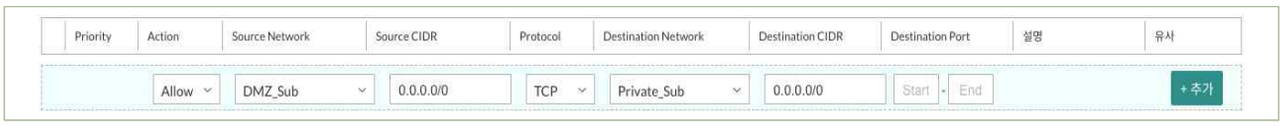
Destination은 서버가 위치한 Tier를 선택합니다.

접속 설정을 이미 한 경우, Destination CIDR 대상으로 고를 수 있도록 보이게 됩니다.

예. PF_211.184.184.16_22_22_TCP (포트포워딩_공인IP_공인포트_프로토콜)



서로 다른 Tier의 서버끼리 통신이 필요한 경우 Source와 Destination을 각각 Tier로 설정합니다.



서버에서 외부로 나가는 Outbound 통신이 필요한 경우 Source에 서버의 Tier와 CIDR를 입력하고 Destination은 External로 설정합니다.

② 내부망 가상자원(서버, 데이터베이스 등)에 공인 IP 미 할당

내부망에 위치하는 서버의 경우 Private Tier에 배치시키고, 외부와의 통신은 내부 서버인 DMZ Tier의 서버(웹서버 등)와만 통신하도록 설정하는 것이 안전합니다.

외부 공중망과 통신을 위한 공인IP 할당은 통상 DMZ Tier에 배치된 서버에만 할당하며, 이를 위한 Port-Forwarding 설정은 1.4 항목의 접속설정 관련 내용을 참고해 주시기 바랍니다.

4 참고 사항

- Server/Networking 포탈 매뉴얼 참조 : Cloud 매뉴얼 (kt.com)

1 기준

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

2 설명

- 클라우드 환경 내 가상자원을 보호하기 위해 네트워크 보안 관제를 수행하여야 한다.

  - 예시

    1) 금융권 보안관제 이용

    2) 금융회사 보안관제 서비스와 연동하여 관제 수행(클라우드 내부 발생하는 네트워크 트래픽 연동 등을 활용)

    3) 클라우드 서비스 제공자가 제공하는 가상자원 보호를 위한 네트워크 보안관제 및 유사기능(DDoS, WAF등) 활용

3 우수 사례

① 금융권 보안관제 이용

kt cloud는 보안이 강화된 금융사 전용인 금융존을 제공하고 있으며, 관련 트래픽 연계를 위해 네트워크 인프라에 금융보안원의 네트워크 tap 장비가 구축되어 있어 금융보안원의 보안관제 이용이 가능합니다.

② 금융회사 보안관제 서비스와 연동하여 관제 수행

금융회사 자체 보안관제를 진행할 경우 kt cloud 네트워크내 위치한 IPS 장비의 로그를 금융사로 실시간 연동하여 금융사 자체적인 보안관제가 가능하도록 지원합니다.

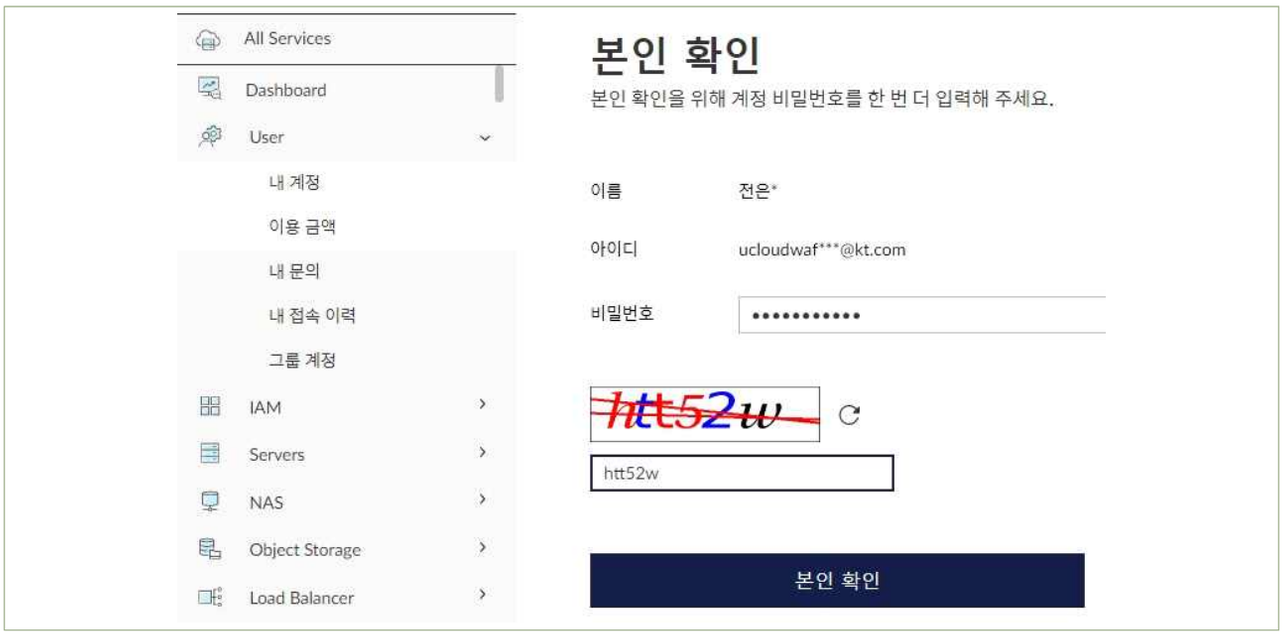
③ kt cloud 제공 네트워크 보안관제 서비스 이용

(보안관제) kt cloud에서는 IPS 보안 인프라 기반의 보안관제 서비스를 제공하며, 전문 보안관제 인력을 통해 24x365 모니터링을 제공합니다. 보안관제 서비스를 통해 외부 네트워크 및 내부 네트워크로부터의 침입시도에 대해 탐지하고 고객서비스를 보호합니다.

보안관제는 고객 서비스 특성을 반영하며 주기적인 보안정책 최적화를 통해 관제가 수행됩니다.

보안관제 서비스 신청을 위해서는 콘솔에서 아래의 순서에 따라 진행하시면 됩니다.

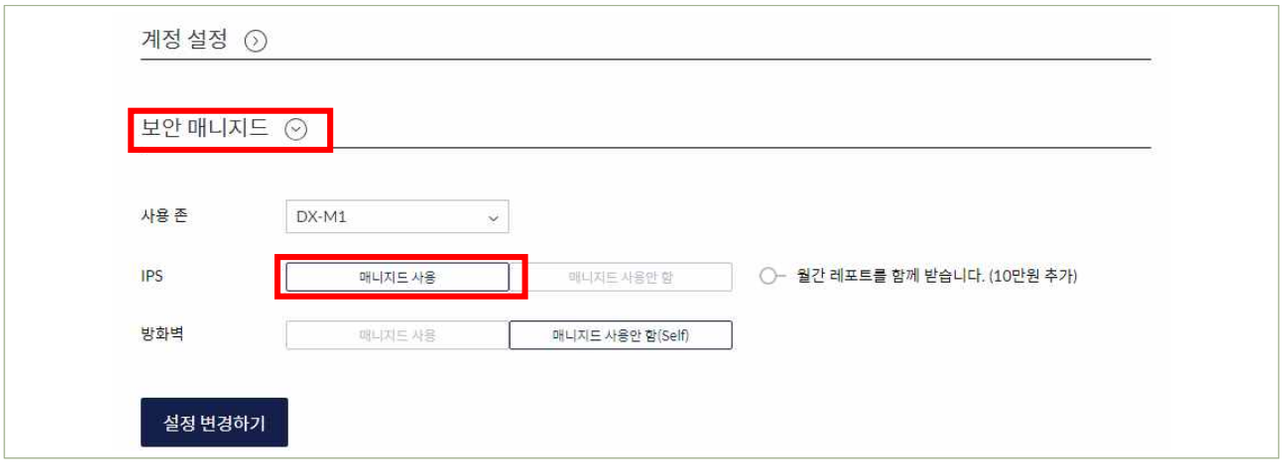
1) 웹 콘솔 접속 후 User 〉 내 계정 〉 본인 확인(비밀번호 재 입력)



| 그림 2-3-1 | 내계정 메뉴 접속을 위한 본인 확인

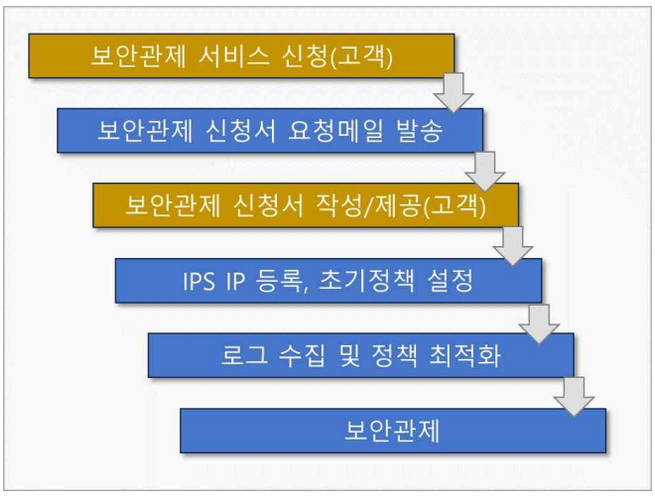
2) 보안 매니지드 메뉴에서 IPS 매니지드 서비스 신청

보안 매니지드 서비스는 2가지 유형이 있으며, IPS 메니지드는 보안관제 서비스를 제공하며 방화벽 매니지드는 고객의 방화벽 정책관리를 별도 전문인력을 통해 지원해 드립니다.



| 그림 2-3-2 | 보안 매니지드 선택항목 신청

보안관제 서비스 신청 후에는 별도 안내메일을 통해 고객서비스 신청서, 고객 네트워크 구성 정보 제공을 요청 드리며, 관련 정보 수신 후 보안관제 수용이 진행됩니다.



| 그림 2-3-3 | 보안관제 서비스 진행 절차

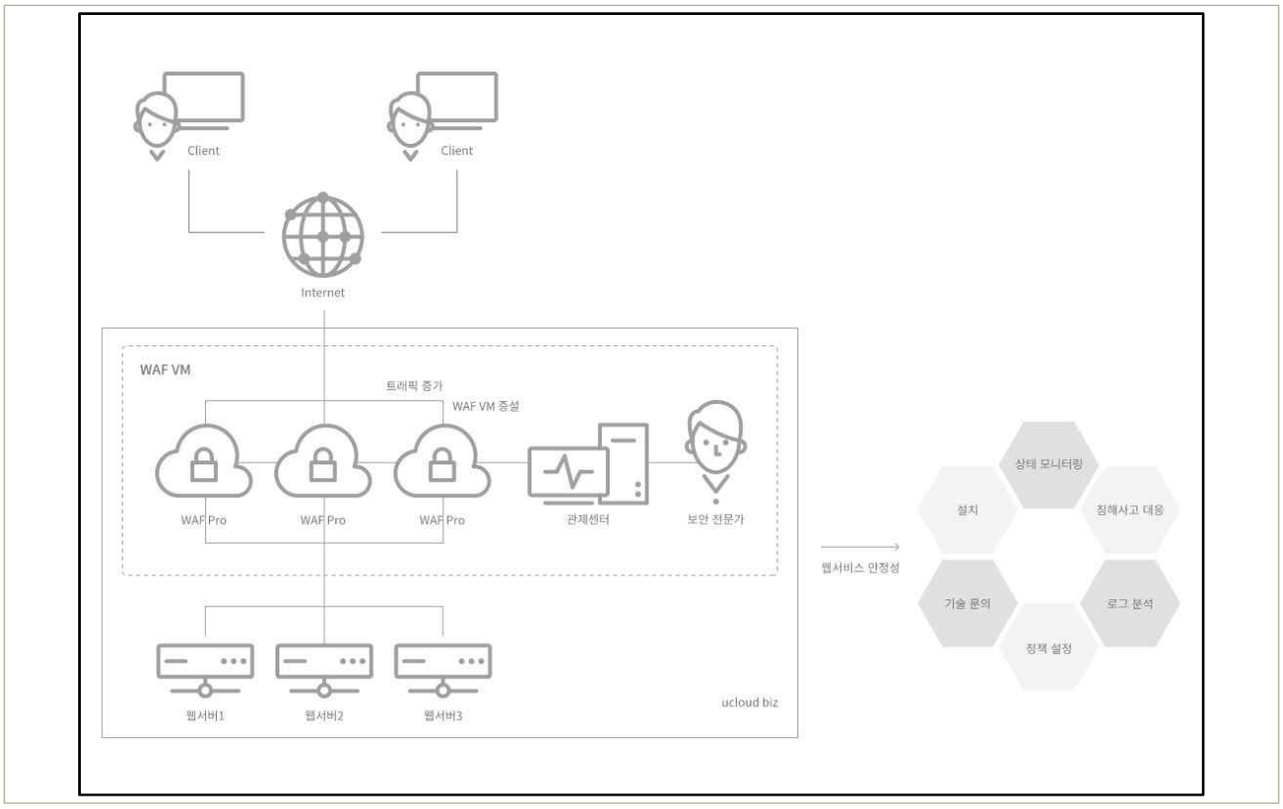
(WAF) 웹 방화벽은 웹서버 앞에 위치하여 외부로부터 들어오는 HTTP/HTTPS 트래픽을 감시하여 웹 애플리케이션에 대한 악의적인 공격이 탐지되면 해당 공격이 웹서버에 도달하기 전에 차단하는 역할을 수행합니다.

kt cloud 웹방화벽에는 WAF, WAF Pro의 2가지 서비스가 제공됩니다.

WAF Pro의 경우 별도의 보안관제 전문 인력에 의해 보호대상 웹서버 등록, 정책 설정 관리, 24x365 모니터링이 진행됩니다. 초기 환경구성을 위해 방화벽 오픈 등 필요한 사항에 대해 고객 안내사항은 메일로 발송됩니다.

WAF의 경우, 고객 안내사항은 메일로 발송되나, 보호대상 웹서버 등록, 정책 설정 관리, 보안 모니터링을 고객이 직접 수행해야 합니다.

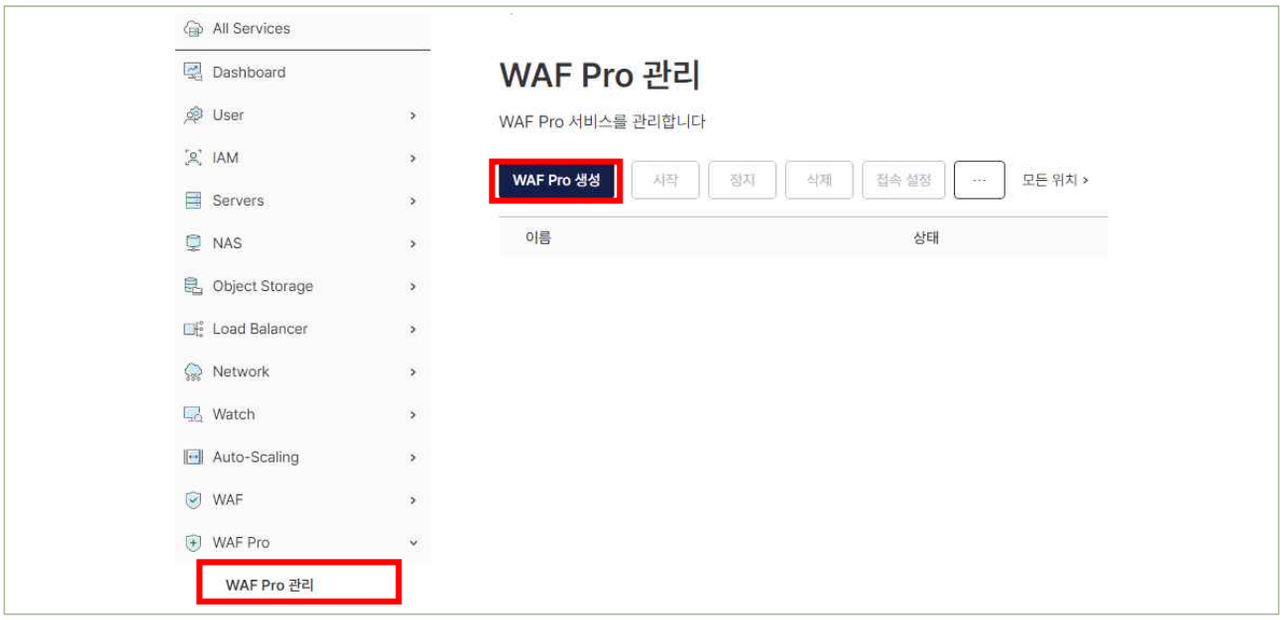
웹방화벽의 네트워크 구성 방법은 Reverse Proxy 방식으로 일반적인 Web Proxy 서버와 동일한 구성으로 위치시킵니다.



| 그림 2-3-4 | WAF Pro 서비스 구성도

웹방화벽 서비스 구성을 위해서는 콘솔에서 아래의 순서에 따라 진행하시면 됩니다(WAF Pro 사례).

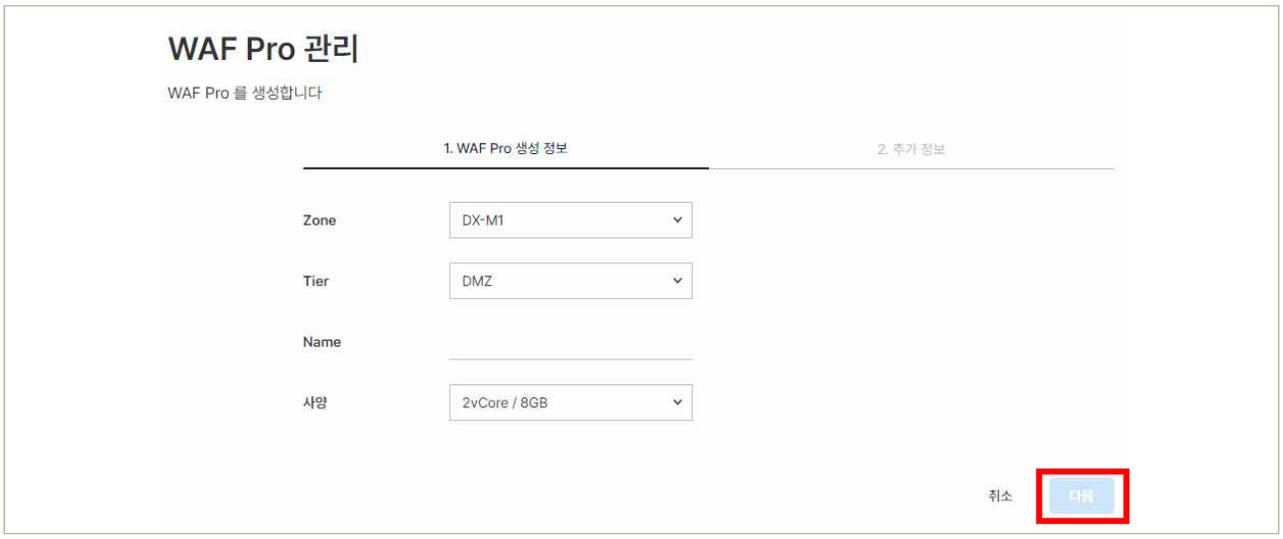
1) 웹 콘솔 WAF Pro 〉 WAF Pro 관리 〉 WAF Pro 생성



| 그림 2-3-5 | WAF Pro 메뉴 화면

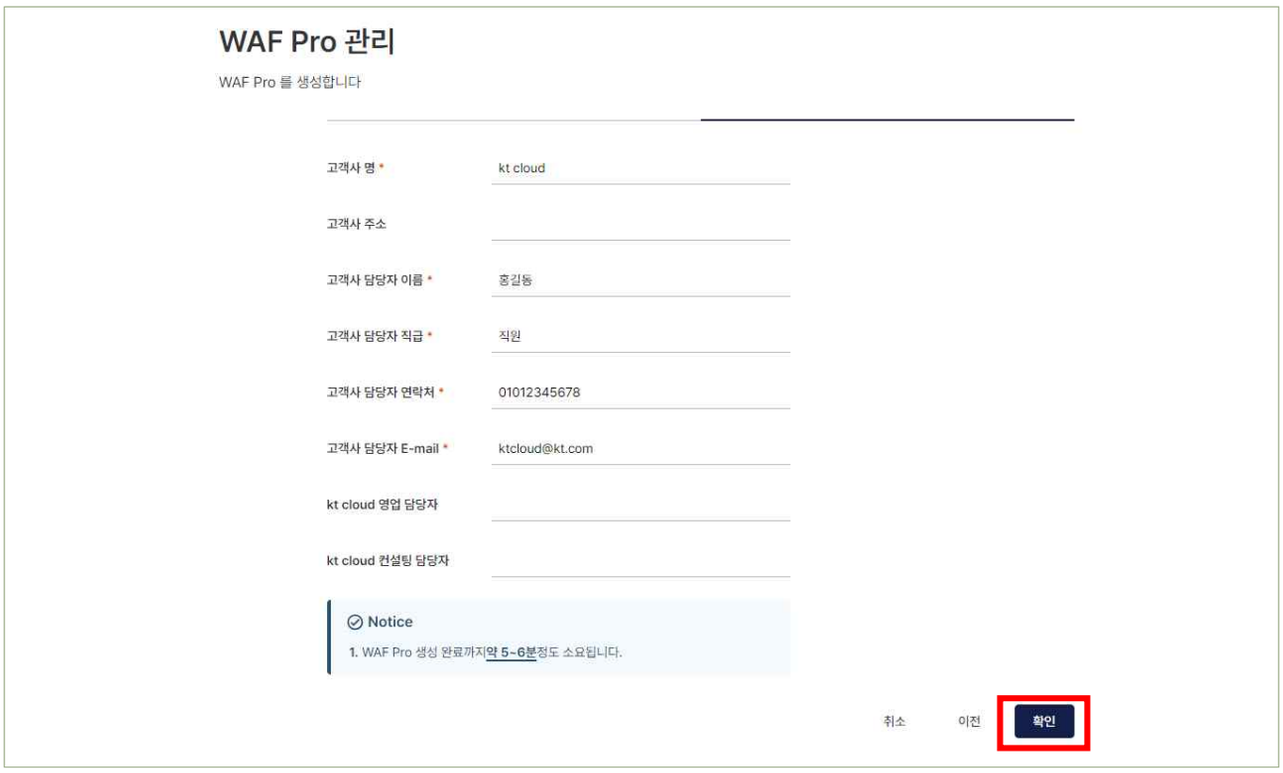
2) WAF 생성

WAF 생성화면에서 생성할 WAF가 위치할 Zone, Tier 및 WAF의 사양(예, 2Core/8GB)을 선택 후 다음버튼을 클릭합니다.



| 그림 2-3-6 | WAF Pro 신규 생성

다음 단계로 담당자 연락처 등의 정보 입력을 통해 생성이 완료됩니다.



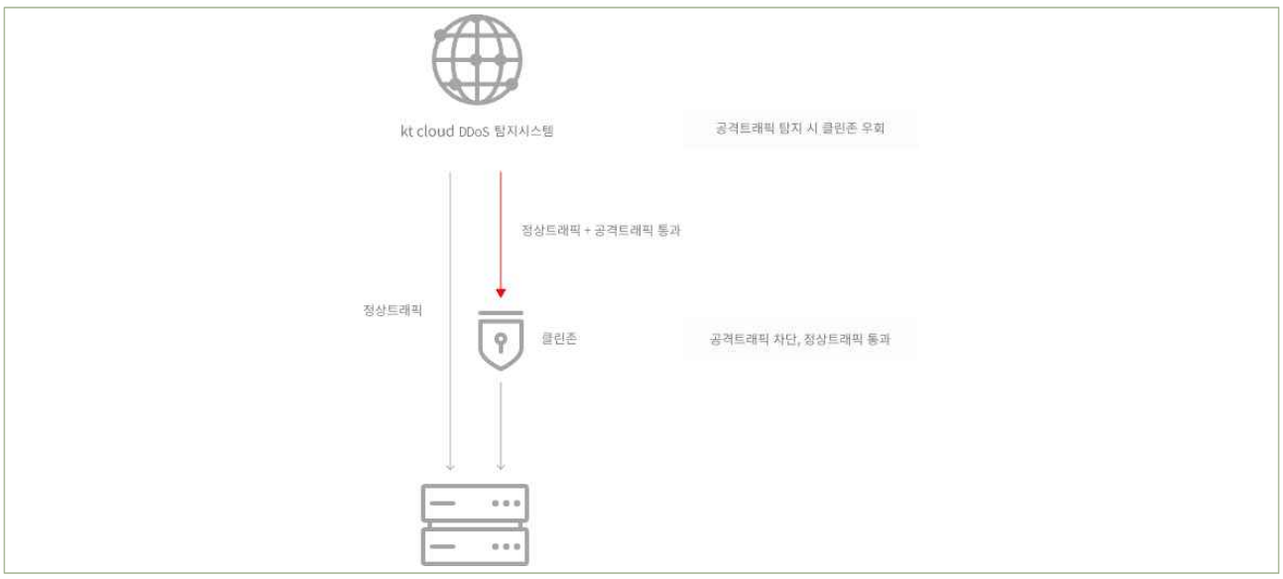
| 그림 2-3-7 | WAF Pro 신규 생성(추가정보 입력)

3) WAF 조회

| 그림 2-3-8 | WAF 생성 결과 조회

WAF 생성 후에는 WAF/WAF Pro 화면에서 생성된 WAF의 조회가 가능합니다
추가로 WAF 환경구성을 위해 방화벽 오픈 등 필요한 사항에 대해 고객 안내사항은 메일로 발송됩니다. 방화벽 오픈 등 환경구성이 완료되면 WAF의 상태가 정지상태에서 사용상태로 변경됩니다.
WAF Pro의 경우 별도의 WAF 보안관제 전문 인력에 의해 24x365 모니터링이 진행됩니다.

(DDoS) DDoS 공격 모니터링 및 방어를 위해 kt cloud에서는 클린존 서비스를 제공합니다. 클린존 서비스는 DDoS 공격 발생시 유해 트래픽을 차단하고 정상 트래픽 만을 서버로 전달하여 DDoS 공격 시에도 정상적인 서비스 운영이 가능합니다(서비스 연속성 보장). kt cloud 인터넷망에 구축된 DDoS 전용 탐지/방어 시스템을 통하여 최신 DDoS 공격 방어가 가능하며, 보안전문가를 통한 24시간 365일 보안관제를 제공합니다.



| 그림 2-3-9 | 클린존(DDoS 방어) 서비스 제공 구조

1) 웹 콘솔 접속 후 클린존 〉 클린존 관리 〉 신청

| 그림 2-3-10 | 클린존 신청 화면

2) 보호 대상 IP를 선택하고 DDoS 대응 담당자 정보 입력 후 신청 버튼 클릭

| 그림 2-3-11 | 클린존 신청정보 입력

4 참고 사항

- 금융사 자체 보안관제를 위한 IPS 로그 연동은 kt cloud 테크센터로 별도 문의주시면 지원 가능합니다.
  - 고객센터 : 080-2580-005
  - 이메일 : techcenter@kt.com
- 보안상품 포탈 매뉴얼 참조 : Cloud 매뉴얼 (kt.com)

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

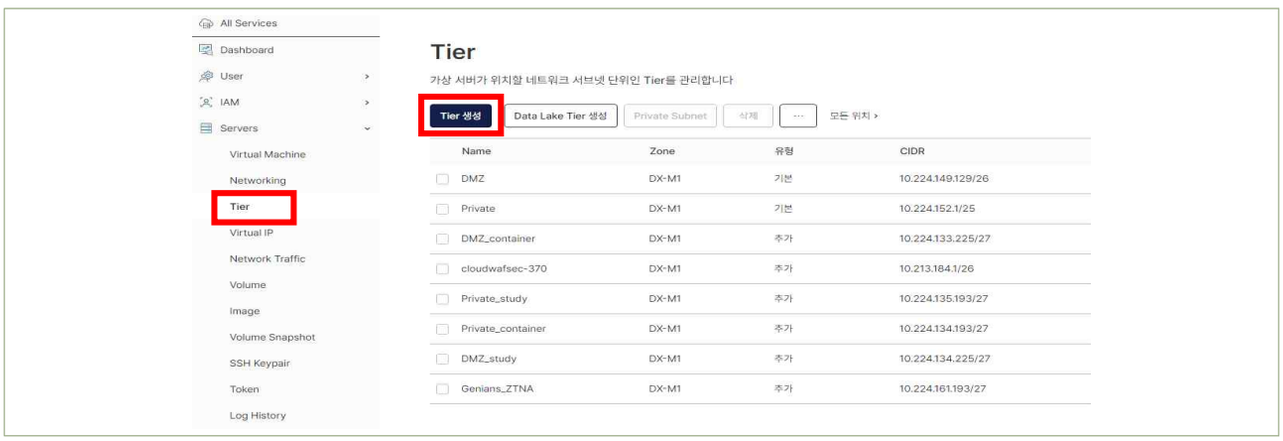
3 우수 사례

① Tier를 통한 DMZ/Private 네트워크 분리

방화벽 기반의 네트워크 분리를 위한 기능을 제공하며, Tier 기능을 통해 업무목적에 따른 네트워크 분리가 가능합니다(DMZ/Private/Dev등).

기본적으로 DMZ, Private 2개의 Tier는 제공되며, 추가적인 네트워크 분리를 위한 Tier의 생성도 가능합니다. Tier에 관한 보다 자세한 설명은 본 참고서 "2.1 업무 목적에 따른 네트워크 구성" 내용을 참고해 주시면 됩니다.

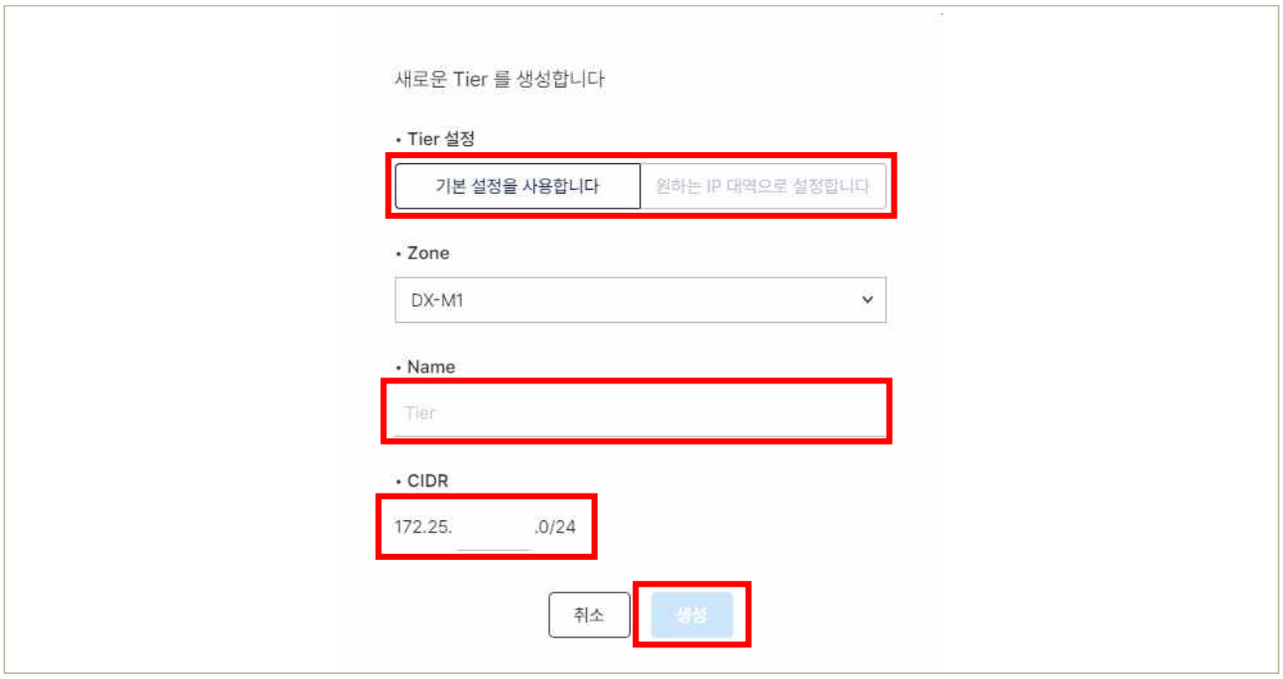
1) 웹 콘솔 접속 후 Servers 〉 Tier 〉 Tier 생성



| 그림 2-4-1 | Tier 관리 화면

2) 목적에 따라 Tier 생성이 가능하며 필요 시 사설 IP 대역 지정

Tier생성 기능을 통해 DMZ, Private Tier로 네트워크를 구분하고 내부서버를 외부접근으로부터 통제할 수 있습니다.



| 그림 2-4-2 | Tier 신규 생성

3) Tier 조회

| 그림 2-4-3 | Tier 생성 결과 확인

Tier 생성 후 DMZ/Private Tier내 서버간 통신이나 DMZ Tier와 외부 공중망의 통신을 위해서는 방화벽 포트 오픈 설정이 필요하며, 이에 대해서는 본 보안참고서내 "1.4 가상자원 생성 시 네트워크 설정 적용", "2.2 내부망 네트워크 보안통제" 내용을 참고해 주시면 됩니다.

② 가상자원 OS레벨 ACL 설정

공개용 웹서버 등에 직접 접속하는 접속자(IP)를 서버에서 ACL 설정을 통해 통제가 가능하며, 세부

적용 방안은 다음과 같습니다.

1) /etc/hosts.allow 파일을 편집하여 접속 허용 대상IP를 추가합니다.
(아래의 예시는 2개의 접속자 IP를 등록한 경우임)

```
# vi /etc/hosts.allow
sshd: 123.123.123.123 123.123.123.124
```

2) /etc/hosts/deny 파일을 편집하여 허용 IP외 모든 접근을 차단하려면 아래와 같이 “sshd : ALL” 내용을 파일 하단에 추가합니다.

```
# vi /etc/hosts.deny
sshd : ALL
```

3) sshd 서비스 재기동 합니다.

```
# service sshd restart
```

4 참고 사항

- 포탈 Tier 매뉴얼 참조 : Cloud 매뉴얼 (kt.com)
- 포탈 Networking 매뉴얼 참조 : Cloud 매뉴얼 (kt.com)

1 기준

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

2 설명

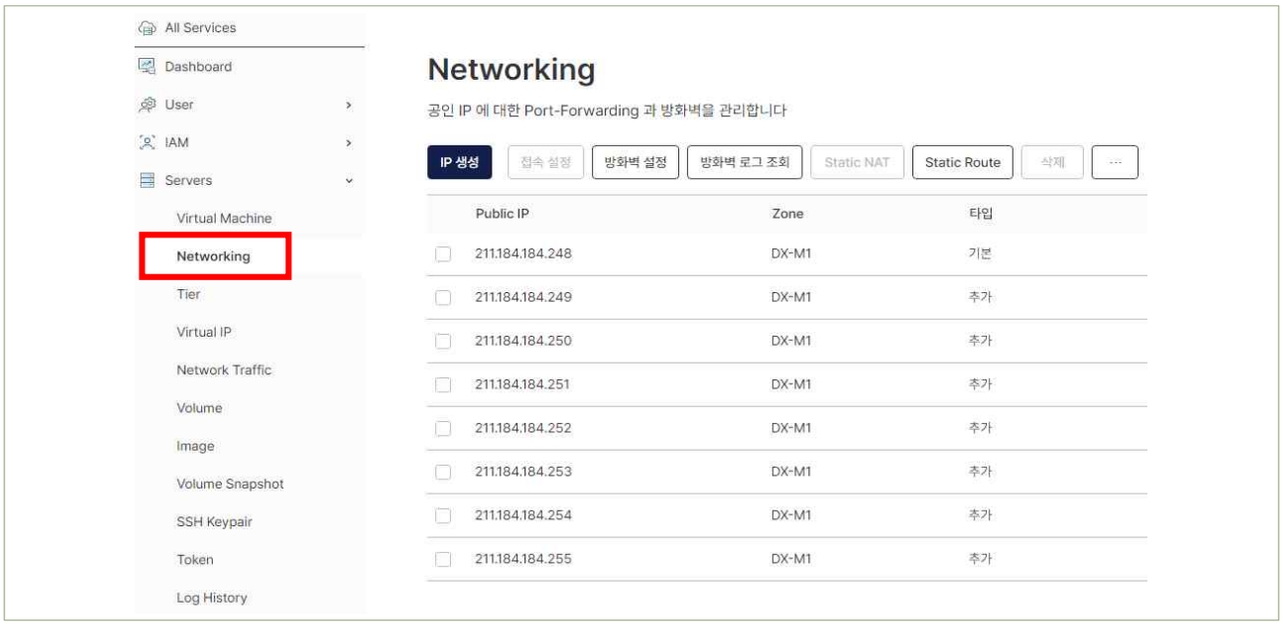
- 클라우드 환경 내 내부망 네트워크 구현 시 사설IP를 부여하고 주기적으로 현황을 검토하여야 한다.
  - 예시
    1) 인터넷 게이트웨이, NAT 게이트웨이 등 관련 기능을 통해 사설IP부여 및 IP 관리 수행
    2) 사설 IP 할당 현황에 대한 주기적 검토 수행

3 우수 사례

서버를 생성하면 사설IP가 자동 할당되며, 필요한 경우 사설IP를 별도 지정할 수 있습니다. 생성된 서버는 동일한 Tier 내에서만 통신이 가능하며, 외부 인터넷 구간에서 접속하려면 NAT설정을 통한 공인IP 할당 작업이 필요합니다.

| 그림 2-5-1 | 서버 생성 후 조회 화면

1) 웹 콘솔 접속 후 Servers 〉 Networking



| 그림 2-5-2 | Network 설정 화면

2) 공인 IP 선택 후 접속 설정

| 그림 2-5-3 | 공인IP를 통한 외부 접속 설정

3) VM 접속을 위한 접속 설정(Port-Forwarding 혹은 1:1 NAT)

(접속설정) (콘솔) Servers 〉 Networking 메뉴에서 접속 설정에 사용할 공인 IP를 선택한 후 '접속설정'을 클릭하면 Port-Forwarding 설정을 할 수 있습니다.

| 그림 2-5-4 | Port-Forwarding 설정 확인

- 서버: 접속 설정을 할 서버를 선택합니다.
- 사설Port: 서버의 어떤 Port로 접근할 것인지 선택합니다. OS 접근을 위해서는 리눅스는 22(SSH), 윈도우는 3389(RDP)를 사용합니다. 선택한 서버의 OS에 따라 자동으로 나타납니다. 이 외에 웹 서비스 80(HTTP), 443(HTTPS), FTP(21) 등이 있습니다.
- 공인IP: 앞서 선택했던 공인IP입니다.
- 공인Port: 외부에서 접근할 때 사용할 공인Port를 지정합니다. 사설Port와 같은 번호를 써도 되고, 다른 번호를 써도 됩니다.
- 프로토콜: 사용할 프로토콜을 설정합니다.

이와 같이 Port를 1:1로 연결할 수도 있고, 아래 '포트를 범위로 설정' 옵션을 사용하여 N:N개로 연결할 수도 있습니다.

| 그림 2-5-5 | 포트를 범위로 설정 가능

4 참고 사항

- Networking 포탈 매뉴얼 참조 : Cloud 매뉴얼 (kt.com)

1 기준

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

2 설명

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

3 우수 사례

금융회사 및 전자금융업자는 클라우드 서비스를 통해 구현한 네트워크 정책에 대해 주기적 검토를 수행

"2. 네트워크 관리" 분야 내 내용을 참고하여 방화벽, ACL, 보안그룹 등에 대해 검토

4 참고 사항

- Networking 포탈 매뉴얼 참조 : Cloud 매뉴얼 (kt.com)

3. 계정 및 권한 관리

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

3 계정 및 권한 관리

1 기준

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

2 설명

- 클라우드를 이용하는 임직원의 업무 및 권한에 따라 계정을 관리하여야 한다.
  - 예시
    1) 자격 증명 등의 기능을 이용하여 계정 권한 관리
    2) 사전에 정의된 행위만이 가능하도록 역할을 생성

- 콘솔 최상위 관리자(ex. 최초 가입계정 등)은 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

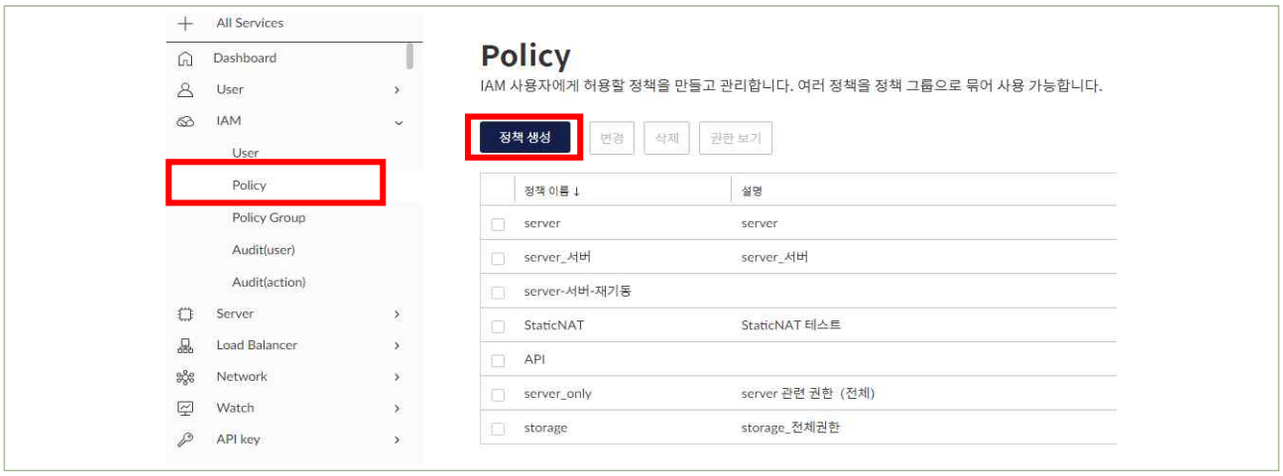
① 사용자 계정 및 권한 관리

IAM 사용자(user)별 권한 관리를 통해 임직원의 업무에 따른 개별 권한부여가 가능합니다.

콘솔에서 루트 계정으로 접속 후 개별 사용자(user)에 대한 권한부여/변경이 가능합니다.

1) 웹 콘솔 접속 후 IAM 〉 Policy 〉 정책 생성

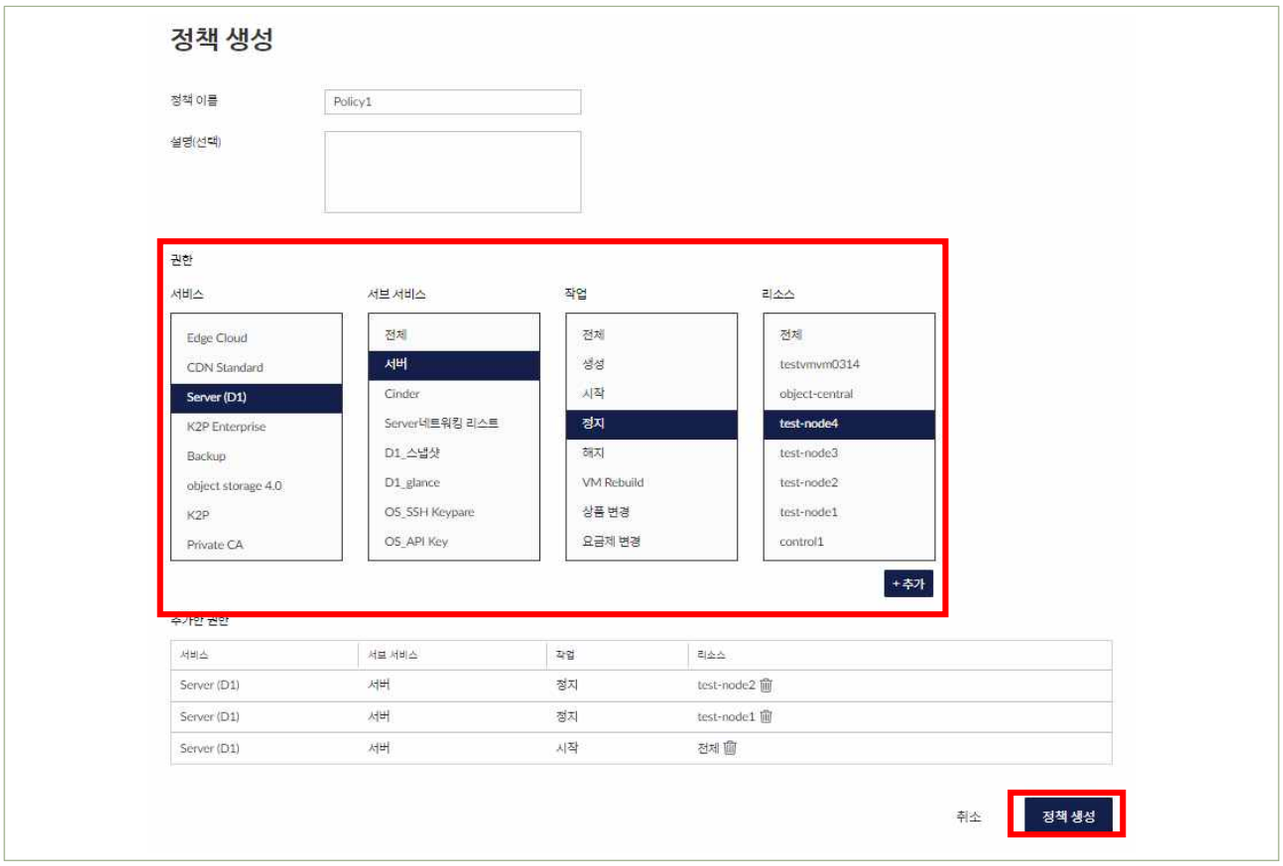
사용자별 권한 부여/관리는 Policy 기능을 통해 가능하며, 권한 관리를 위해 우선 Policy를 생성합니다.



| 그림 3-1-1 | 사용자 정책(Policy) 관리

2) 정책 명, 필요 권한 추가 후 정책 생성

Policy 정책 생성 화면에서 사용자에게 부여할 자원과 작업 유형을 선택합니다. 예를 들어, 서버의 시작, 정지 권한을 부여할 수 있으며, 작업 권한은 로드밸런서, 스토리지등 서비스에 따라 달라집니다.



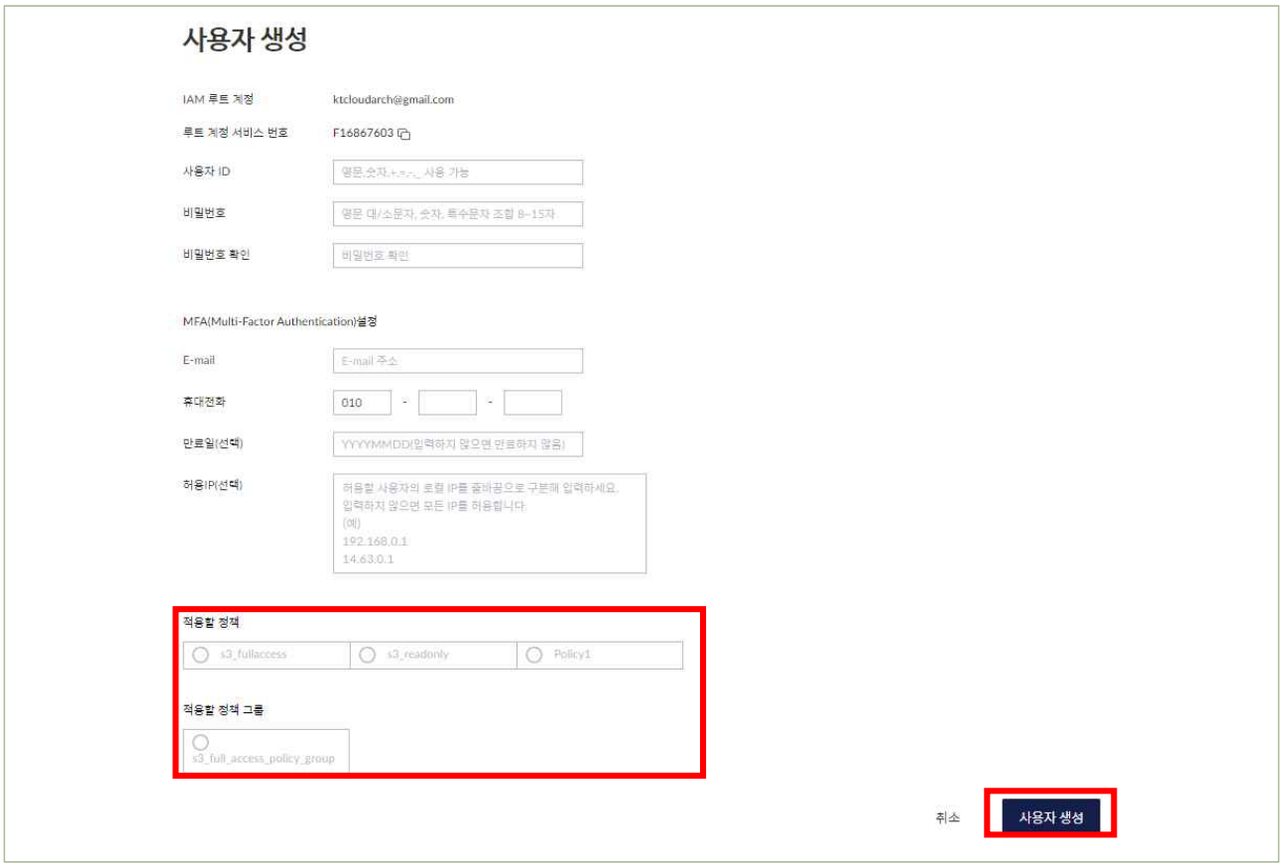
| 그림 3-1-2 | 사용자 권한 관리를 위한 정책 생성

3) IAM 〉 User 〉 사용자 생성

| 그림 3-1-3 | IAM 사용자 생성

4) 사용자 생성 시 권한 정책 적용

앞서 Policy에서 생성한 권한 정책은 IAM에서 사용자 생성시 조회 및 선택할 수 있습니다.



| 그림 3-1-4 | IAM 사용자 생성시 권한 할당

IAM 〉 Policy Group 메뉴에서 '정책 그룹 생성' 버튼을 통해 여러 Policy를 Policy Group으로 묶어서 사용하는 것 또한 가능합니다.

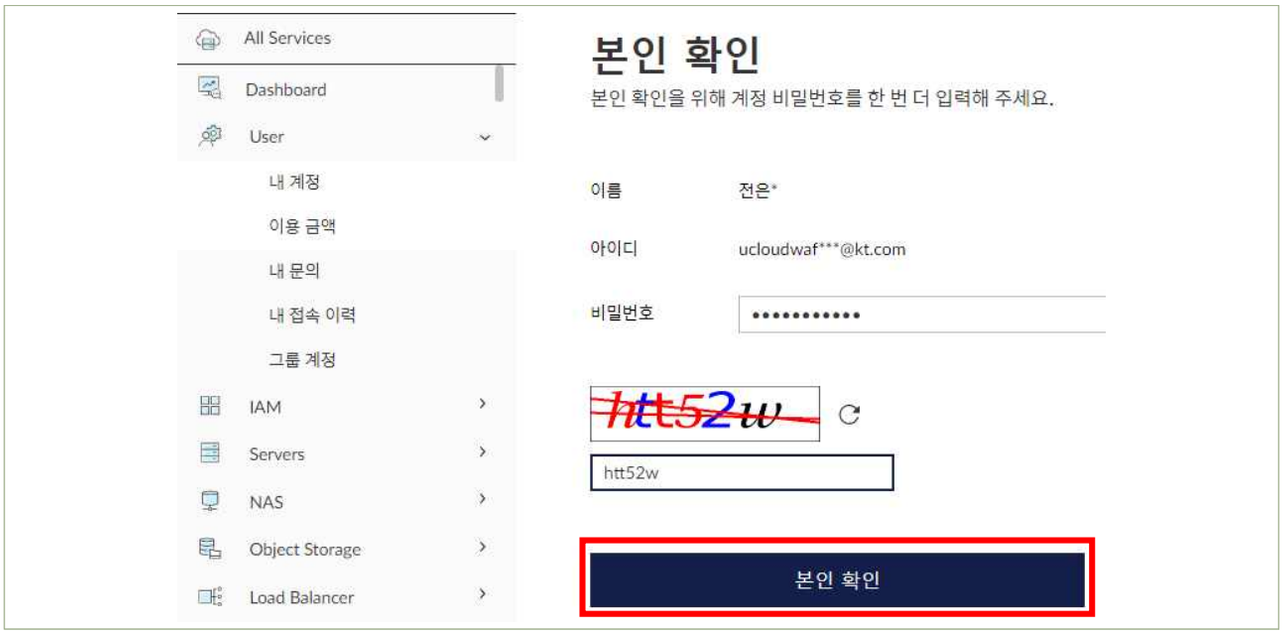
| 그림 3-1-5 | 정책 그룹 생성 예시

② 루트 계정의 접근 제한

(MFA 적용)

콘솔 root 계정(최상위 관리자)의 보안강화를 위해 SMS, 이메일 인증 등 MFA 인증 설정이 가능합니다.

1) 웹 콘솔 접속 후 User 〉 내 계정 〉 본인 확인(비밀번호 재 입력)

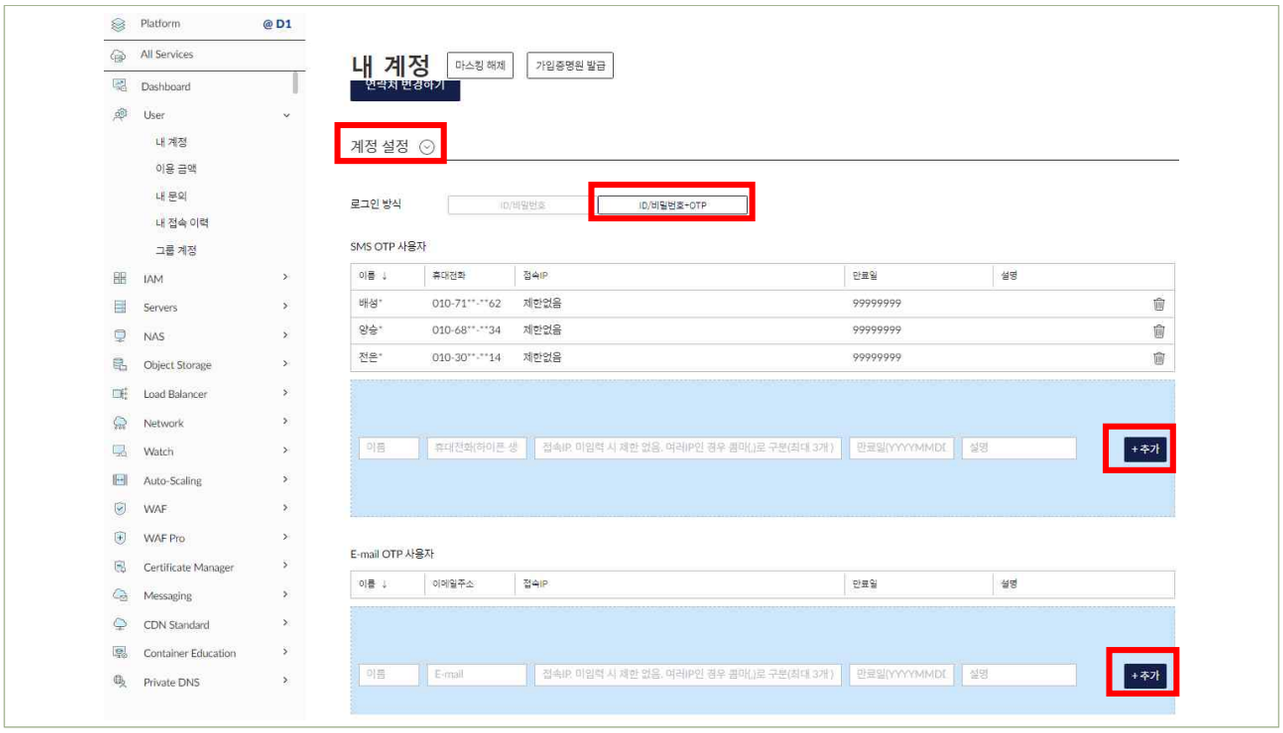


| 그림 3-1-6 | 내 계정 메뉴 접속을 위한 본인 재확인

2) 계정 설정 〉 로그인 방식 변경(ID/비밀번호 + OTP)

내 계정 화면의 하단 계정 설명 항목 중 로그인 방식의 ID/비밀번호+OTP 버튼을 선택하면 하단에 SMS 및 Email OTP 설정을 위한 연락처 정보 등록창이 표시됩니다.

각 항목 입력 후 우측의 추가 버튼을 클릭합니다.



| 그림 3-1-7 | 내 계정 화면에서 MFA 설정(루트 사용자)

3) SMS/Email 정보 추가 후 내 계정 화면의 하단의 설정 변경하기 버튼을 클릭하여 최종 MFA 변경 정보를 저장합니다.

| 그림 3-1-8 | 내 SMS/Email OTP 연락처 기재

(root 계정의 접속 IP 제한)

콘솔 관리자 계정의 보안강화를 위해 접속IP를 제한하도록 설정할 수 있습니다.

1) User 〉 내 계정 화면 하단의 접속 IP 허용 관리를 통해 접근 경로 제한 가능합니다.
2) 하단 접속IP 허용 관리 우측의 사용 버튼을 클릭합니다.
3) 접속IP허용 항목에 IP 추가 후 우측의 추가하기 버튼을 클릭합니다.
4) 마지막으로 화면 하단의 설정 변경하기 버튼을 클릭하여 변경사항을 저장합니다.

| 그림 3-1-9 | 접속허용 IP 등록

4 참고 사항

- IAM 사용 포탈 매뉴얼 참조 : **Cloud 매뉴얼 (kt.com)**

1 기준

식별번호	기준	내용
3.2.	**이용자별 계정 부여**	**클라우드 서비스 이용하는 임직원(개인)별 인증 수단을 할당하여야 한다.**

2 설명

- 클라우드를 이용하는 임직원(이용자) 별 인증수단을 부여하여야 하며, 필요 시 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

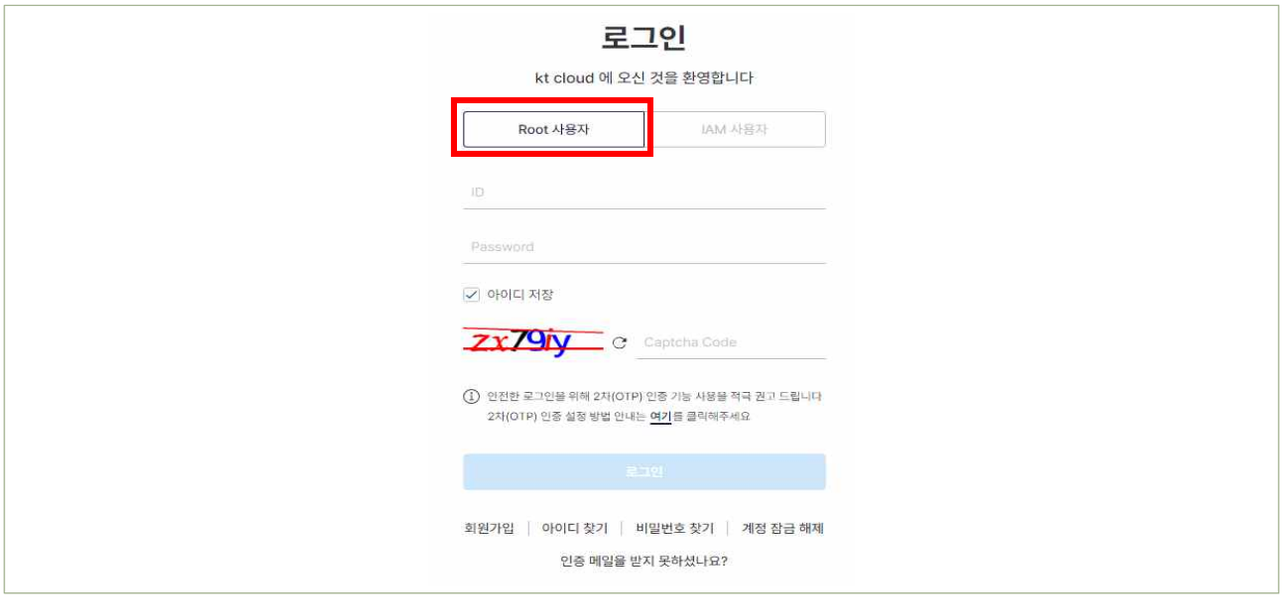
콘솔의 IAM 기본 기능을 통해 개인별 계정을 할당하고 개별 계정에 대한 보안강화를 위해 2차 인증을 설정할 수 있습니다.

① 개인별 계정 할당

사용자별 콘솔계정을 부여할 수 있으며 사용자 계정 생성을 위해 콘솔에 루트계정으로 접속 후 user 생성을 진행합니다.

1) 콘솔 루트 사용자 접속

콘솔 로그인 시 상단의 Root 사용자 탭을 선택하여 Root 계정으로 로그인합니다.



| 그림 3-2-1 | 콘솔 로그인

2) 웹 콘솔 접속 후 IAM 〉 User 〉 사용자 생성

콘솔 접속 후 User 메뉴에서 임직원 개인별 계정을 생성합니다.

| 그림 3-2-2 | IAM 사용자 관리

② IAM User의 MFA 인증 설정

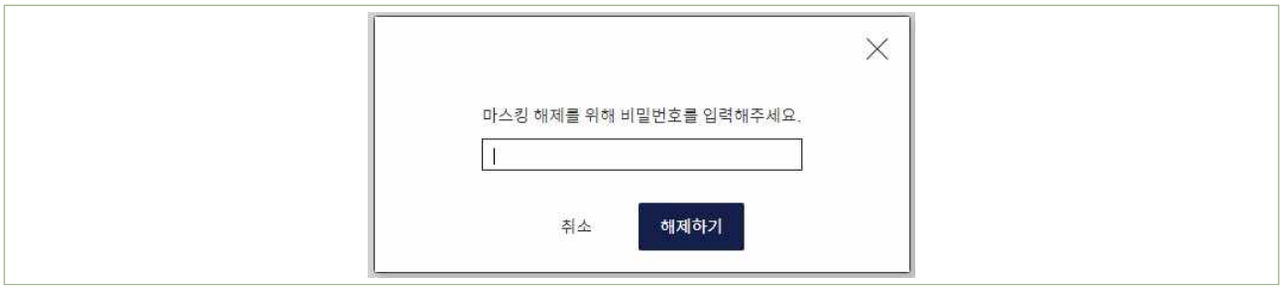
IAM 사용자 계정에 대한 MFA 설정을 위해 사용자 목록에서 대상 사용자 계정을 선택 후 화면 상단의 변경 버튼을 클릭해 사용자 상세 화면을 접속합니다.

다만, 사용자 변경을 위해 사전 단계로 본인 재확인을 위한 마스킹 해제 단계를 진행해야 합니다.

1) 웹 콘솔 접속 후 IAM 〉 User 〉 대상 사용자 선택 〉 마스킹 해제

| 그림 3-2-3 | User화면에서 마스킹 해제 수행

2) 계정 비밀번호 재 입력



| 그림 3-2-4 |

3) 사용자 변경

| 그림 3-2-5 | 사용자 선택 후 변경 실행

4) MFA 설정(휴대전화 번호 or 이메일 주소 입력)

사용자 변경 화면에서 MFA 설정을 위한 Email 또는 휴대전화 정보를 입력 후 하단의 MFA 설정변경 버튼을 클릭합니다.

| 그림 3-2-6 | IAM 사용자 MFA 설정

5) 사용자 변경(MFA 설정)이 완료되면 이후 콘솔 로그인 시 사용자에 설정된 OTP(SMS/Email) 인증을 하여 로그인 합니다.

| 그림 3-2-7 | 로그인 시 OTP인증 유형 선택

4 참고 사항

- IAM 사용 포탈 매뉴얼 참조 : **Cloud 매뉴얼 (kt.com)**

1 기준

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

2 설명

- 클라우드를 이용하는 임직원의 인사변경 사항 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

인사변경 발생시 IAM 기능을 통해 해당 이용자 계정의 패스워드를 변경하거나 계정을 삭제할 수 있습니다.

1) 루트 계정으로 웹 콘솔 접속 후 IAM 〉 User 에서 사용자 목록 중 대상 사용자ID를 선택 후 화면 상단의 변경 또는 삭제 버튼을 클릭합니다.

| 그림 3-3-1 | 사용자 선택 후 변경 실행

2) 사용자 선택 후 변경 버튼을 클릭한 경우 사용자 변경 화면이 팝업으로 나타나며, 비밀번호, 비밀번호 확인 항목에 새로운 비밀번호를 입력 후 우측의 비밀번호 변경 버튼을 클릭시

인사변경 대상 사용자의 패스워드는 변경됩니다.

| 그림 3-3-2 | 사용자 패스워드 변경 또는 허용IP 변경

3) IAM에서 인사변경 대상 사용자를 삭제할 경우 루트계정으로 콘솔 접속 후 IAM〉 User 화면에서 사용자 목록에서 해당 사용자를 선택 후 화면상단의 삭제 버튼을 클릭합니다. 이후 나타나는 팝업 화면에서 삭제하기를 클릭합니다.

4 참고 사항

- IAM 사용 안내 포탈 매뉴얼 참조 : **Cloud 매뉴얼 (kt.com)**

1 기준

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

2 설명

- 클라우드 환경(콘솔 등)에 관리자 권한으로 로그인 시 추가인증 수단을 적용하여야 한다.
  - 예시
    1) 이메일 인증
    2) SMS 인증
    3) 별도 인증도구(OTP, 바이오인증 등) 활용 등

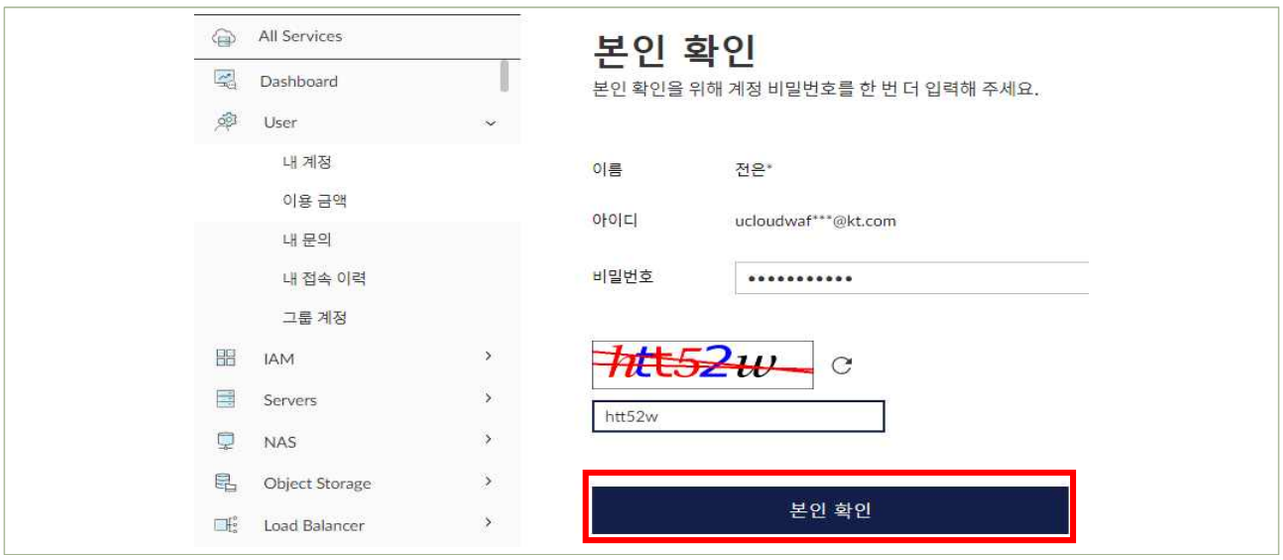
3 우수 사례

콘솔 root 계정(최상위 관리자)의 보안강화를 위해 SMS, 이메일 인증 등 MFA 인증 설정이 가능합니다.

1) 웹 콘솔 접속 후 User 〉 내 계정 〉 본인 확인(비밀번호 재 입력)

콘솔에 루트 계정으로 로그인 상태에서 User 〉 내 계정 메뉴를 클릭하면 **그림1**과 같이 본인 확인 화면이 나타납니다.

본인 확인화면에서는 루트계정 비밀번호와 캡차를 입력 후 하단 본인 확인 버튼을 클릭합니다.



| 그림 3-4-1 | 사용자 본인 재확인

2) User 〉 내 계정 〉 계정 설정

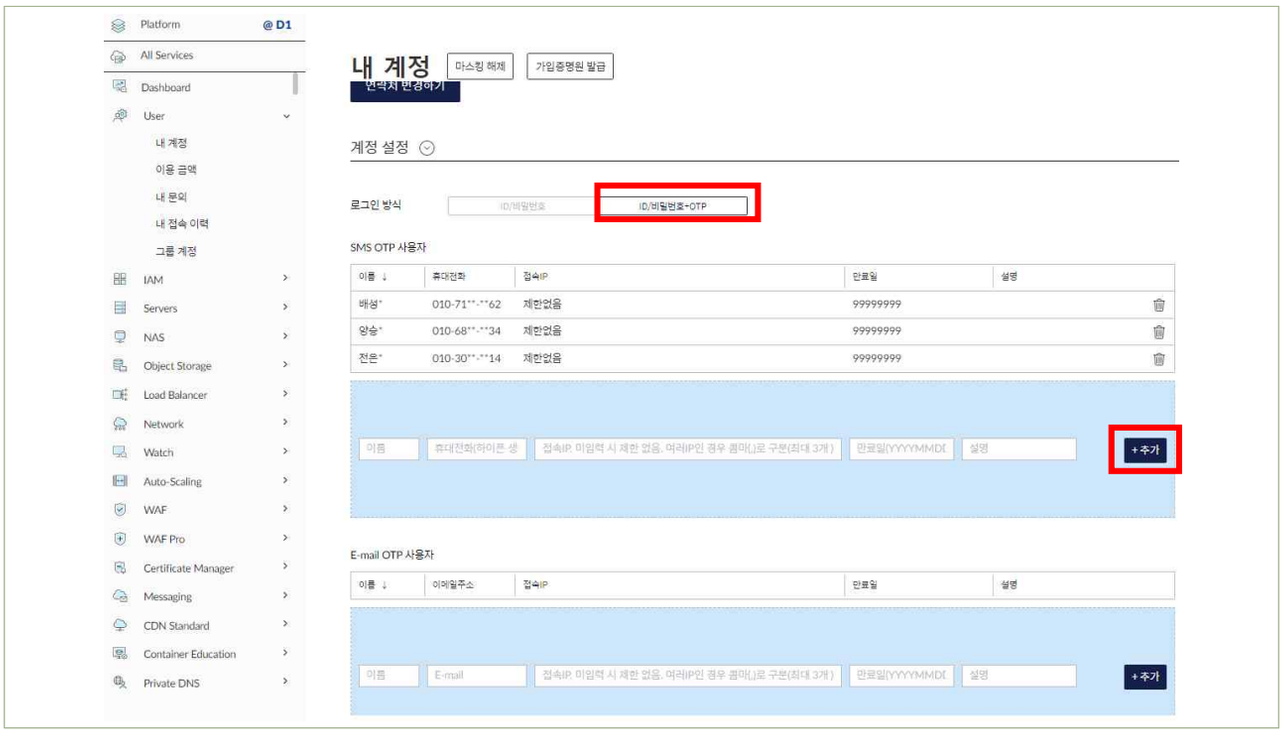
사용자 본인 재확인 후 표시되는 내 계정 화면에서 연락처 정보 하단에 계정 설정 탭을 클릭합니다.

| 그림 3-4-2 | 내 계정 화면에서 계정 설정 탭 선택

3) 계정 설정 〉 로그인 방식 변경 선택(ID/비밀번호 + OTP)

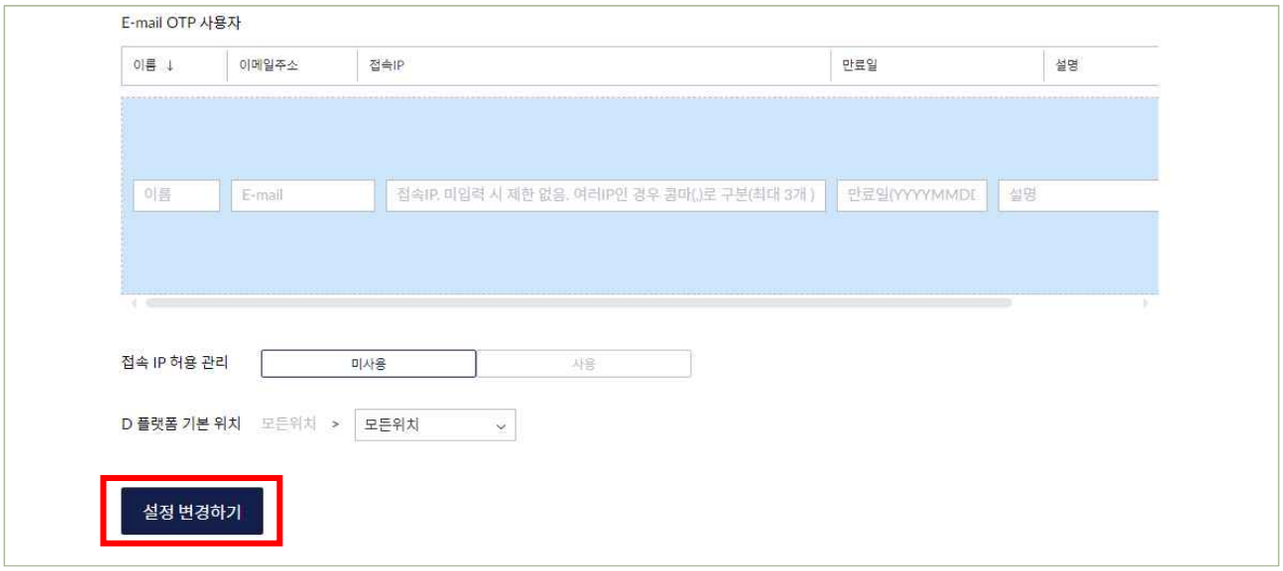
계정 설정 화면 상단 로그인 방식의 ID/비밀번호+OTP 버튼을 선택하면 화면 하단에 SMS 및 Email OTP 설정을 위한 연락처 정보 등록창이 추가로 표시됩니다.

MFA 설정에 필요한 SMS 또는 Email 정보를 입력 후 우측의 추가 버튼을 클릭합니다.



| 그림 3-4-3 | MFA 추가 등록

4) SMS/Email등 MFA 정보 추가 후 내 계정 화면의 최하단에 위치한 설정 변경하기 버튼을 클릭하여 최종 MFA 변경 정보를 저장합니다.



| 그림 3-4-4 | MFA 설정정보 저장

4 참고 사항

- IAM 사용 포탈 매뉴얼 참조 : **Cloud 매뉴얼 (kt.com)**

1 기준

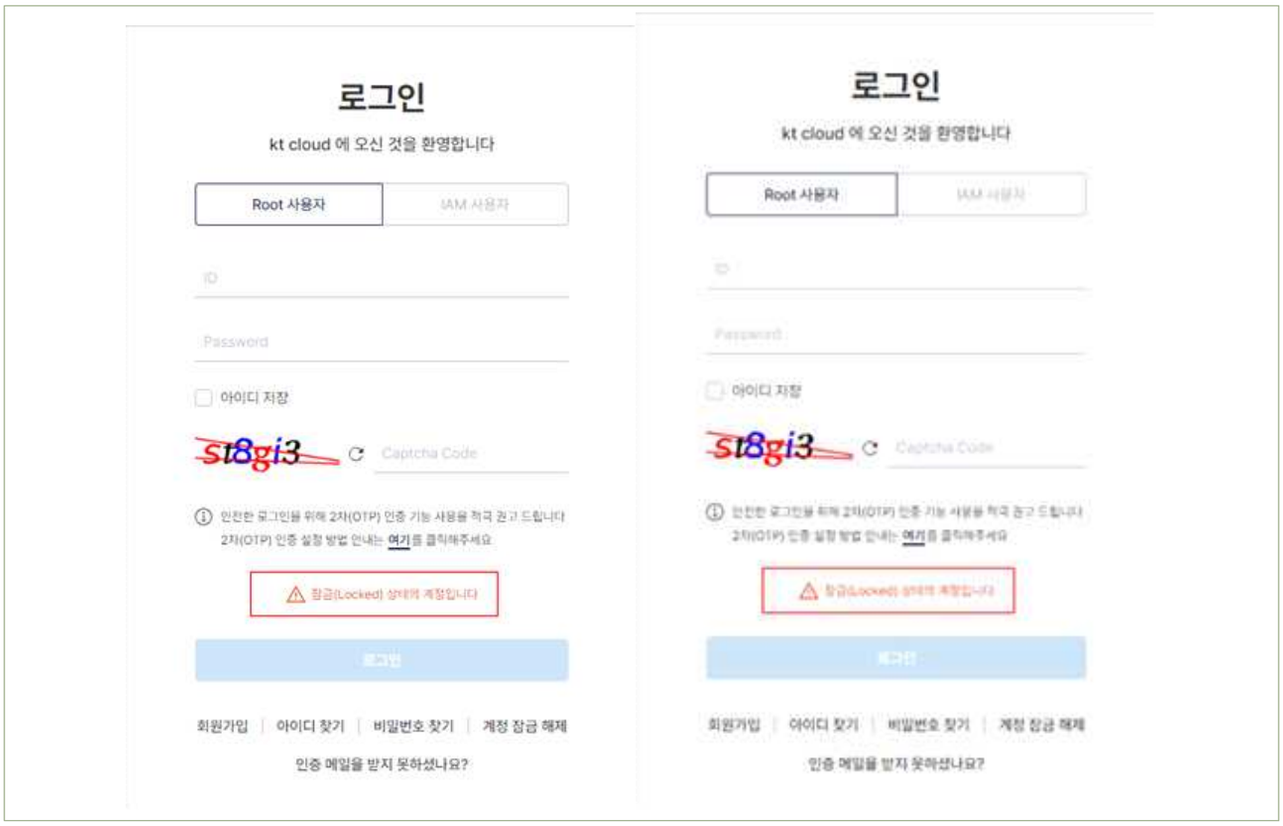
식별번호	기준	내용
3.5.	**클라우드 가상자원 관리 시스템 로그인 규칙 수립**	**클라우드 가상자원 관리시스템 계정에 대한 로그인 규칙(오류횟수 지정 등) 등을 수립하여야 한다**

2 설명

- 클라우드 가상자원 관리시스템 계정에 대한 로그인 규칙을 수립하여야 한다.
  - 예시
    1) 로그인 오류에 따른 보안통제 방안 수립(5회이상 로그인 실패 시 계정 잠김 등)

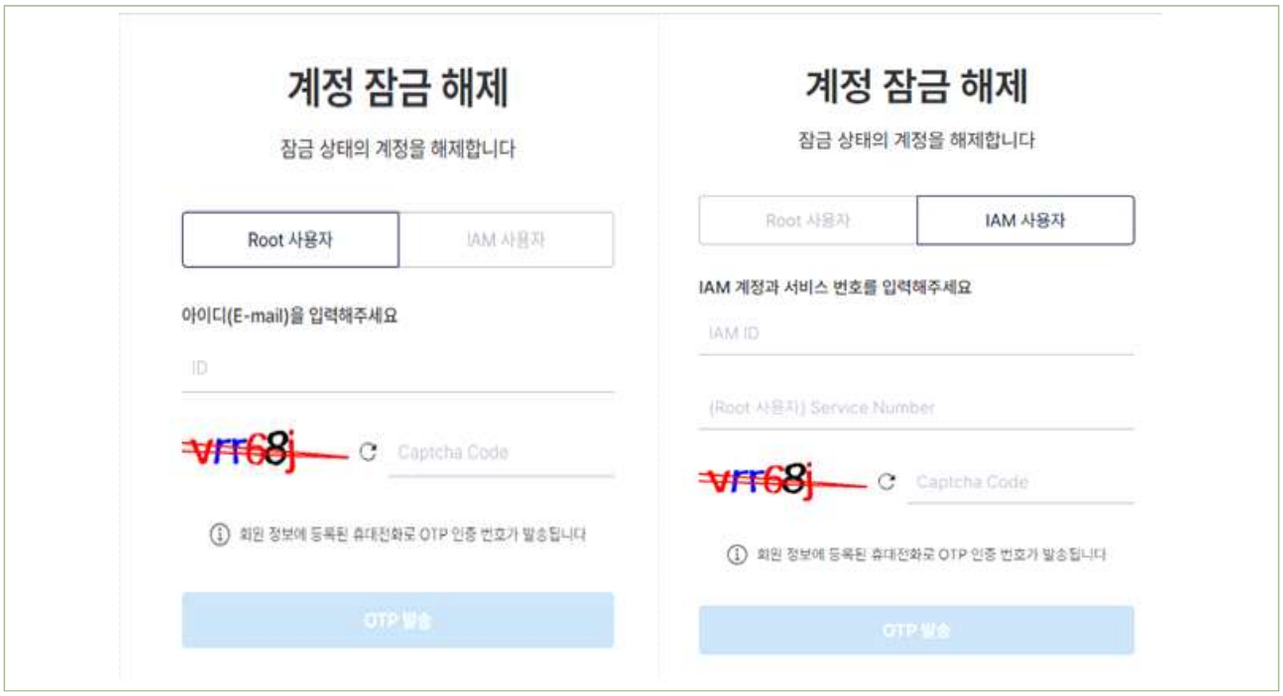
3 우수 사례

콘솔 로그인 시 기본 5회 이상 로그인 실패 시 계정 로그인이 자동 잠금 처리됩니다. 잠금 규칙 설정을 위한 별도 기능은 제공되지 않습니다.



| 그림 3-5-1 | 로그인 실패시 잠금(좌측 root 계정, 우측 IAM 계정)

5회 이상 실패로 계정 로그인이 잠금 처리된 경우 콘솔 로그인 화면에서 OTP인증을 통해 계정 잠금 해제가 가능합니다.



| 그림 3-5-2 | 계정잠금 해제 화면(좌측 root 계정, 우측 IAM 계정)

4 참고 사항

- IAM 사용 포탈 매뉴얼 참조 : **Cloud 매뉴얼 (kt.com)**

1 기준

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

2 설명

- 클라우드 가상자원 관리시스템 접근 가능한 계정 생성 시 안전한 비밀번호 규칙을 수립하여 적용하여야 한다.
  - 예시
    1) 비밀번호는 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설정
    2) 분기별 1회 이상 변경
    3) 가상자원마다 관리자(root, administrator) 계정은 비밀번호를 다르게 설정

3 우수 사례

패스워드는 유추하기 어려운 조합으로 하며 이름, 전화번호 등 개인정보를 포함하지 않을 것을 권장합니다.

패스워드는 숫자, 영문자, 특수문자를 조합하여 생성해야 하며, 콘솔계정의 패스워드 등록 규칙은 다음과 같습니다.

- 영문 대/소문자, 숫자, 특수문자 조합한 8~15자
- 콘솔 패스워드 설정 시 위 기준을 준수해야 패스워드 등록/변경이 가능합니다.

콘솔 계정의 패스워드는 90일 주기로 정기적인 변경을 권장합니다.

| 그림 3-6-1 | 계정 비밀번호 사용 규칙

4 참고 사항

- IAM 사용 포탈 매뉴얼 참조 : **Cloud 매뉴얼 (kt.com)**

1 기준

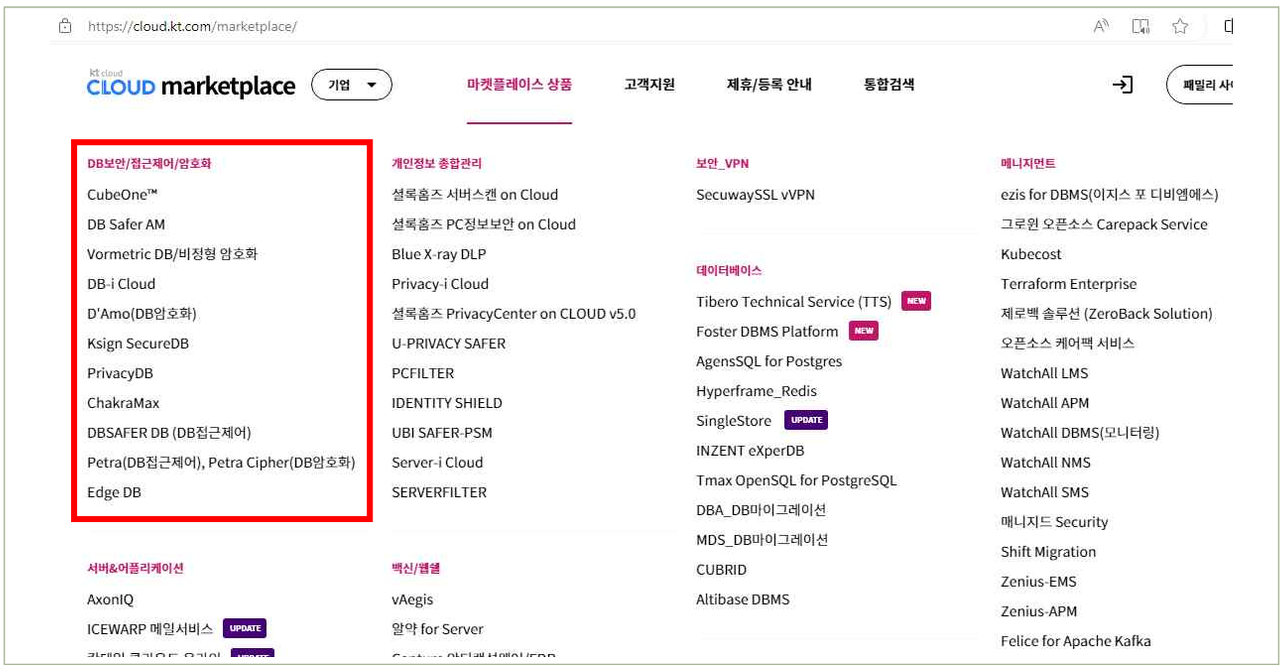
식별번호	기준	내용
3.7.	**공개용 웹서버 접근 계정 제한**	**클라우드를 통해 공개용 웹서버를 운영하는 경우 접근 계정을 적절하게 제한하여야 한다.**

2 설명

- 클라우드 환경을 통해 공개용 웹서버를 운영하는 경우 접근 계정을 적절하게 제한하여야 한다.
  - 예시
    1) 계정 관리 기능을 통해 공개용 웹서버만 접근 가능한 계정을 개인별 부여하여 관리
    2) 공개용 웹서버에 접근 가능한 계정으로 로그인 시 추가인증 수단 적용 등

3 우수 사례

서버 접근계정의 제한 및 서버 접속 시 OTP등 2차 인증은 별도의 접근제어 솔루션을 통해 지원됩니다. 접근제어 솔루션은 kt cloud 마켓플레이스 내 DB보안/접근제어/암호화 카테고리 솔루션을 참고해 주시기 바랍니다.



4 참고 사항

- 마켓플레이스 링크 : https://cloud.kt.com/marketplace/

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. 암호화 호출 권한 관리
4.5. 안전한 암호화 알고리즘 적용

4 암호키 관리

1 기준

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

2 설명

- 관련 법령(전자금융거래법, 개인정보보호법, 신용정보법 등)에 따라 암호화가 필요한 대상이 저장 및 처리되는 가상자원에 대해서는 암호화를 적용을 고려하여야 한다.

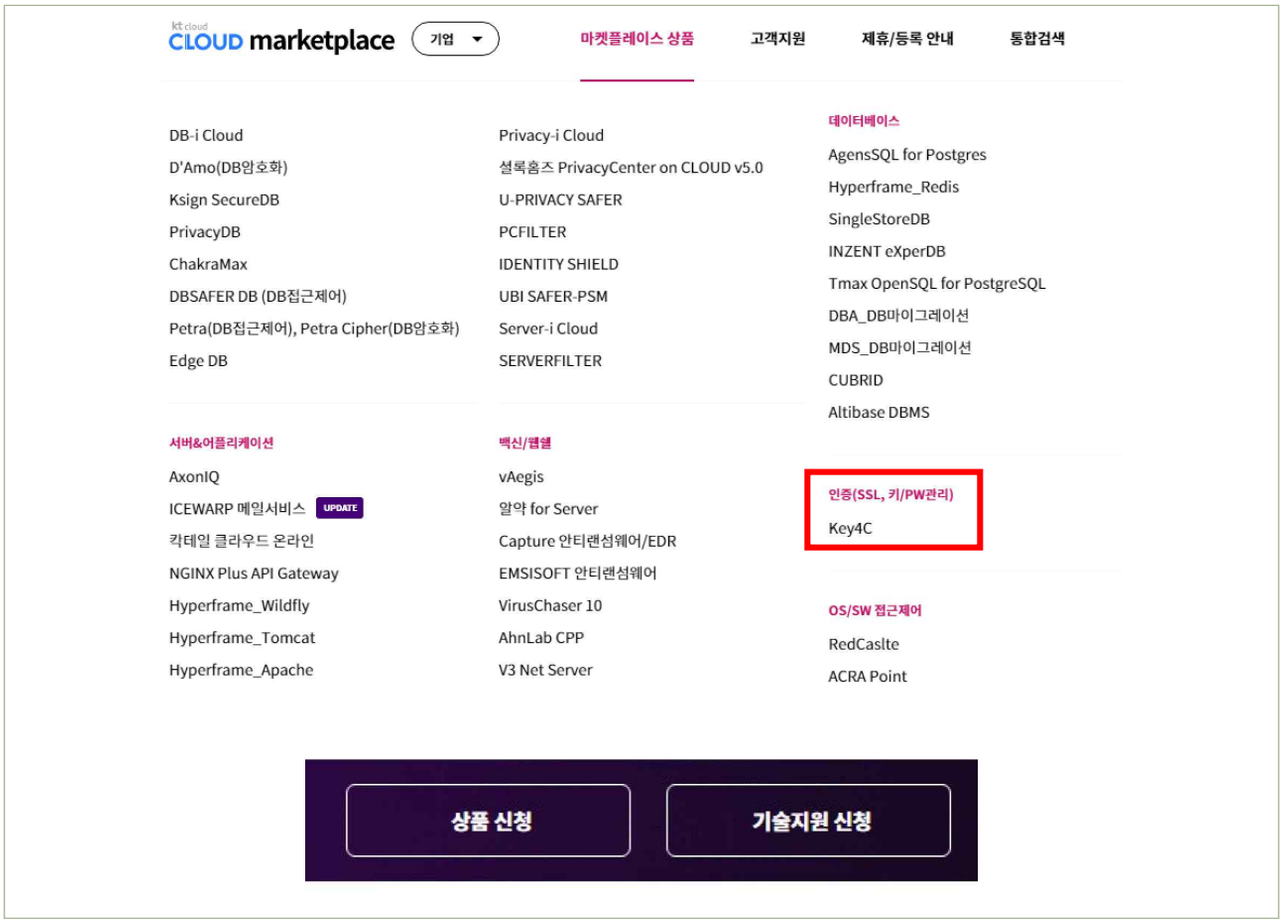
  - 예시

    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

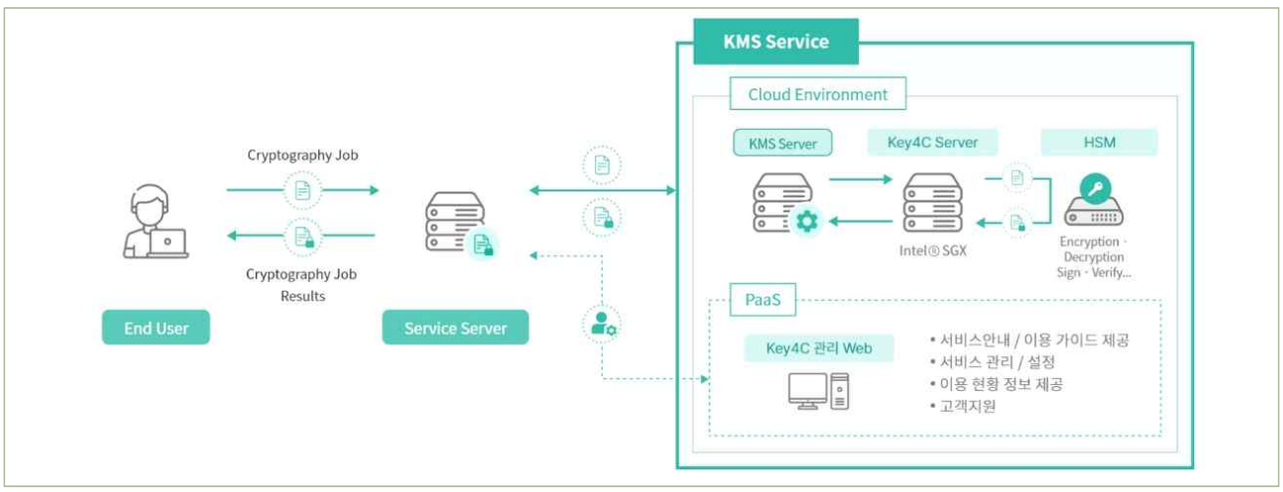
3 우수 사례

암호화 키의 생성 및 안전한 보관/관리를 위해 Cloud 기반의 HSM 또는 KMS 솔루션을 활용할 수 있으며, kt cloud 마켓플레이스에 등록된 관련 솔루션을 활용할 수 있습니다.

1) 마켓플레이스 접속(https://cloud.kt.com/marketplace)
2) 관련 솔루션 신청

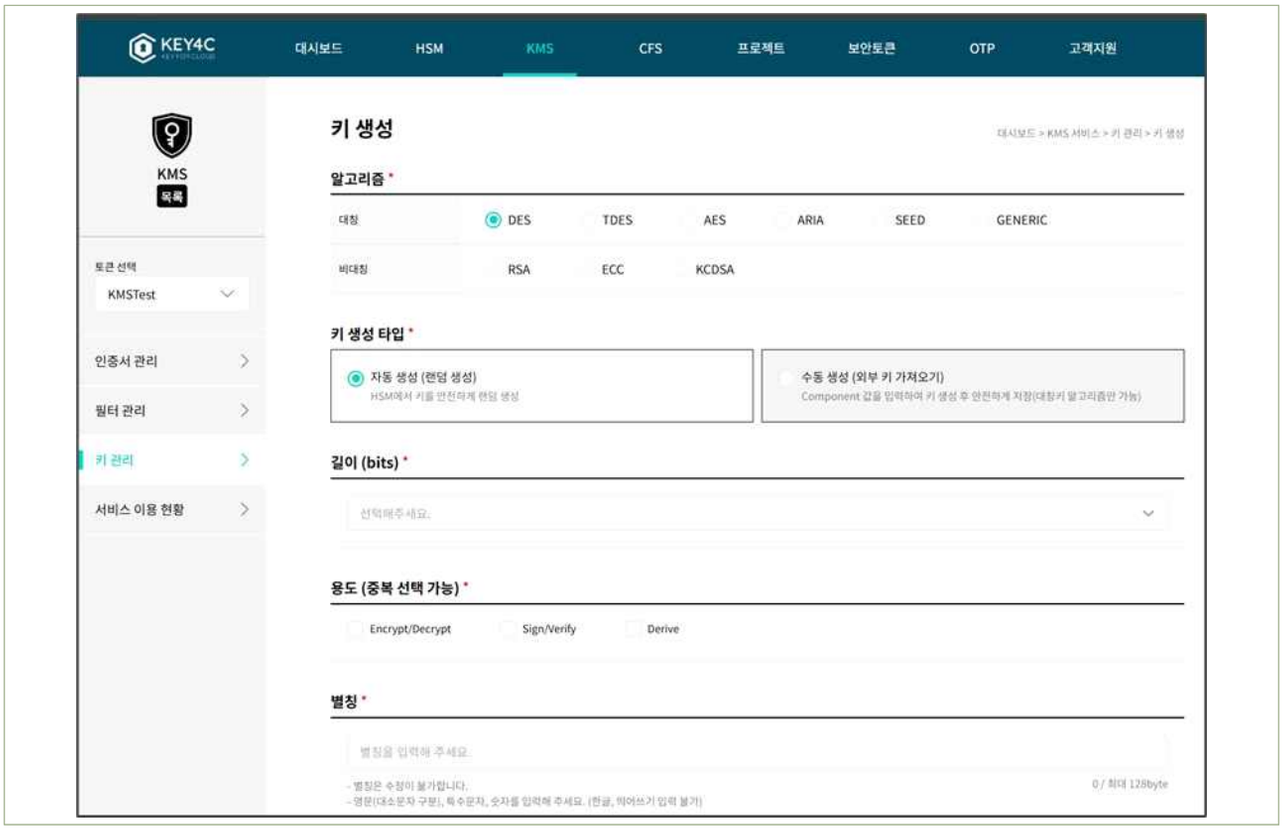


| 그림 4-1-1 | 마켓플레이스 키관리 솔루션 예시



| 그림 4-1-2 | KMS 서비스 개요

암호화를 위한 키 생성은 KMS (Key4C 예시)에서 가능하며, 키를 신규 생성하거나 또는 기존의 이용자 별도 관리중인 키를 가져와서 KMS에 저장 및 관리하는 방식도 가능합니다. KMS는 별도의 콘솔화면이 제공되며 해당 콘솔에서 암호화 키의 생성 및 관리가 가능합니다(그림3 참조).



| 그림 4-1-3 | KMS 키 생성 화면

4 참고 사항

- (참조) 마켓플레이스 관련 상품 링크 : 마켓플레이스 (kt.com)
- (참조) KMS(Key4C) 콘솔(대시보드) 접속 링크 : https://key4c1.cloudhsm.kr/console/login

1 기준

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

2 설명

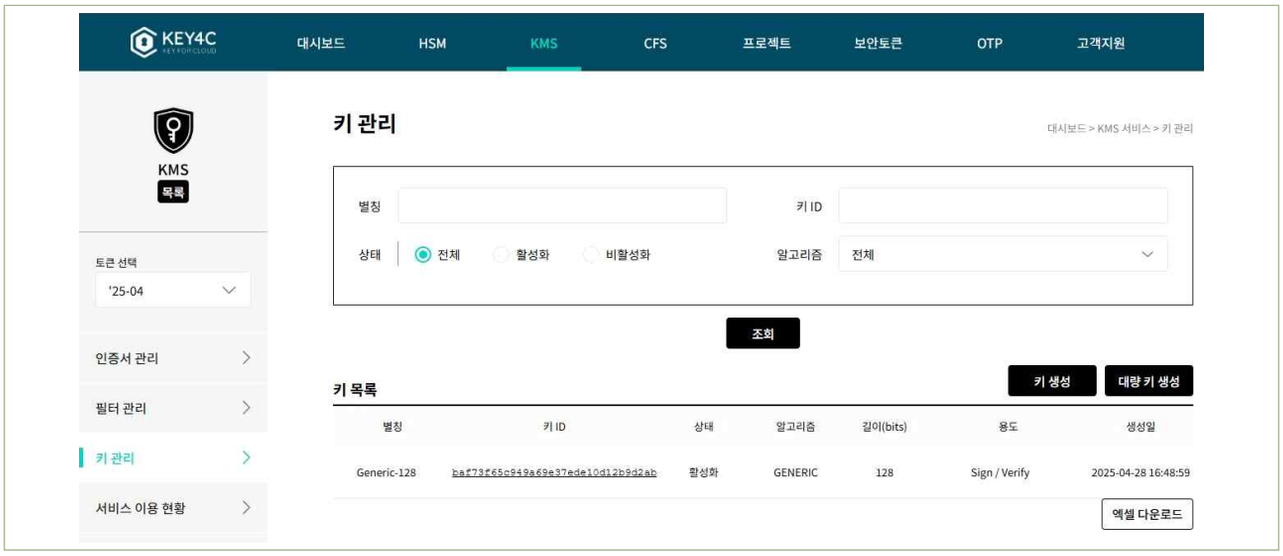
- 암호화 기능 이용 시 암호키 관리 방안을 수립하여야 한다.
  - 예시
    1) KMS(Key Management Service)를 통한 암호화 키 방안 수립(생성, 변경, 폐기 등)
    2) 클라우드 서비스 제공자가 직접 제공하는 암호화키 이용 시 적절한 관리방안 수립
    3) 키 사용기간 수립 및 암호키 유출등에 대응할 수 있도록 키 삭제 및 재적용 관련 기능 수립
    4) 생성된 암호화키를 안전하게 보관할 수 있는 방안 수립 등

3 우수 사례

안전한 암호화 키의 관리를 위해 Cloud KMS 솔루션(Key4C 예시)을 통해 암호화 키의 생성, 폐기 등 일련의 관리를 진행할 수 있습니다.

키의 생성은 Key4C 콘솔(대시보드)에서 UI 기반 생성/폐기를 수행하거나 Key4C서버와 연동을 통하여 키 관리를 동일하게 진행할 수 있습니다.

KMS 웹 콘솔화면에서 생성된 키의 내역을 확인하고 관리할 수 있습니다. KMS 웹 콘솔화면 접속을 위해서는 별도의 사전 계정등록 절차가 필요합니다.

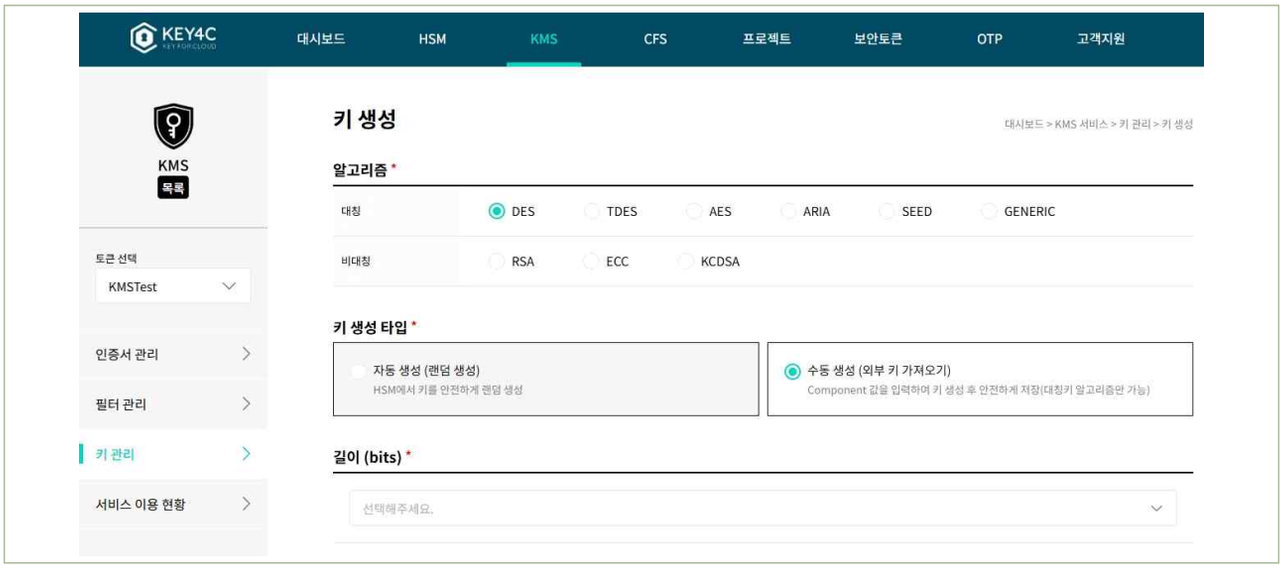


| 그림 4-2-1 | KMS 키 관리 화면

① 암호화 키 생성

KMS 웹 콘솔을 통한 키 생성절차는 아래와 같습니다.

- 솔루션 (Key4c 예시) 콘솔 접속 〉 KMS 서비스 〉 키관리 메뉴에서 암호화 키 생성 및 생성결과 확인



| 그림 4-2-2 | KMS 키 생성 화면

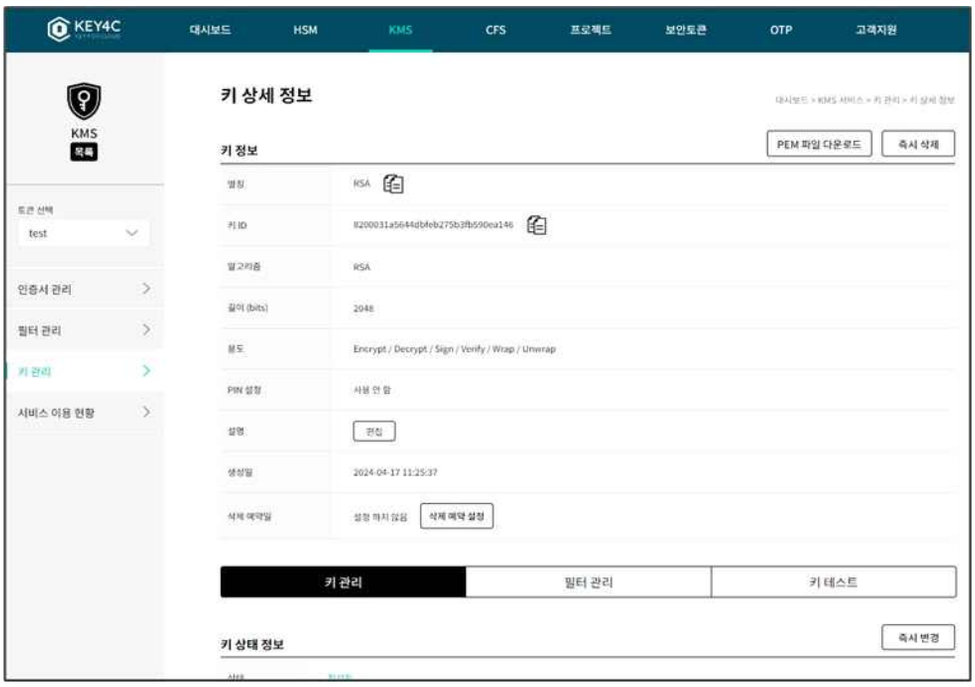
② 암호화 키 삭제/비활성화

암호키의 유출 등에 대비하여 사용중인 암호화 키의 삭제/비활성화 하거나 예약삭제 등록을 통해 엄호키의 사용기간 설정이 가능합니다.

1) 암호키 즉시 삭제

KMS 콘솔 웹 접속 〉 KMS 서비스 〉 키 관리 〉 키 상세정보 화면

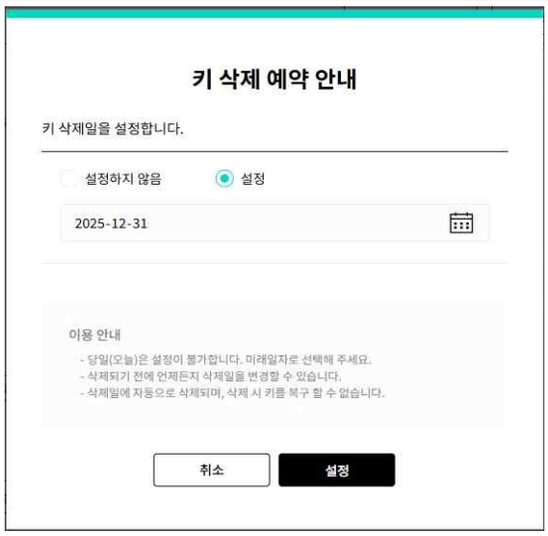
키관리 화면에서 관리 대상 키를 선택 후 상단 우측 즉시삭제 버튼을 이용해 즉각적인 암호키의 삭제 처리가 가능합니다.



| 그림 4-2-3 | KMS 키 상세정보 화면(키 삭제)

2) 암호키 삭제 예약

키 상세화면 하단 삭제 예약 버튼을 통해 일정 기간 이후 키가 삭제되도록 예약처리가 가능합니다. 암호키의 삭제 예약 이후 원복을 위해서는 예약취소가 가능합니다.



| 그림 4-2-4 | 키 삭제예약

3) 암호키 교체

키 상세화면 하단에서 즉시교체 버튼을 클릭시 기존에 발급한 키를 교체할 수 있습니다.

| 그림 4-2-5 | KMS 키 상세화면(키 변경)

4 참고 사항

- (참조) 마켓플레이스 관련 상품 링크 : 마켓플레이스 (kt.com)

1 기준

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

2 설명

- 클라우드 환경 내 암호키 관리 서비스(ex. KMS) 이용 시 암호키 서비스 관리자 권한을 적절하게 통제하여야 한다.
  - 예시
    1) 암호키 관리 서비스 관리자 권한은 최소인원에게 부여하고 부여현황에 대해 상시모니터링 수행
    2) 사용자가 생성하는 각 키에 대해서는 관리자를 별도 지정할 수 있어야 하며, 각 조건에 따라 최소한의 권한 부여 등

3 우수 사례

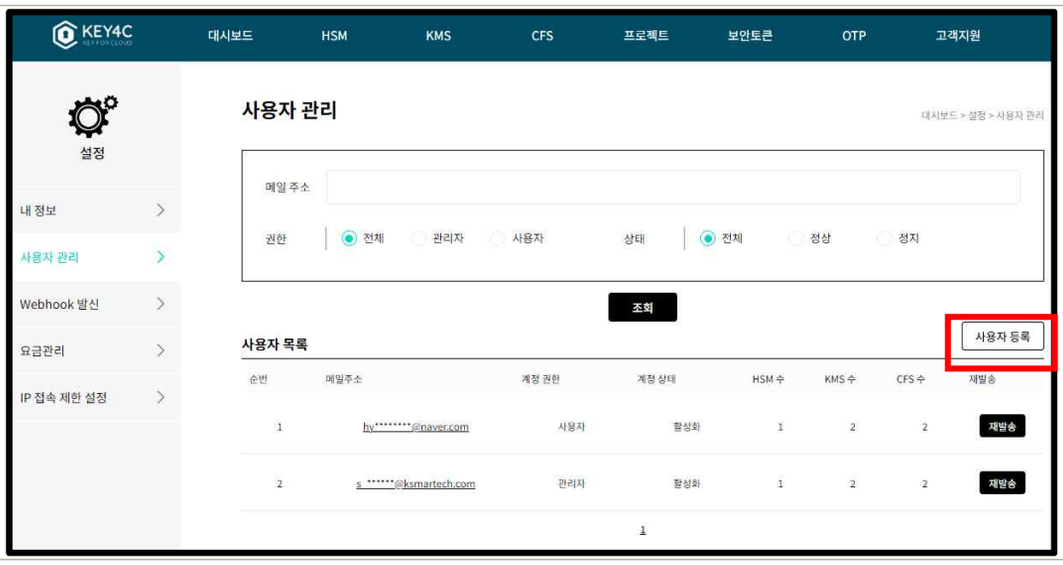
Cloud KMS 솔루션의 사용자 계정 관리 기능을 통해 최소한의 담당자만 키를 생성하는 등의 권한 관리가 가능합니다(Key4C 사례). 사용자 계정은 관리자, 사용자로 권한을 제어할 수 있습니다.
또한, 사용자 계정의 비활성화나 서비스 권한을 변경하여 암호키 접근에 대한 통제가 가능합니다.

- 관리자 권한은 사용자 관리를 통해 새로운 계정을 생성할 수 있습니다.
- 관리자 권한은 KMS를 사용하기 위한 토큰 생성 권한을 갖으며, 토큰 생성 후 키 생성을 할 수 있습니다.
- 관리자 권한은 필터 관리를 통해 암호화 키를 호출하는 서버 및 클라이언트를 제어할 수 있습니다.
- 사용자 권한은 생성된 토큰 내에서 원하는 키를 생성, 삭제하고 모니터링 할 수 있습니다
- 새로운 계정 등록 시, 사용하고 있는 서비스들의 관리 권한을 제어할 수 있습니다.

KMS 사용자 관리 기능을 통해 관리자 및 사용자 신규 생성이 가능합니다.

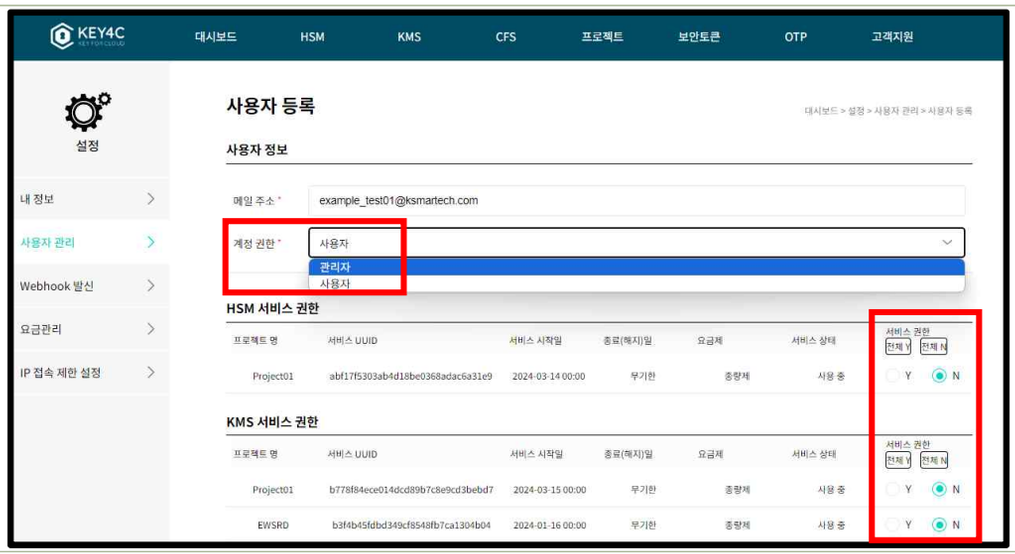
- 솔루션 웹 콘솔 접속 〉 설정 〉 사용자 관리 화면에서 기존에 생성된 사용자의 확인 및 관리가 가능합니다.

- 사용자 관리화면 우측의 사용자 등록 버튼 클릭을 통해 사용자 추가가 가능합니다.



| 그림 4-3-1 | KMS 사용자 관리

- 사용자 등록 화면에서 사용자 유형(관리자/사용자) 및 서비스 권한 선택 후 사용자 생성이 가능합니다.



| 그림 4-3-2 | 사용자 등록 화면

4 참고 사항

- (참조) 마켓플레이스 관련 상품 링크 : 마켓플레이스 (kt.com)

1 기준

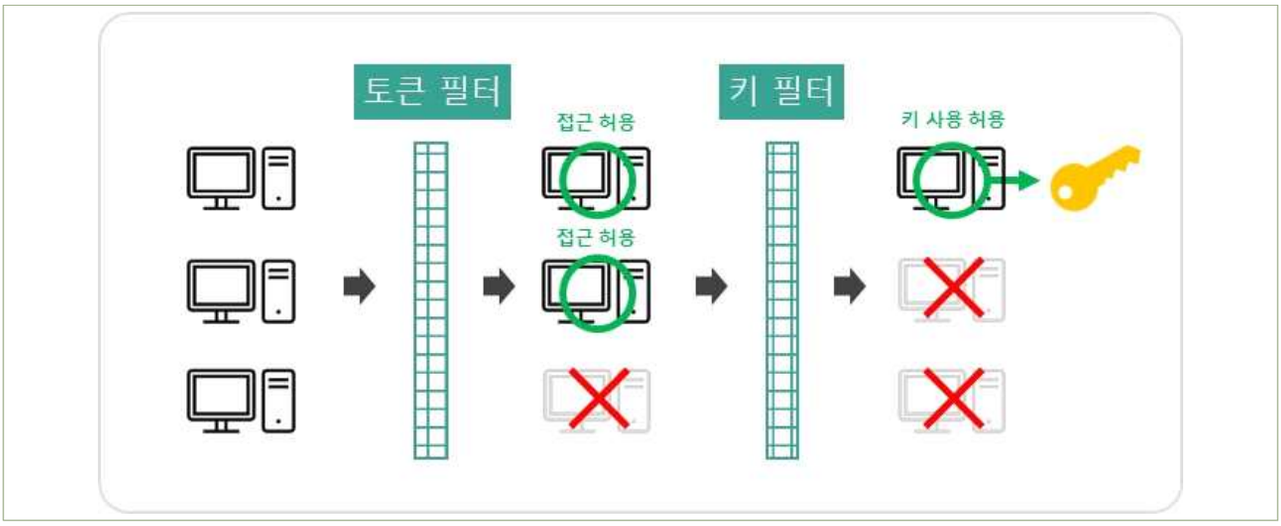
식별번호	기준	내용
4.4.	암호키 호출 권한 관리	클라우드 암호키 호출 권한을 관리하여야 한다.

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

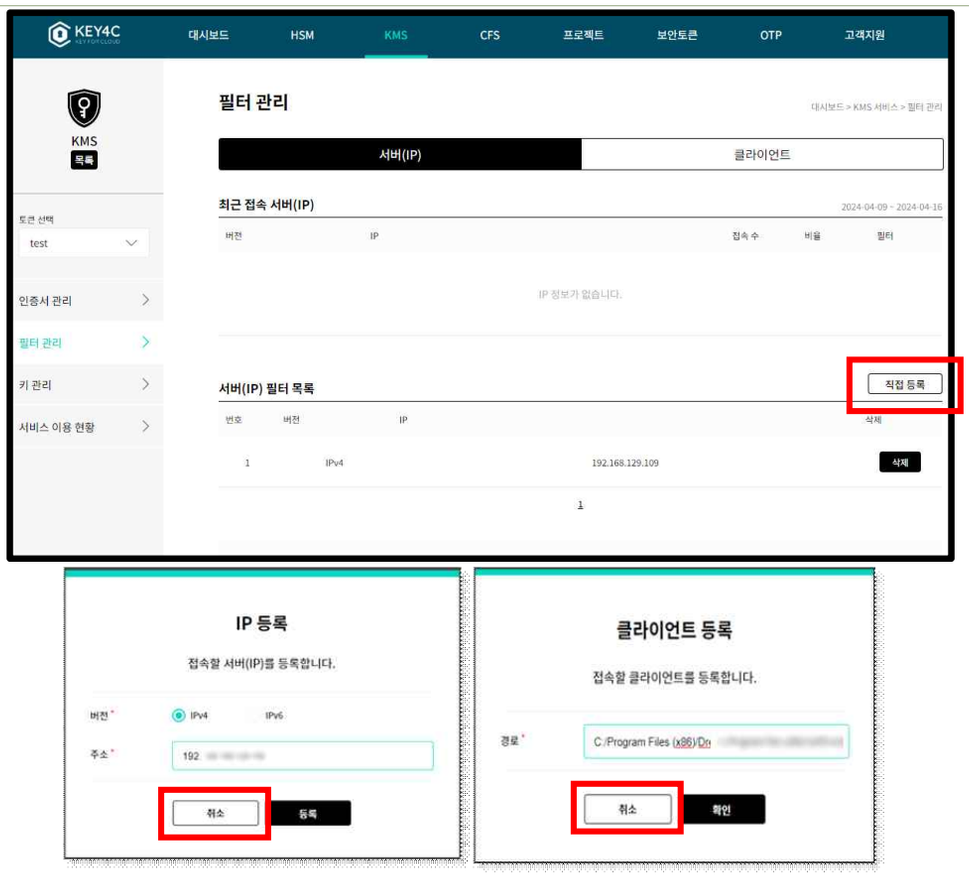
Cloud KMS 솔루션에서는 암호화 키는 접근 가능한 서버/클라이언트에서만 접근 가능하도록 필터 관리를 적용하고 있습니다. 따라서, 암호화키 호출 시 목적에 따라 접근하는 서버/클라이언트를 지정할 수 있습니다(접속을 허용하는 서버, 클라이언트에서만 키를 호출하여 사용 가능)



| 그림 4-4-1 | KMS 필터(접근제한) 개념

KMS 필터관리 메뉴에서 접근 가능한 서버IP 또는 클라이언트의 등록을 통한 접근제한 설정이 가능합니다. (관리자만 가능, 사용자 권한 불가)

- KMS 웹 콘솔 접속 〉 KMS 서비스 〉 필터 관리 화면
- 상단 서버(IP) 탭 또는 클라이언트 탭 선택 후 하단 서버 등록 버튼 클릭
- 서버IP 또는 클라이언트 등록 후 확인 버튼 클릭

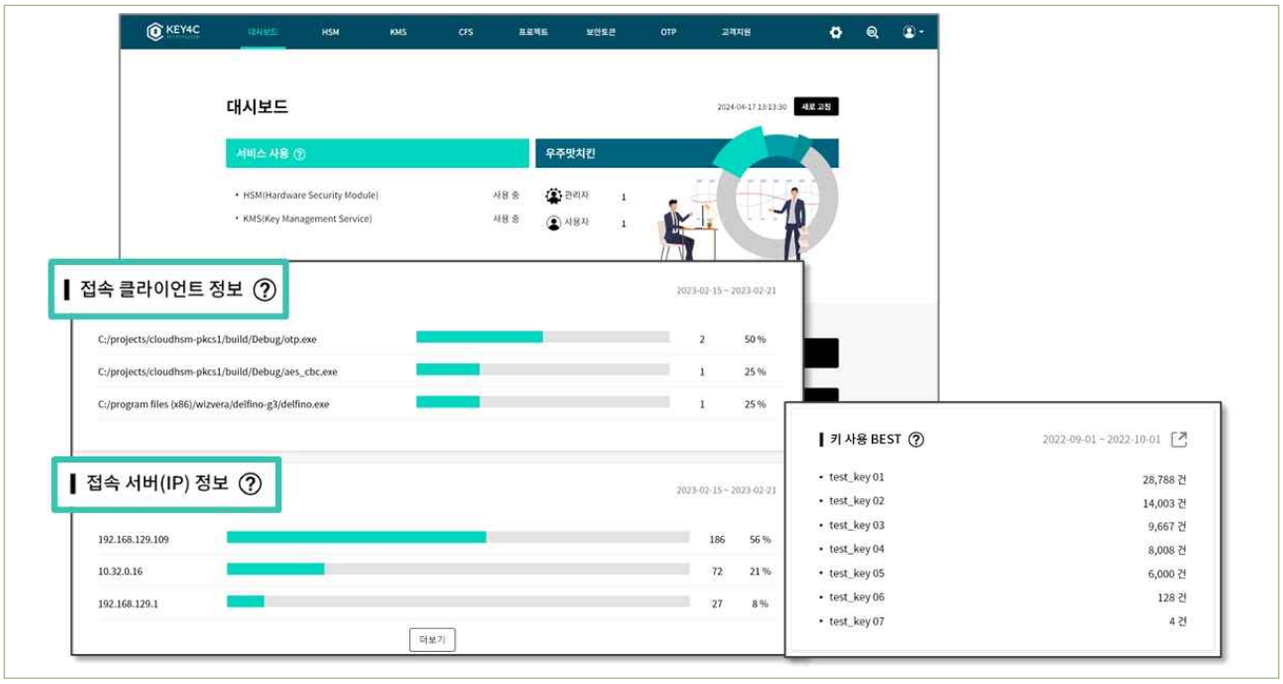


| 그림 4-4-2 | KMS 필터관리 화면

KMS에서는 대시보드 화면을 통해 생성된 키의 접속현황 등 전체적인 이용현황에 대한 모니터링이 가능합니다.

솔루션 콘솔내 대시보드 화면을 통해 암호키 호출 현황에 대해 모니터링 가능

- KMS 콘솔 〉 KMS 서비스 〉 서비스 이용 현황 메뉴 선택



| 그림 4-4-3 | KMS 대시보드 및 모니터링 화면

4 참고 사항

- (참조) 마켓플레이스 관련 상품 링크 : 마켓플레이스 (kt.com)

1 기준

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

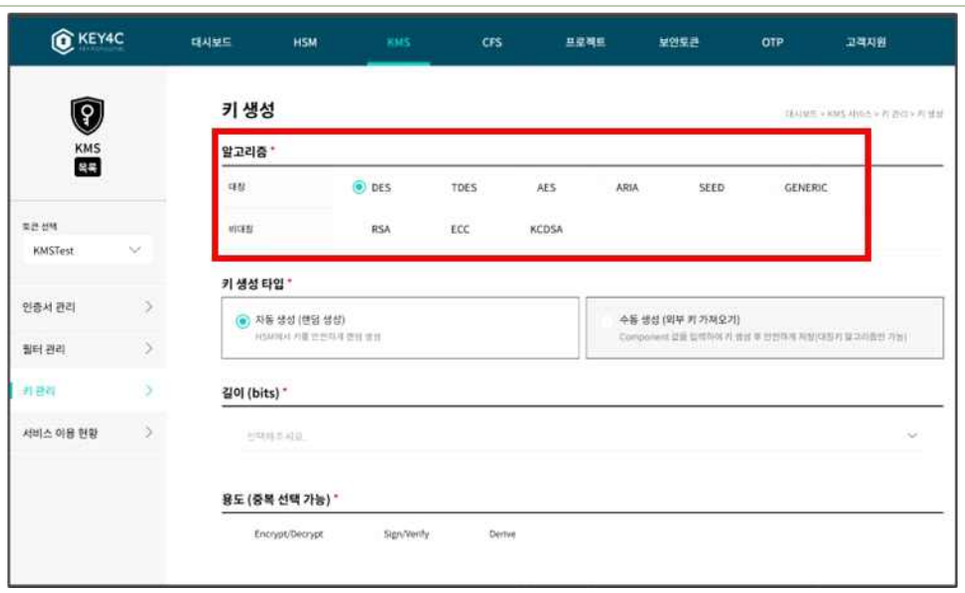
2 설명

- 암호화 기능 이용 시 안전한 암호화 알고리즘을 적용하여야 한다(또는 확인하여야 한다.).
  - 예시
    1) 이용자가 관리하는 암호키로 암호화 기능 적용 시 안전한 암호화 알고리즘 적용(금융부문 암호기술 활용 가이드 등 참고)
    2) 클라우드 KMS 서비스를 통해 암호화 시 안전한 암호화 알고리즘을 제공하는지 확인

3 우수 사례

Cloud KMS 솔루션에서는 암호화 키 생성시 대칭키 알고리즘, 비대칭키 알고리즘을 지원합니다.

- 대칭키 알고리즘 : DES, TDES, AES, ARIA, SEED, GENERIC
- 비대칭키 알고리즘 : RSA. ECC, KCDSA 지원 (EDWARDS는 HSM 서비스 경우에만 지원)



| 그림 4-5-1 | KMS 키 생성시 알고리즘 선택

4 참고 사항

- (참조) 마켓플레이스 관련 상품 링크 : 마켓플레이스 (kt.com)

5. 로깅 및 모니터링 관리

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

5 로깅 및 모니터링 관리

1 기준

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

2 설명

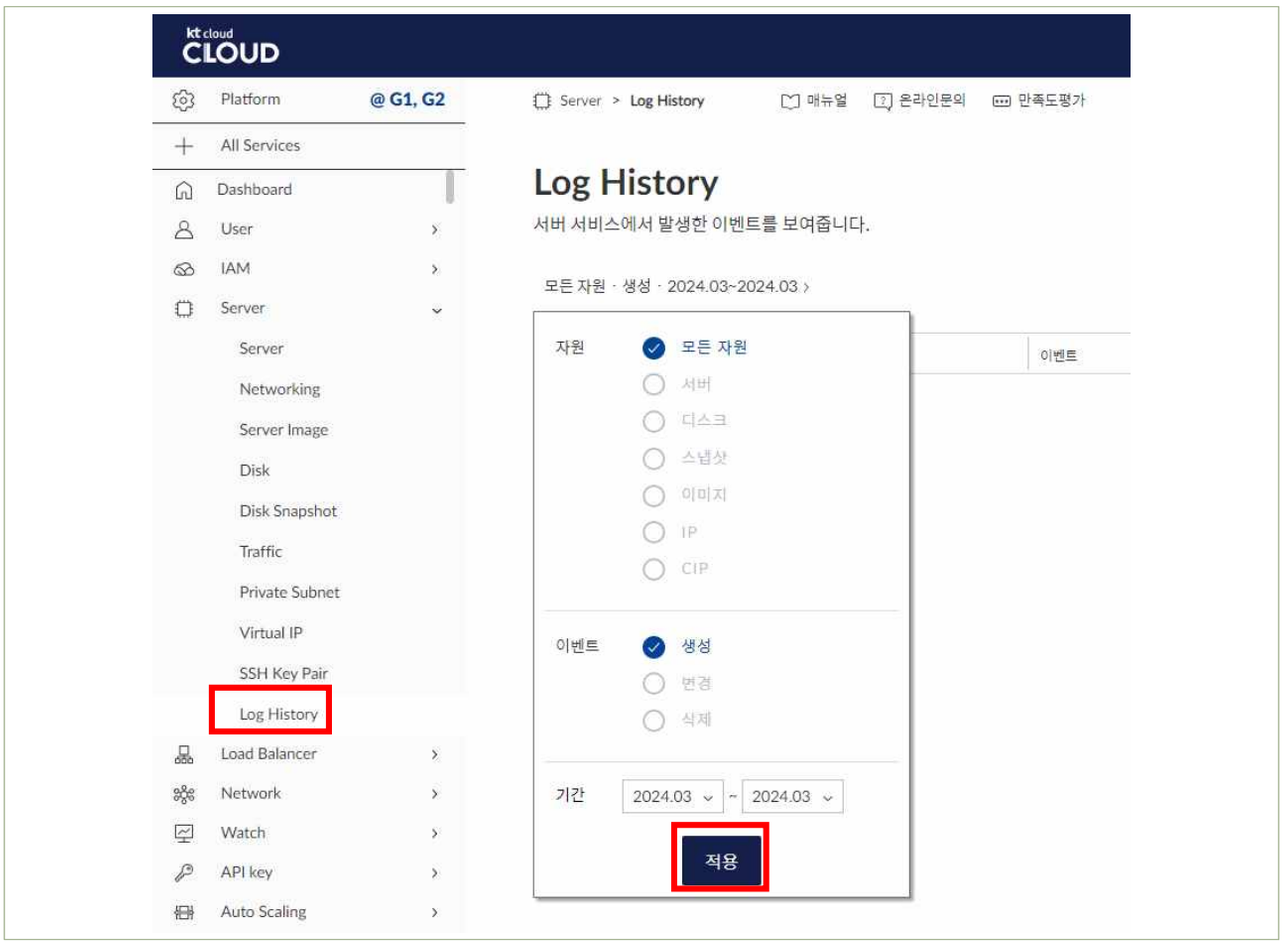
- 이용자의 가상자원 이용 관련 일련의 행위에 대한 추적성을 확보할 수 있는 방안이 마련되어야 한다.
  - 행위 감사로그
    1) 가상자원 변경 사항에 관한 행위(생성, 변경, 삭제 등)
    2) 가상자원에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근기록
    3) 가상자원을 사용한 일시, 사용자 및 가상자원의 형태(서버, 데이터베이스, 스토리지 등)를 확인할 수 있는 접근 기록
    4) 가상자원내 전산자료의 처리 내용을 확인할 수 있는 사용자 로그인, 액세스 로그 등 접근 기록

3 우수 사례

가상자원의 생성, 변경이나 디스크, 서버 이미지, 방화벽 정책 관리 등 Cloud 주요 자원에 대한 로그 조회는 Log History 서비스를 통해 제공됩니다.

(G플랫폼) 서버, 디스크, 디스크 스냅샷, 이미지, IP, CIP(Customer IP) 가상자원에 관련된 생성, 변경 삭제 이벤트 이력을 조회할 수 있습니다.

1) 웹 콘솔 접속 후 Servers 〉 Log History 〉 로그 범위 설정



| 그림 5-1-1 | G플랫폼 로그 검색조건 설정

2) 로그 조회

예시처럼 검색 조건에 따라 전체 주요 자원에 대한 생성이력이 조회됩니다.

Log History

서버 서비스에서 발생한 이벤트를 보여줍니다.

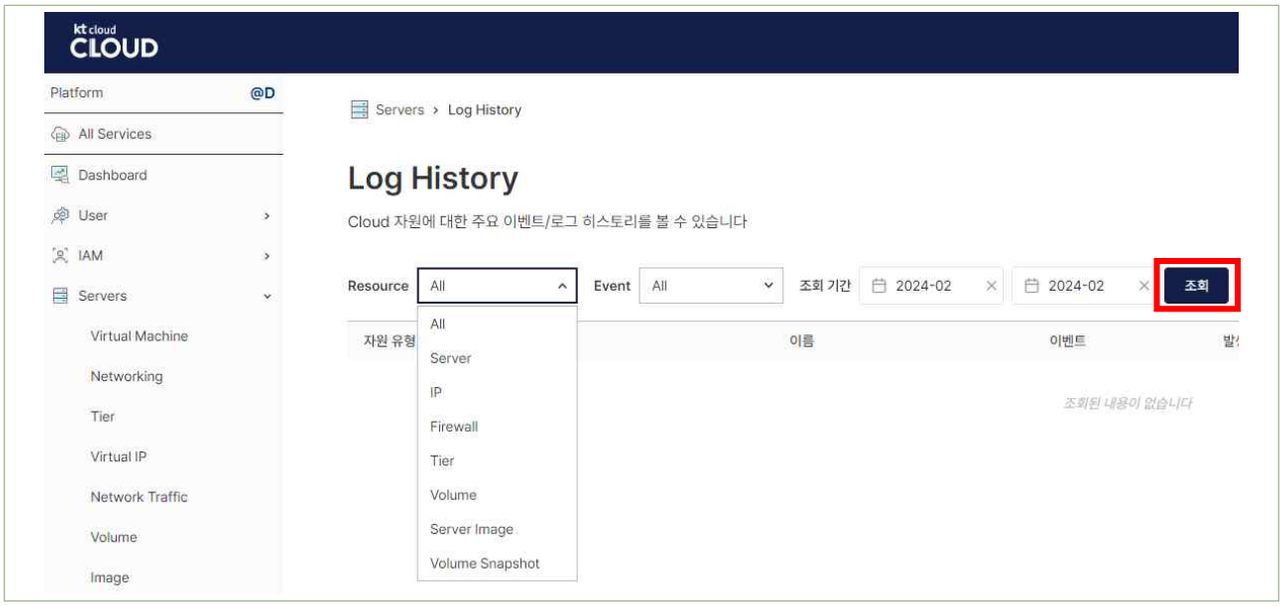
모든 자원 · 생성 · 2024.01~2024.03

자원	이름	이벤트	일시	비고
cip	CHUB1	생성	2024-01-30 13:29:29	1.1.1.0/24
cip	TCIP	생성	2024-02-14 16:39:20	10.17.1.192/27
disk	ssdprovisionedtest	생성	2024-01-16 16:26:56	100GB
server	server-g2	생성	2024-02-08 10:41:28	Centos 7.9 64bit / 2vcore 4GB
server	ytestobj	생성	2024-02-15 09:35:32	Ubuntu 20.04 64bit / 2vCore 4GB
snapshot	testsnapshotkk	생성	2024-01-25 15:27:44	DataDiskAttachTest

| 그림 5-1-2 | 로그 조회 결과

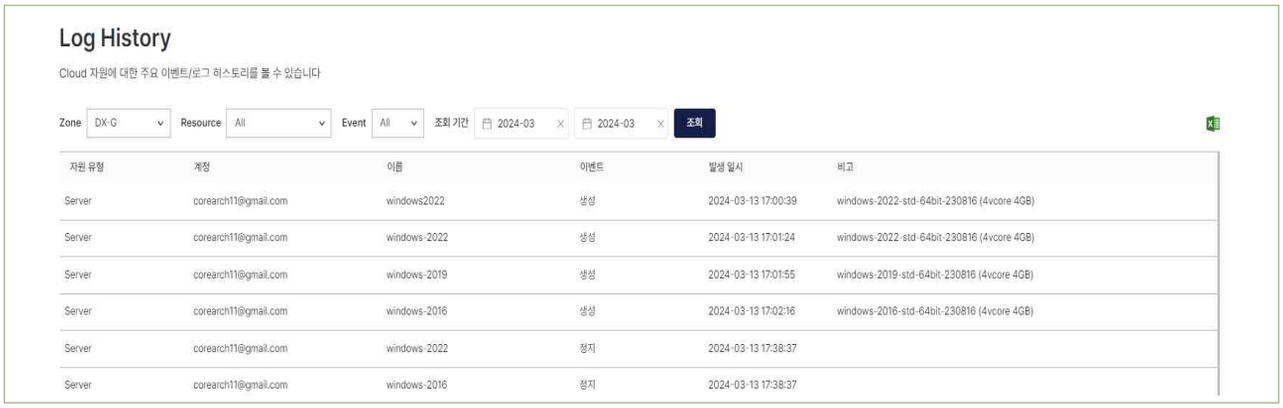
(D플랫폼) 서버, 볼륨, 볼륨 스냅샷, 이미지, Tier, IP, 방화벽 가상자원에 관련된 생성, 변경, 삭제 이벤트 이력을 조회할 수 있습니다.

1) 웹 콘솔 접속 후 Servers 〉 Log History 〉 로그 범위 설정



| 그림 5-1-3 | D플랫폼 로그 조회 화면

2) 로그 조회



| 그림 5-1-4 | 로그 조회 결과

4 참고 사항

- (참조) Watch 매뉴얼 참조 : Cloud 매뉴얼 (kt.com)

1 기준

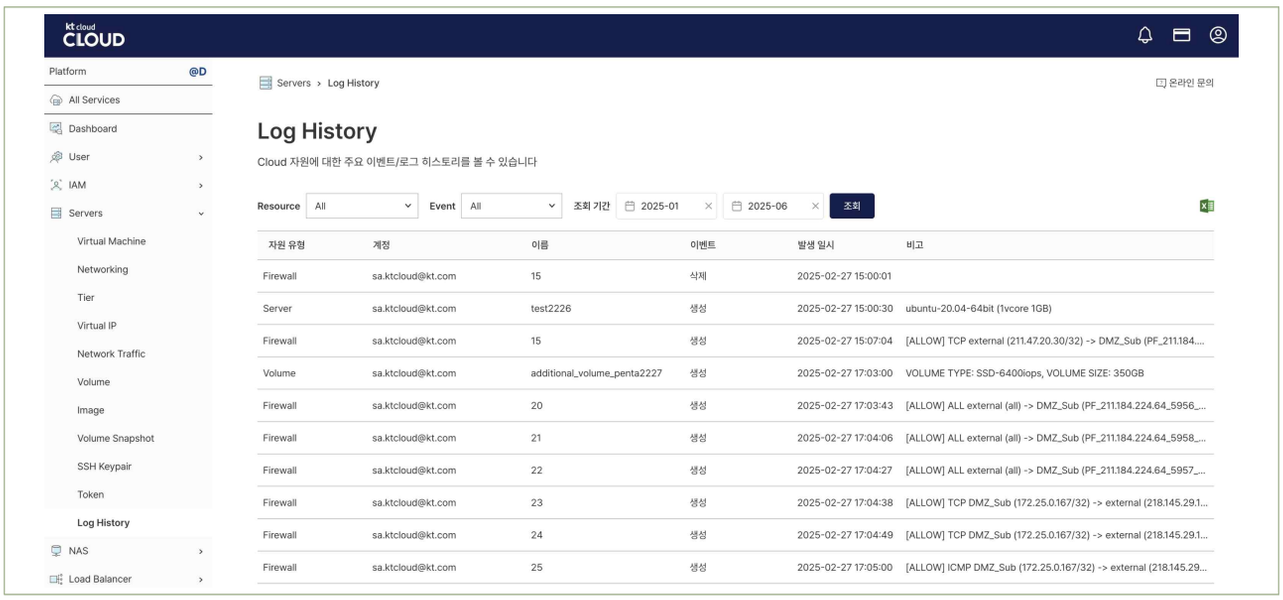
식별번호	기준	내용
5.2.	**가상자원 이용 행위추적성 증적 모니터링**	**가상자원 이용에 관한 행위추적성 증적에 대해 모니터링 및 주기적 검토를 수행하여야 한다.**

2 설명

- 클라우드 가상자원 이용에 관한 행위추적성 증적에 대해상시 모니터링 및 주기적 검토를 수행하여야 한다.
  - 예시
    1) 클라우드 가상자원 이용에 관한 행위추적성 증적(ex. 감사로그 등)에 대한 상시 모니터링 수행
    2) 전자금융감독규정 및 금융회사 내부규정등에 수립된 검토 기간에 맞추어 클라우드 가상자원 이용에 관한 행위추적성 증적에 대한 주기적 검토 수행

3 우수 사례

- 가상자원 이용에 대한 로그 확인
- Servers ➔ Log History 화면에서 가상자원의 생성, 변경, 삭제에 대한 로그 히스토리 조회가 가능합니다.



- Log History에서 조회된 로그에 대해 금융회사에서는 인가 받지 않은 가상자원 접속, 생성, 변경, 삭제 등에 대한 주기적인 검토가 가능합니다.

4 참고 사항

- (참조) Log History 매뉴얼 참조 : Cloud 매뉴얼 (kt.com)

1 기준

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

2 설명

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

3 우수 사례

① Watch 서비스 이용한 모니터링

Watch는 kt cloud 인프라 자원과 그 위에서 동작하는 애플리케이션 모니터링을 위한 서비스입니다. kt cloud watch는 사용자가 별도의 설치/설정 작업 없이도 모니터링 활동이 가능하도록 설계되어 있어 Agentless한 방식으로 기본적인 모니터링 데이터를 자동 수집합니다.

즉, 서버를 생성하면 아무런 추가 작업 없이, 일정 시간 경과 후에 kt cloud watch로 모니터링이 가능한 것입니다. 다만, 이러한 기본 모니터링은 서비스 정책/시스템 제약 등의 사유로 선별된 모니터링 항목을 제공합니다.

업무 상황에 맞는 추가 모니터링 항목이 필요할 경우, 사용자가 직접 데이터를 수집/저장할 수 있는 방법을 제공합니다.

설치형 Agent 혹은 Open API를 활용하면, 사용자 정의 데이터로 kt cloud watch 모니터링 항목을 만들어 사용할 수 있습니다.

Watch 서비스에서 자동으로 수집/생성하는 모니터링 항목은 아래와 같습니다.

| 표 5-3-1 | 기본 모니터링 항목

구분	내용
kt cloud server (VM)	총 6종 (CPU Utilization, Free Memory, Disk Read/Write, Network In/Out)
kt cloud server (VR)	총 7종 (CPU Utilization, Free Memory, Disk Read/Write, Network In/Out, Conntrack)
kt cloud load balancer	총 3종 (Requests, Throughput, Connections)
kt cloud db	총 11종: 기본 6종 + db 특화 모니터링 항목 5종 (DATAFileSystemUsage, MEMORYUsage, PROCESSMysql, PROCESSKeepalived, ISFaulty)
kt cloud autoscaling (autoscaling group)	총 6종 (CPU Utilization, Free Memory, Disk Read/Write, Network In/Out)

1) Watch 접속하기

Watch는 일반적으로 다음과 같은 순서에 따라 접속 가능합니다.

포탈 상품소개 페이지에서 Monitoring 〉 Watch를 선택 후 상품신청 버튼을 클릭합니다. (단, 이때 서버 신청이 먼저 이루어져 있어야 합니다.)

Watch 하위 메뉴를 클릭하여 Watch(현황) 및 Alarm, Metric 버튼을 클릭해 Alarm정보를 확인하고 관리할 수 있습니다.

| 그림 5-3-1 | Alarm 현황 조회 화면

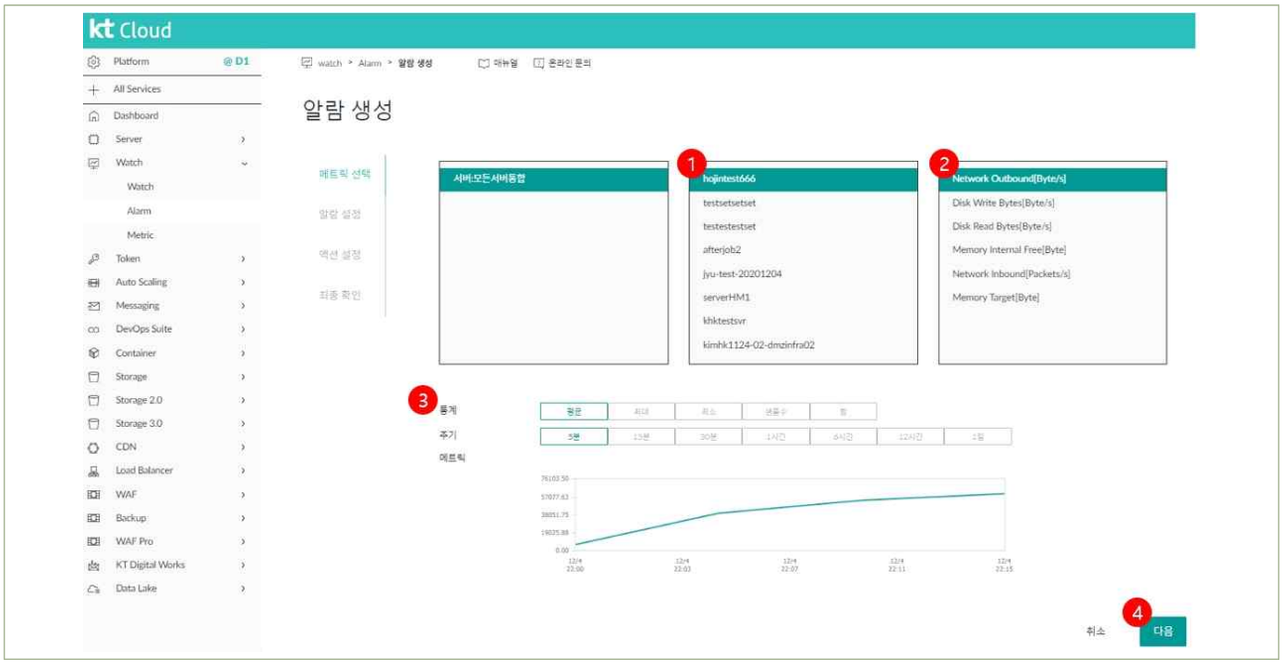
- (1) Alarm 페이지로 넘어가 Alarm 현황을 알 수 있습니다.
- (2) Metric 페이지로 넘어가 자원, 유형별로 Metric을 확인할 수 있습니다.
- (3) 현재 설정된 Alarm의 조건(빨간색 점선)과 Metric을 확인할 수 있습니다.

2) Watch 알람의 생성 및 삭제

kt cloud 콘솔에서 Watch를 선택한 후 Alarm 버튼을 클릭하여 Alarm을 생성하고 삭제할 수 있습니다.

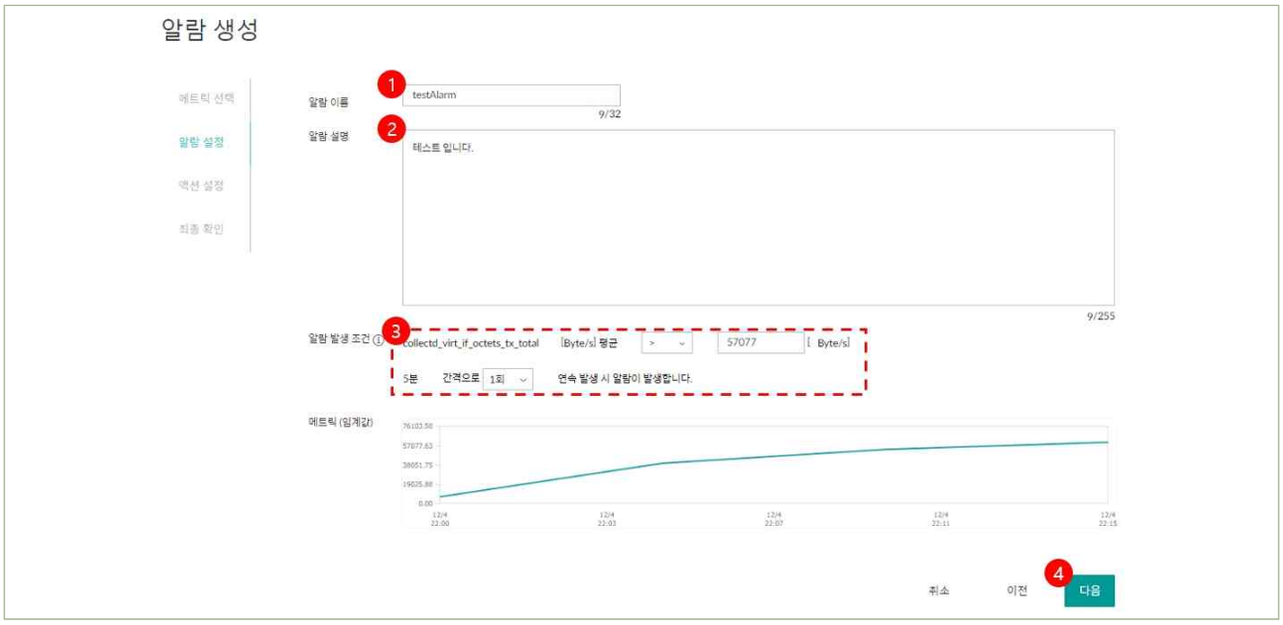
Watch 〉 Alarm 메뉴에서 '알람 생성' 버튼을 클릭합니다.

| 그림 5-3-2 | 알람 생성



| 그림 5-3-3 | 알람 생성 – 메트릭 선택 화면

- (1) Alarm 발생 조건을 만드는 자원을 선택합니다.
- (2) Alarm을 발생시킬 Metric(이름, 이름에 해당하는 값) 조건을 클릭합니다. (Manual은 Network Outbound를 예시로 합니다.)
- (3) 조건을 클릭하면 하단에 통계는 "평균" 주기는 "5분"이 기본값으로 메트릭 그래프가 출력됩니다.
- (4) 다음을 클릭하여 알람을 설정합니다.



| 그림 5-3-4 | 알람 생성 – 알람 설정 화면

- (1) Alarm 이름을 기입합니다. Manual은 "testAlarm"으로 기입했습니다.
- (2) Alarm 설명을 기입합니다. Manual은 "테스트입니다."
- (3) Alarm 발생 조건을 기입합니다. Manual은 "NetworkOutbound" Byte 평균이 "57077" Byte보다 "클 때"가 5분 간격으로 "1회" 발생시 Alarm이 발생합니다.
- (4) 다음을 클릭하여 액션을 설정합니다.

| 그림 5-3-5 | 알람 생성 – 액션 설정 화면

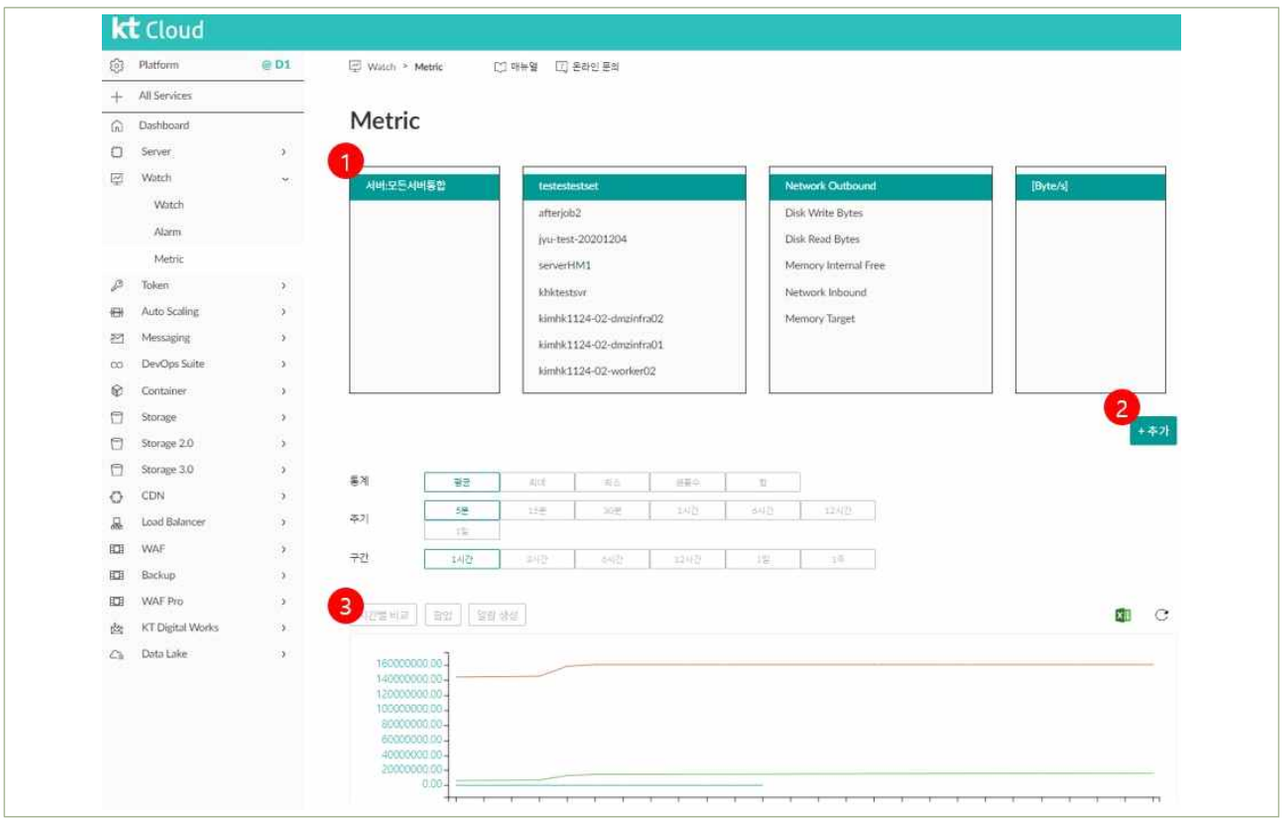
- (1) Alarm 상태를 선택합니다. "발생","안정","데이터 부족" 세 가지 중 선택합니다.
- (2) 액션 선택을 선택합니다. "이메일", "SMS", "오토스케일링" 세 가지 중 선택합니다.
- (3) 이메일을 받을 주소를 기입합니다. Manual은 "test@kt.com"입니다.
- (4) + 추가 버튼을 클릭합니다.
- (5) 다음을 클릭하여 신청 내역을 최종 확인한 후 생성하기를 클릭합니다.

| 그림 5-3-6 | 알람 정보 확인 화면

- (1) 클라우드 콘솔의 Alarm 목록 테이블은 알람 "이름", "상태", "알람 발생조건", "활성화 여부"(액션 수행여부), "구분"((자원명):(개별서버메트릭|통합서버메트릭)) 정보를 보여줍니다.
- (2) 상태를 보고 싶은 Alarm에 해당하는 행의 체크박스를 클릭합니다.
- (3) "상태변경" 버튼을 통해 알람의 상태를 변경할 수 있습니다.
- (4) "활성화" 버튼을 통해 해당 Alarm을 사용할지 여부를 확인할 수 있습니다.
- (5) "..." 버튼의 "메트릭 보기"를 선택하여 해당 Alarm을 발생시키는 메트릭 그래프를 볼 수 있습니다.
- (5-1) "..." 버튼의 "액션 보기"를 선택하여 해당 Alarm이 SMS를 발생시키는지 E-mail을 발생시키는지 확인할 수 있습니다.
- (5-2) "..." 버튼의 "알람 히스토리"를 선택하여 해당 Alarm 발생 이력을 확인할 수 있습니다.
- (6) 모든 상태 〉 버튼에 마우스를 Hang over하여 상태별로 필터링이 가능합니다.

3) Metric(Dimension(특정 시간, Metric 이름, Metric 값)의 집합) 조회

kt cloud 콘솔에서 Watch를 선택한 후 Metric 버튼을 클릭하여 서버 별 Metric 정보를 통합하여 그래프로 시각화 할 수 있습니다.



| 그림 5-3-7 | Watch 메트릭 조회

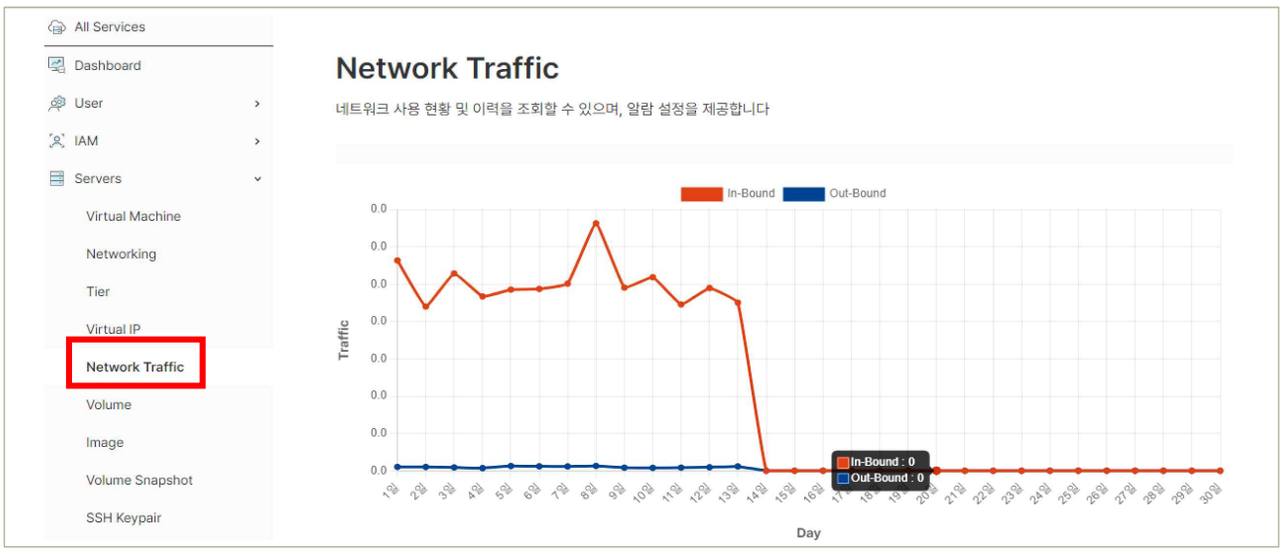
- (1) 메트릭 목록 화면에서 그래프로 표현하고 싶은 네임스페이스((자원명):(통합|개별)), 자원 이름, Metric 이름, Metric 단위를 선택할 수 있습니다.
- (2) "+추가" 버튼을 눌러 Metric을 추가합니다.
- (3) 통계, 주기, 구간 별로 네임스페이스의 Metric을 볼 수 있습니다.
- *본 메뉴얼에는 "서버:모든서버통합" 있으나, 그 외 서버:운영체제, 서버:스펙별통합, 서버:개별서버매트릭 등도 선택 가능합니다.

② Network Traffic 서비스 이용한 네트워크 모니터링

Network Traffic 기능은 일자별 서버 트래픽의 추이를 그래프로 한눈에 확인할 수 있으며, 알람 설정을 통해 일정 수준 이상 인바운드 혹은 아웃바운드 트래픽이 발생할 때 알람 통보를 문자메시지 또는 이메일을 통해 받을 수 있는 기능합니다.

1) 웹 콘솔 접속 후 Servers 〉 Network Traffic 〉 네트워크 트래픽 모니터링

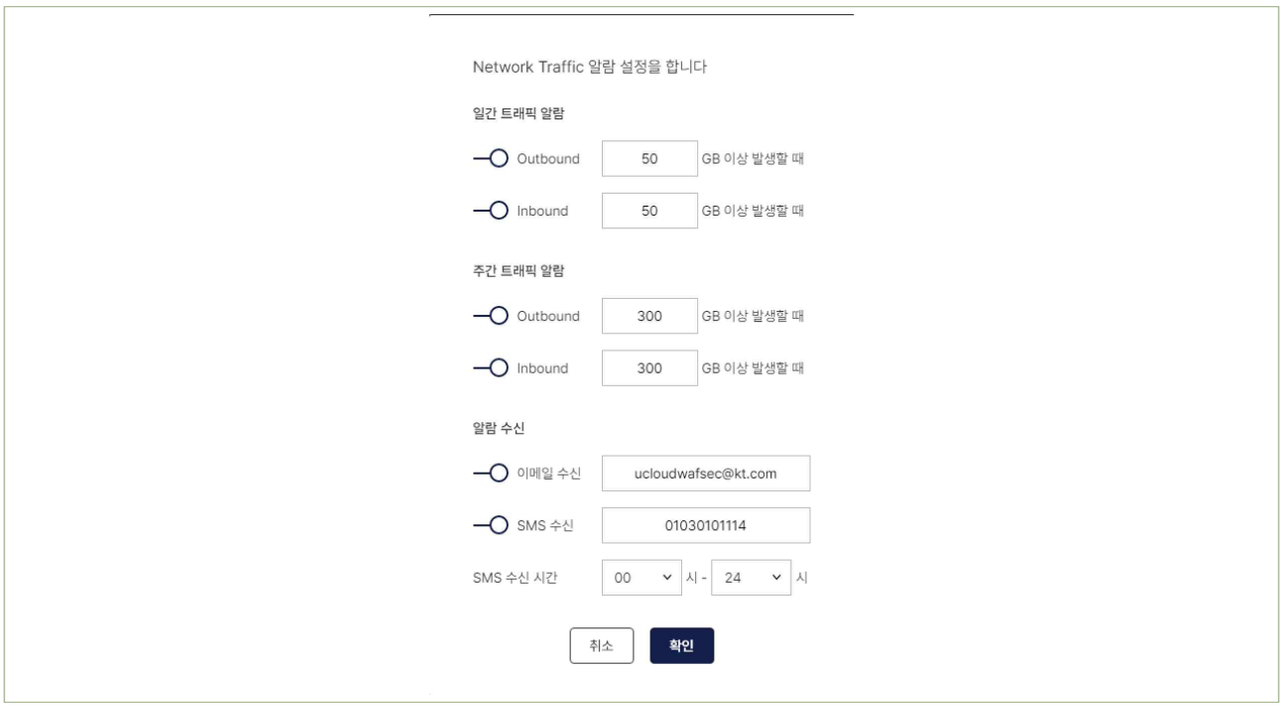
Zone별로 inbound/outbound 트래픽 사용 현황 및 이력을 조회할 수 있습니다. 그래프 및 표로 조회가 가능하며 엑셀 데이터 제공 기능 또한 사용할 수 있습니다.



| 그림 5-3-8 | Network Traffic 조회

2) 네트워크 트래픽 임계치에 따른 알람 설정

3) 일간/주간 트래픽 임계치 설정 및 알람 수신 설정



| 그림 5-3-9 | 트래픽 알람 설정

4 참고 사항

- Watch 서비스 포탈 매뉴얼 참조 : **Cloud 매뉴얼 (kt.com)**
- Network Traffic 포탈 매뉴얼 참조 : **Cloud 매뉴얼 (kt.com)**

1 기준

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

2 설명

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

3 우수 사례

- API를 통해 API 사용 이력을 확인할 수 있습니다.
  - [User ➔ 내 문의 ➔ 문의하기] API 이력 확인 요청
  - 문의하기를 통해 API 사용 이력을 요청하면, 답변을 통해 요청에 적합한 API 가이드가 제공됩니다. 금융회사에서는 해당 API를 통해 API 사용에 대한 이력(호출대상, 호출자, 호출일시)을 확인할 수 있습니다.

문의 상세

이전페이지 | 회원정보

문의자ID		상태	2선접수
문의자명		회신 이메일	
휴대폰		문의날자	
접수자		2선이관일	
2선접수자		3선이관일	
문의서비스	Cloud 포탈	문의유형	상품 | 기능오류(기타)
재문의횟수	0	답변횟수	1
문의제목			
문의내용	안녕하세요 고객이 주기적인 VM등의 리소스 생성삭제 등의 로그를 받기를 희망하셔서 kt cloud 공공 D 존의 api를 사용하여 로그를 받아보려고 했습니다. User-> API Gateway key 관리 탭의 생성 버튼을 눌러 api key를 생성해보려고 했지만 첨부와 같이 오류가 발생합니다. 확인 부탁드립니다. 감사합니다.		
첨부파일	apigwkeyerror.png		

답변등록 / 2선이관

답변 상세

답변제목	Re: API Gateway key 관리 생성이 안됩니다.			긴급/이슈	
답변자그룹	KT Cloud 임/직원	답변자명		답변날자	
답변내용	kt cloud를 사용해 주셔서 감사합니다. 문의하신 내용에 대한 답변을 드립니다. [답변 내용] Open API의 인증 처리는 콘솔 기능의 API Gateway key가 아닌, 매뉴얼(https://cloud.kt.com/docs/open-api-guide/d/guide/how-to-use)의 D플랫폼 인증 토큰 발행 기능을 활용 부탁드립니다 리소스들에 대한 로그 조회는 매뉴얼에 명시가 되어 있지 않아서 아래 사용 방법 전달드립니다. DX-G Endpoint : https://api.ucloudbiz.olleh.com/gd1/logs DX-G-YS Endpoint : https://api.ucloudbiz.olleh.com/gd4/logs Request Header : X-Auth-Token (위 매뉴얼 확인) Request Parameter - resource : Load Balancer, NAS, Server, Firewall, Tier, IP, Volume Image, Volume, Volume Snapshot, Server Image, Cdn Standard, Waf, Waf Pro - event : all, create, delete, update - start : YYYY-MM-DDTHH:mm:ss (ex : 2025-01-01T00:00:00) - end : YYYY-MM-DDTHH:mm:ss (ex : 2025-05-16T00:00:00) 추가적인 문의 사항 있으시면 재문의 주시기 바랍니다. 감사합니다.				
첨부파일					

| 그림 5-4-1 | Api 이력 확인 요청

4 참고 사항

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

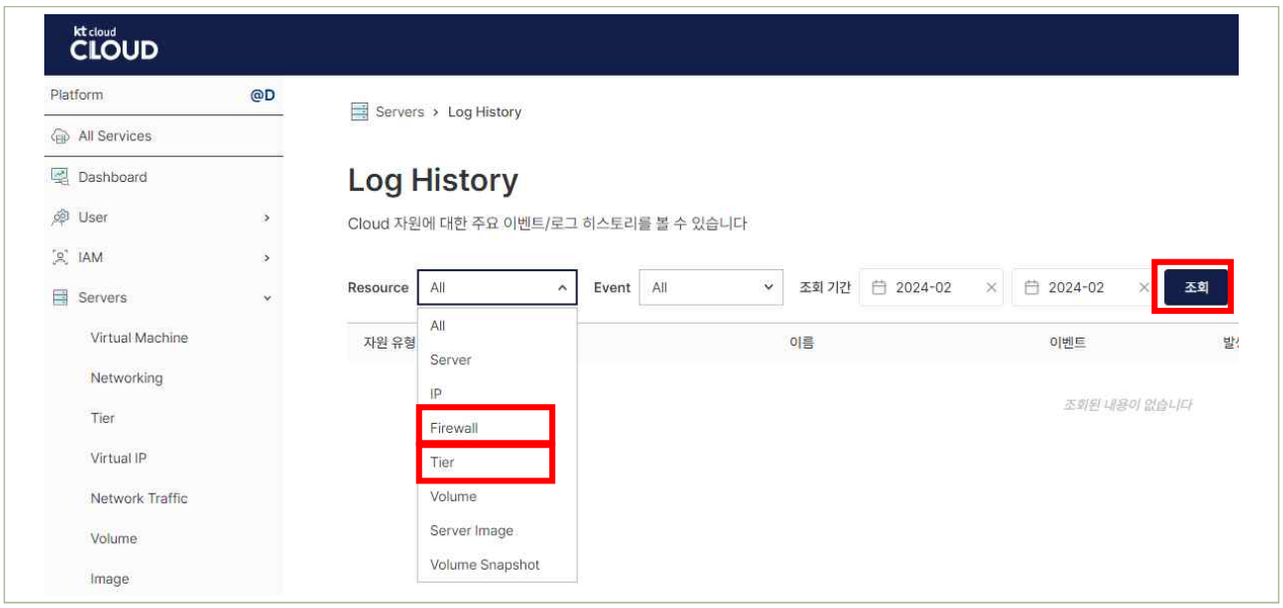
3 우수 사례

다양한 네트워크 기능 사용에 대한 감사로그 확인이 가능합니다. 즉, NAT 규칙 생성이나 방화벽 정책 생성/삭제, Tier 생성/삭제 등에 대한 변경이력에 대해 확인이 가능합니다.

1) 웹 콘솔 접속 후 Servers 〉 Log History

| 그림 5-5-1 | 로그 조회 화면

2) Resources 항목에서 Firewall 선택 후 조회

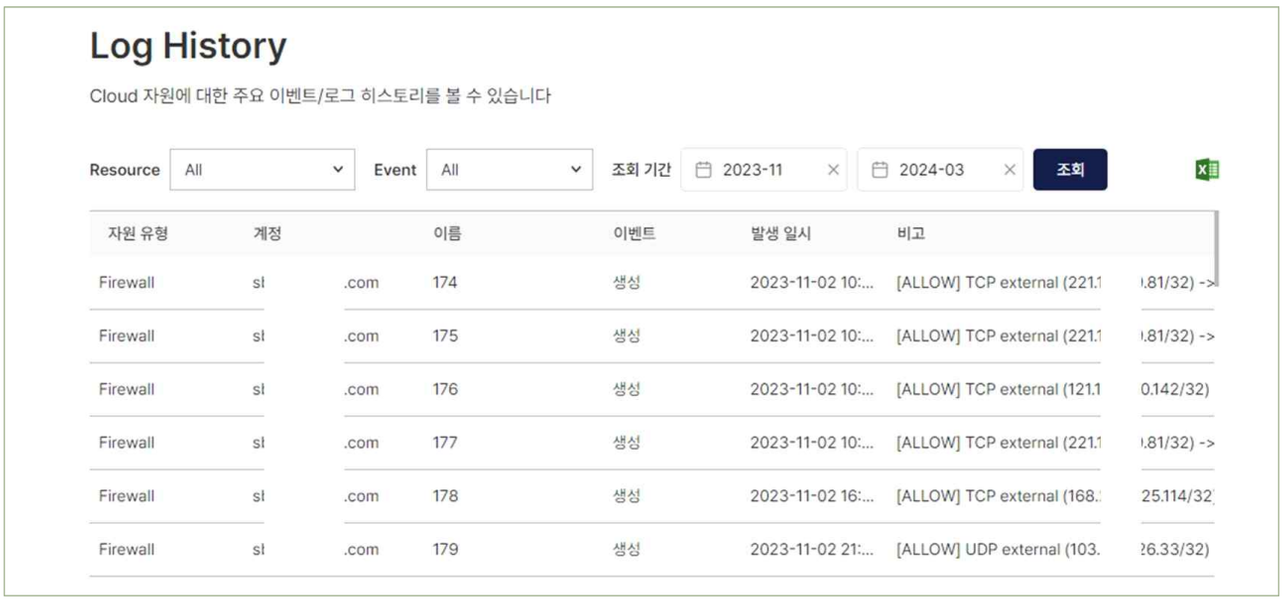


| 그림 5-5-2 | Log 조회 대상 리소스 유형 선택

3) 결과 조회

로그 조회 화면에서 리소스 유형을 Firewall을 선택하면 NAT 설정이나 방화벽 포트 오픈 등 정책 설정 이력이 조회됩니다.

Tier 생성, 삭제 이력의 경우 Log History 리소스 선택 시 Tier를 선택하여 조회 화면 Tier 생성, 삭제 이력 확인이 가능합니다.



| 그림 5-5-3 | 방화벽 정책 변경 로그 조회 결과

4 참고 사항

- Log History 포탈 매뉴얼 참조 : Cloud 매뉴얼 (kt.com)

1 기준

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

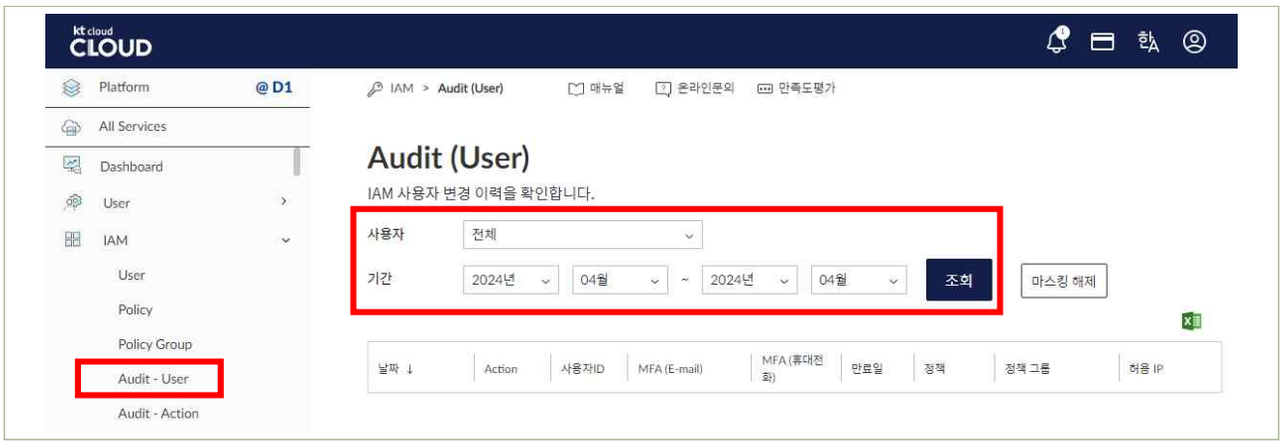
2 설명

- 클라우드 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

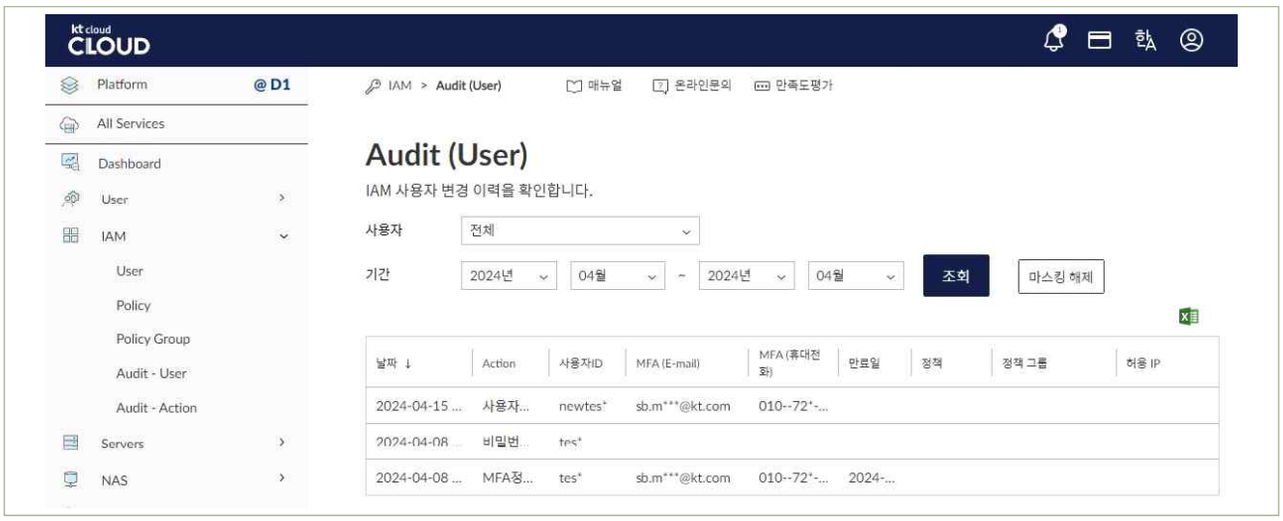
가상자원관리시스템 계정의 생성 및 변경에 대한 로그를 확인할 수 있습니다.

1) 웹 콘솔 접속 후 IAM 〉 Audit -User 메뉴 선택
2) 화면 상단 검색 기간 등을 입력 후 조회 버튼을 클릭합니다



| 그림 5-6-1 | IAM 계정 변경 로그 조회

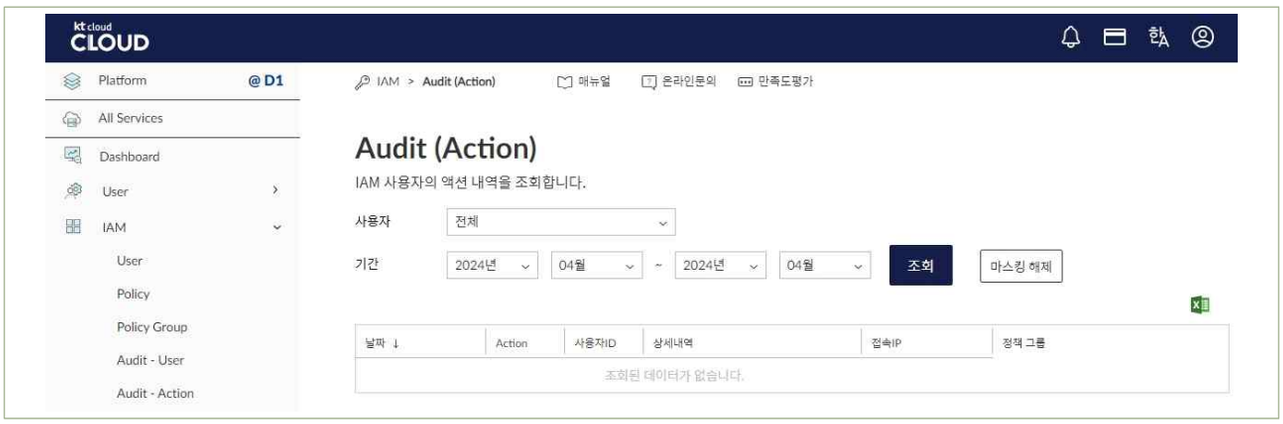
3) 포탈 IAM 계정 변경 로그가 아래와 같이 조회됩니다.



| 그림 5-6-2 | 계정 변경 로그 조회 결과

IAM 계정의 변경 외에 해당 계정의 포탈 접속등 행위 이력에 대해서도 조회가 가능합니다.

1) 웹 콘솔 접속 후 IAM 〉 Audit-Action 메뉴 선택



| 그림 5-6-3 | IAM 계정 행위 로그 조회

4 참고 사항

- IAM Audit (Action) 포탈 매뉴얼 참조 : Cloud 매뉴얼 (kt.com)

1 기준

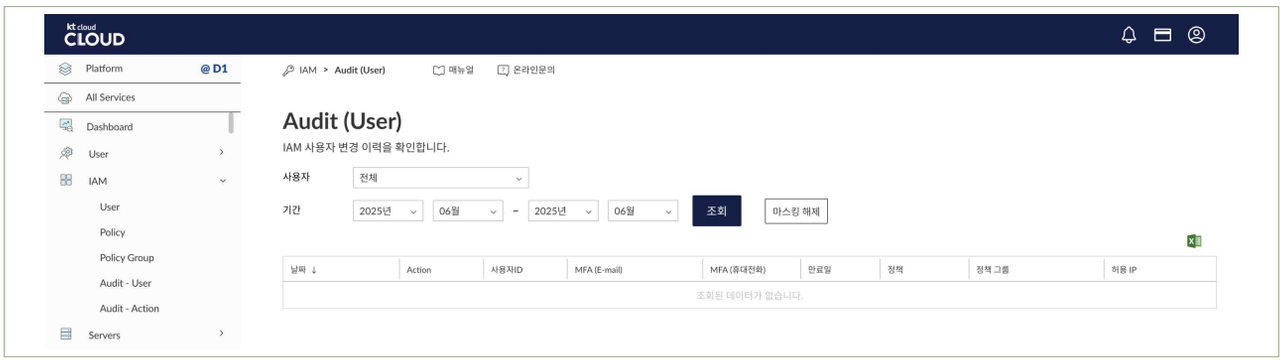
식별번호	기준	내용
5.7.	**계정 변경사항에 대한 모니터링 수행**	**클라우드 서비스 이용 계정 변경사항 (생성, 삭제 등) 에 관한 로깅 및 모니터링을 수행하여야 한다.**

2 설명

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

3 우수 사례

- 가상자원관리시스템 계정의 생성 및 변경에 대한 로그를 확인할 수 있습니다.
  - [IAM -〉 Audit-User ➔ 조회] IAM 계정 변경 로그 조회 가능



| 그림 5-7-1 | 계정 변경사항 조회

금융회사에서는 위 로그를 통해 인가받지 않은 계정의 생성, 삭제 등에 대한 상시적인 모니터링을 수행하여야 합니다.

또한, 위 로그에 대해 주기적 (전자금융감독규정 또는 내부 규정등에 의거)로 검토해야 합니다.

4 참고 사항

- IAM 포탈 매뉴얼 참조 : Cloud 매뉴얼 (kt.com)

6. API 관리

6.1. API 호출 시 인증수단 적용
6.2. API 호출 시 무결성 검증
6.3. API 호출 시 인증 키 보호대책 수립
6.4. API 이용 관련 유니크값 유효기간 적용
6.5. API 호출 구간 암호화 적용

6 API 관리

1 기준

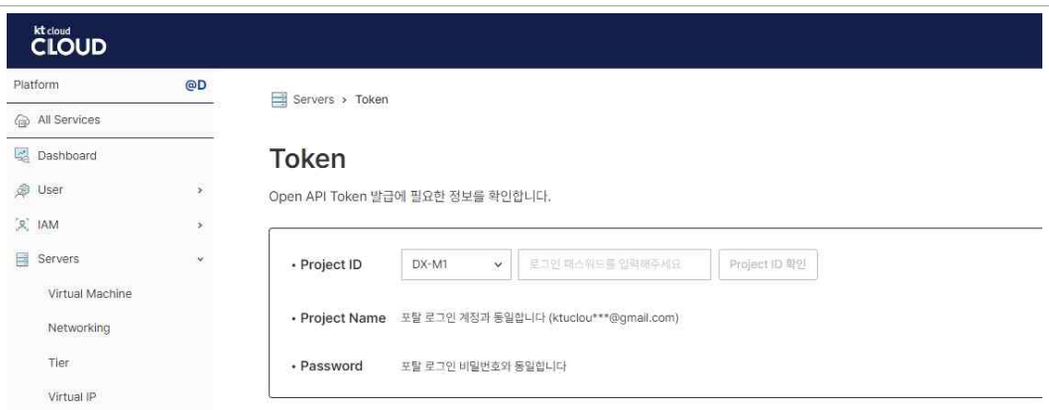
식별번호	기준	내용
6.1.	API 호출 시 인증수단 적용	클라우드 가상자원 관리를 위한 API 호출 시, 안전한 인증수단을 적용하여 보안성을 강화하여야 한다.

2 설명

- API 호출 시 이용자를 인증할 수 있는 수단을 적용하여야 한다.
  - 예시
    1) API 호출이 가능한 IP 지정
    2) IAM 기능과 연동하여 API를 호출할 수 있는 권한 제어
    3) API 호출시 사용되는 인증값을 단기 인증 값으로 사용 등

3 우수 사례

- **(민간, 공공 – D플랫폼)**
  - D1콘솔에서 [Servers 〉 Token]메뉴를 통해 API 호출 인증을 위한 Project ID, Project Name, Password 조회 기능을 제공합니다.



| 그림 6-1-1 | API 인증 Token 제공

- API 사용 가이드에서 Token 발급 가이드를 제공합니다.

서비스 이용 방법 (Platform @D)

개요

kt cloud 의 @D Platform 에서 사용 가능한 Open API 가이드 문서입니다.
본 페이지에서는 Open API 호출을 위한 기본 준비 사항를 예제와 함께 안내해드립니다.

1. kt cloud 의 Open API 는 RESTful API 방식으로 제공되며, OpenStack API 와의 호환성을 지원합니다.
2. HTTP method 방식과 사전 정의된 Request 파라미터에 따라 클라우드 자원 및 서비스 항목들을 등록, 수정, 삭제 및 조회 할 수 있습니다.
3. 기본적인 Open API 호출 방법은 아래와 같습니다.
   Step 1. 인증 토큰 발급 > Step 2. Open API 호출 > Step 3. 응답 또는 에러 처리

Step 1. 인증 Signature 생성

DX-M1 Zone(@D1)의 Open API를 사용하기 위해서는, 먼저 인증 요청을 통해 인증 토큰을 발급 받아야 합니다.

Notice

1. 인증 토큰은 발급 후 "60분" 동안만 사용 가능합니다.
2. 인증 토큰은 다른 이유로 인해 유효하지 않게 될 수 있습니다. (ex. 사용자 역할 변경 등)

1. API URI (인증 토큰 발행)

POST https://api.ucloudbiz.olleh.com/d1/identity/auth/tokens

| 그림 6-1-2 | Token 발급 가이드

- D1 플랫폼의 Token 발급을 위해 Request Body 내 필요 정보를 기입합니다.

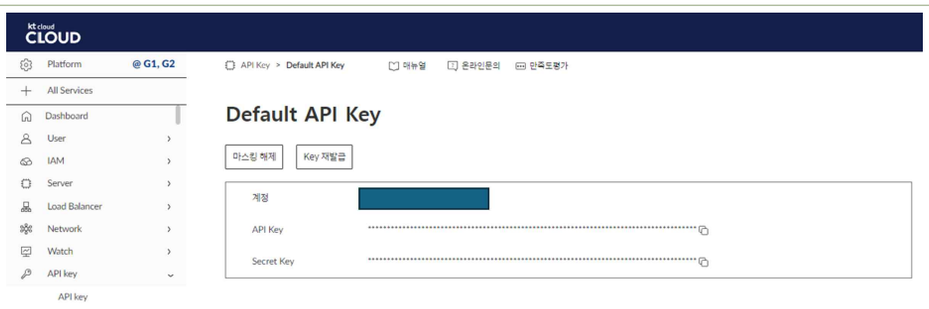
Name	In	Type	Description
auth	Body	Object	
auth.identity	Body	Object	
identity.methods	Body	Array	Default로 "password" 값 사용
identity.password	Body	Object	
password.user	Body	Object	
user.domain	Body	Object	
user.domain.id	Body	String	Default로 "default" 값 사용
user.name	Body	String	사용자의 id
user.password	Body	String	사용자의 password
auth.scope	Body	Object	
scope.project	Body	Object	
project.domain	Body	Object	
project.domain.id	Body	String	Default로 "default" 값 사용
project.name	Body	String	사용자의 id

| 그림 6-1-3 | Request Body 정보 기입

- 발급받은 인증 Token의 유효시간은 1시간으로 지정되어 있으며, 이후에 재발행이 필요합니다.
- 인증 토큰 발급 요청이 성공하면 “201 Created” 응답 코드와 함께, 인증 토큰이 응답 헤더의 “X-Subject-Token” 필드값으로 전달됩니다. 응답 본문에는 인증토큰의 만료 날짜와 시간이 표시됩니다.

(민간 – G플랫폼)

- G플랫폼 콘솔 [API Key]메뉴를 통해 API Key, Secret Key 조회하는 기능을 제공합니다.
- 제공되는 API Key, Secret Key는 신규 Key 재발급 기능을 제공합니다.



| 그림 6-1-4 | G플랫폼 API Key

- ‘URL Parameter, API Key, Secret Key’를 이용하여 HMAC SHA-1을 통해 인증 Signature를 생성합니다.
  * API 호출에 사용하는 URL Parameter는 아래와 같은 규칙으로 정의

Order	Type	Description
1	API Key	발급 받은 API Key
2	API 명령어	command 필드에서 사용하는 API 기능에 대한 값
3	API 명령어 옵션	API 명령어 관련 필수 또는 부가적으로 사용되는 항목
4	응답 양식	요청에 대한 응답을 XML 또는 JSON 으로 제공 받을 지 선택 (Default 는 XML)

| 그림 6-1-5 | URL Parameter 규칙 정의

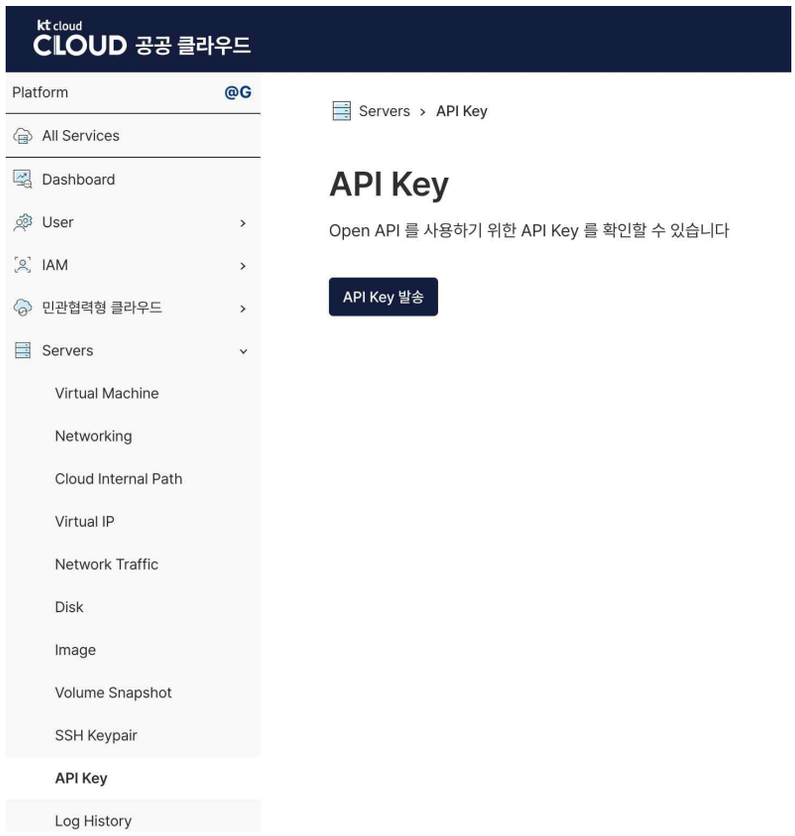
- API 호출시 사용되는 아래 Parameter들을 추가하여, API의 사용 만료 시간 설정이 가능합니다.

Parameter	Example	Description
signatureVersion	signatureVersion=3	signatureVersion 파라미터가 없거나, 필드 값이 다른 경우에는 expires 파라미터는 무시됩니다.
expires	expires=2021-03-15T09:45:19.659Z	만료 시간을 YYYY-MM-DDThh:mm:ssZ 형식(ISO 8601)으로 설정

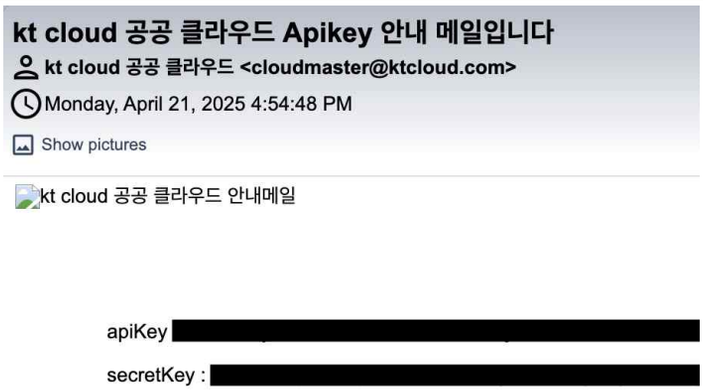
| 그림 6-1-6 | API 사용 만료 시간 설정

(공공 - G플랫폼)

- G플랫폼 콘솔 [Servers 〉 API Key]메뉴를 통해 API Key, Secret Key를 계정 메일 주소로 발송하는 기능을 제공합니다.



| 그림 6-1-7 | API 키 발송



| 그림 6-1-8 | API key 안내 메일

- 인증 Signature를 생성하는 방법은 민간과 동일합니다.
- API Key 재발급은 제공하지 않습니다.

4 참고 사항

- Open API 사용 가이드 참조(민간, 공공 동일)

  D1 플랫폼 : https://cloud.kt.com/docs/open-api-guide/d/guide/how-to-use

  G1/G2 플랫폼 : https://cloud.kt.com/docs/open-api-guide/g/guide/how-to-use

1 기준

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

2 설명

- API 호출 시 호출 메시지의 무결성을 보장하기 위한 방안을 확보하여야 한다(또는 확인하여야 한다).
  - 예시
    1) API 보안 키와 서명을 통한 변조방지 대책 마련 등

3 우수 사례

- **(민간, 공공 – D플랫폼)**
  - 발급된 API 인증 토큰에 대해 유효성 체크 기능을 제공합니다. DX-M1 Zone 의 Open API를 사용하기 위해서는 먼저 인증 요청을 통해 인증 토큰을 발급 받아야 합니다.
  - 인증 토큰은 발급 후 60분 동안만 사용 가능합니다.
  - 인증 토큰은 다른 이유로 인해 유효하지 않게 될 수 있습니다. (ex. 사용자 역할 변경 등)
  - Open API 호출 시, 유효한/유효하지 않은 헤더로 API 호출 시 정상/실패 처리 결과가 제공됩니다.

- **(민간, 공공 – G플랫폼)**
  - API 호출에 대한 Signature가 유효할 경우 성공 응답을 제공합니다.

[Request]

curl -ki -XGET 'https://api.ucloudbiz.olleh.com/server/v1/client/api?apiKey={API KEY}&command=listVirtualMachine&zoneid=eceb5d65-6571-4696-875f-5a17949f3317&signature={인증 Signature}'

[Response]

```
HTTP/1.1 200 OK
Date: Tue, 16 Apr 2024 09:45:16 GMT
Server: Apache-Coyote/1.1
X-Content-Type-Options: nosniff
X-XSS-Protection: 1;mode=block
content-security-policy: 1
content-security-policy: default-src='none'
content-security-policy: script-src='self'
content-security-policy: connect-src='self'
content-security-policy: img-src='self'
content-security-policy: style-src='self'
Content-Type: text/xml;charset=UTF-8
Transfer-Encoding: chunked
```

- API 호출에 대한 Signature가 유효하지 않은 경우 401 오류 응답을 제공합니다.

[Request]

curl -ki -XGET 'https://api.ucloudbiz.olleh.com/server/v1/client/api?apiKey={API KEY}&command=listVirtualMachine&expires=2024-04-15T12%3A00%3A00%2B0530&signatureVersion=3&zoneid=eceb5d65-6571-4696-875f-5a17949f3317&signature={인증 Signature}'

[Response]

```
HTTP/1.1 401 Unauthorized
Date: Tue, 16 Apr 2024 08:50:50 GMT
Server: Apache-Coyote/1.1
X-Content-Type-Options: nosniff
X-XSS-Protection: 1;mode=block
content-security-policy: 1
content-security-policy: default-src='none'
content-security-policy: script-src='self'
content-security-policy: connect-src='self'
content-security-policy: img-src='self'
content-security-policy: style-src='self'
Content-Type: text/xml;charset=UTF-8
Content-Length: 236

<?xml version="1.0" encoding="UTF-8"?><listvirtualmachinesresponse cloud-stack-v
ersion="4.11.0.12"><errorcode>401</errorcode><errortext>unable to verify user cr
edentials and/or request signature</errortext></listvirtualmachinesresponse>[OS
```

4 참고 사항

1 기준

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

2 설명

- API 호출 시 인용되는 유니크 값(ex. 보안키 등)은 안전하게 보관 및 관리하여야 한다.
  - 예시
    1) API 호출을 서명하는데 사용되는 비밀키, 인증서 등은 노출되지 않도록 관리하여야 한다.

3 우수 사례

- **(민간, 공공 – D플랫폼)**
  - Token 발급을 위한 Project ID 조회 시, 계정의 비밀번호 인증을 통해 조회가 가능합니다.
  - 주기적으로 대상 계정의 비밀번호 변경을 통해 안정적으로 관리 가능 가능합니다.

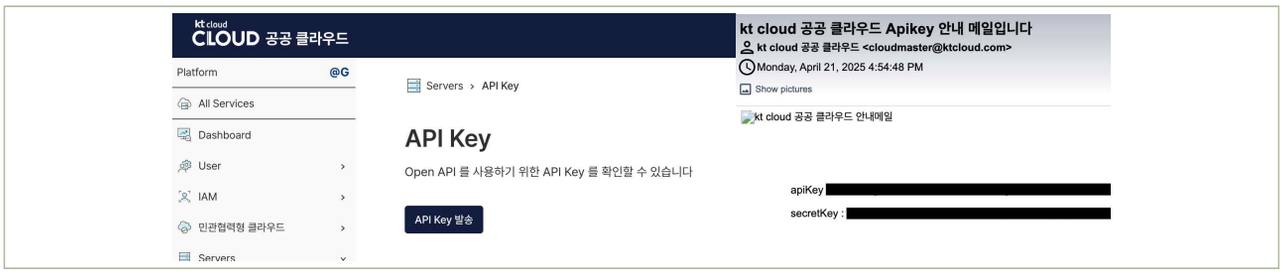
| 그림 6-3-1 | Token 발급 정보 확인

- **(민간 – G플랫폼)**
  - API Key 조회를 위한 마스킹 해제 시, 계정의 비밀번호 인증을 통해 조회가 가능합니다.

| 그림 6-3-2 | API Key 조회

(공공 – G플랫폼)

- API Key 조회를 위하여 API Key를 계정 메일로 발송할 수 있습니다.



| 그림 6-3-3 | API Key 발송

4 참고 사항

1 기준

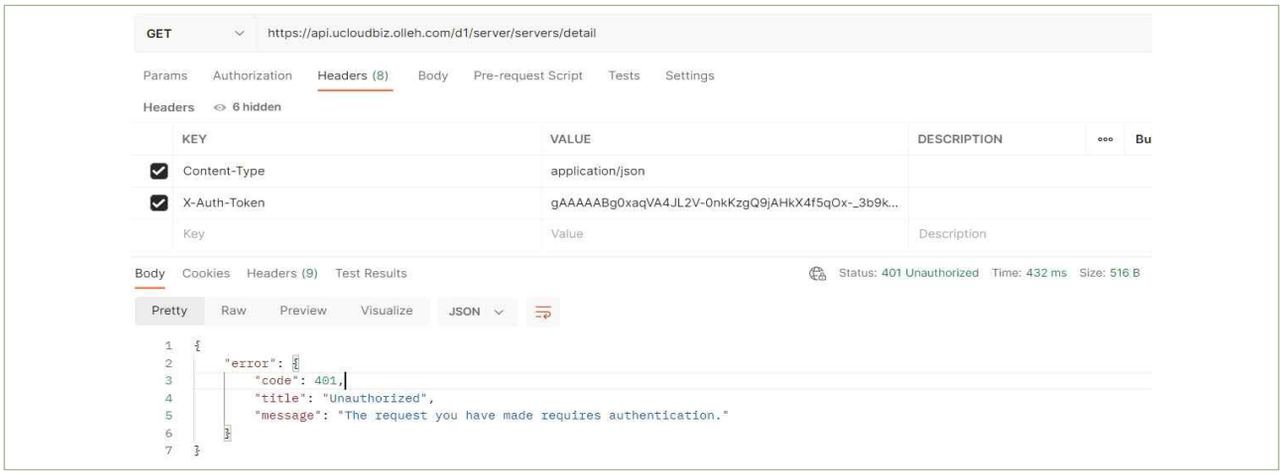
식별번호	기준	내용
6.4.	**API 이용 관련 유니크값 유효기간 적용**	**클라우드 가상자원 관리를 위해 API 기능 이용 시, 세션 유효기간 및 유니크값(보안키 등)에 대한 만료기간을 설정하여야 한다.**

2 설명

- API 세션 및 서명값에 대한 유효기간을 설정하고, 유니크값(보안키 등) 유출 방지 대책으로 만료기간을 적용하여야 한다.
  - 예시
    1) API 호출 세션의 유효기간 설정
    2) 서명의 유효기간 확인
    3) API 보안키 만료기간 설정
    4) 유니크값(보안키 등) 폐기 및 재발급 기능으로 만료기간 준수 등

3 우수 사례

- **(민간, 공공 - D플랫폼)**
  - DX-M1 Zone의 Open API를 사용하기 위해서는 먼저 인증 요청을 통해 인증 토큰을 발급받아야 합니다. 발급되는 토큰에 대해서는 1시간 기준으로 유효하며, 만료된 토큰으로 API 호출 시 오류가 발생합니다.
    D1 토큰 발급 시, expires_at을 통해 토큰 만료시간 확인이 가능합니다.
    만료된 토큰으로 API 실행 시 401 오류가 리턴됩니다.



| 그림 6-4-1 | 만료된 토큰으로 API 실행

(민간, 공공 - G플랫폼)

- API 호출 시 Signature의 유효기간을 설정하는 parameter를 통해 만료시간 설정기능을 제공합니다.

Parameter	Example	Description
signatureVersion	signatureVersion=3	signatureVersion 파라미터가 없거나, 필드 값이 다른 경우에는 expires 파라미터는 무시됩니다.
expires	expires=2021-03-15T09:45:19.659Z	만료 시간을 YYYY-MM-DDThh:mm:ssZ 형식(ISO 8601)으로 설정

| 그림 6-4-2 | Signature 유효기간 제공 parameter

- API 호출 시 만료된 Signature 기반으로 401 오류가 리턴됩니다.

[Request]

curl -ki -XGET 'https://api.ucloudbiz.olleh.com/server/v1/client/api?apiKey={API KEY}&command=listVirtualMachine&expires=2024-04-15T12%3A00%3A00%2B0530&signatureVersion=3&zoneid=eceb5d65-6571-4696-875f-5a17949f3317&signature={인증 Signature}'

[Response]

```
HTTP/1.1 401 Unauthorized
Date: Tue, 16 Apr 2024 08:50:50 GMT
Server: Apache-Coyote/1.1
X-Content-Type-Options: nosniff
X-XSS-Protection: 1;mode=block
content-security-policy: 1
content-security-policy: default-src='none'
content-security-policy: script-src='self'
content-security-policy: connect-src='self'
content-security-policy: img-src='self'
content-security-policy: style-src='self'
Content-Type: text/xml;charset=UTF-8
Content-Length: 236

<?xml version="1.0" encoding="UTF-8"?><listvirtualmachinesresponse cloud-stack-v
ersion="4.11.0.12"><errorcode>401</errorcode><errortext>unable to verify user cr
edentials and/or request signature</errortext></listvirtualmachinesresponse>[OS
```

(민간 – G플랫폼)

- API Key 분실 및 유출 시 Key 재발급 기능을 통해 새로운 Key 발급이 가능합니다.

| 그림 6-4-3 | API Key 재발급

4 참고 사항

1 기준

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

2 설명

- API를 통한 클라우드 가상자원 관리 수행 시 네트워크 트래픽 보호를 위한 암호화된 통신구간을 적용하여야 한다. (또는 확인하여야 한다.)
  - 예시
    1) TLS 1.3 지원

3 우수 사례

KT Cloud의 Open API는 TLS(SSL) 암호화 통신이 적용되어 있으며, TLS 1.3을 지원합니다.

```
% curl -v --tls-max 1.3 https://api.ucloudbiz.olleh.com
* Host api.ucloudbiz.olleh.com:443 was resolved.
* IPv6: (none)
* IPv4: 211.252.122.71
*   Trying 211.252.122.71:443...
* Connected to api.ucloudbiz.olleh.com (211.252.122.71) port 443
* ALPN: curl offers h2,http/1.1
* (304) (OUT), TLS handshake, Client hello (1):
*  CAfile: /etc/ssl/cert.pem
*  CApath: none
* (304) (IN), TLS handshake, Server hello (2):
* (304) (IN), TLS handshake, Unknown (8):
* (304) (IN), TLS handshake, Certificate (11):
* (304) (IN), TLS handshake, CERT verify (15):
* (304) (IN), TLS handshake, Finished (20):
* (304) (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / AEAD-CHACHA20-POLY1305-SHA256 / [blank] / UNDEF
* ALPN: server did not agree on a protocol. Uses default.
```

| 그림 6-5-1 | TLS1.3 지원

7. 스토리지 관리

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

7 스토리지 관리

1 기준

식별번호	기준	내용
7.1.	**스토리지 접근 관리**	**스토리지 목적에 따라 외부 공개 차단 등 적절한 접근 관리를 수행하여야 한다.**

2 설명

- 스토리지 목적에 따라 외부 공개 차단 등 적절한 접근 관리를 수행하여야 한다.
  - 예시
    1) 외부에 공개가 필요한 Bucket에 대해서만 Bucket policy를 통한 익명 사용자 접근허용. (Default 비허용)
    2) Object 별 ACL 설정을 통한 접근 허용/비허용 (Default 비허용)
    3) Presigned URL을 통한, 일시적 접근 허용.

3 우수 사례

(API) S3 API 기반의 Object Storage는 외부에 공개가 필요한 Bucket에 대해서만 Bucket policy를 통해 공개가 필요한 자원들에 대해서 익명 사용자 접근허용이 가능합니다.

(Example)

예시로 아래 버킷 정책을 사용하여, 지정한 경로의 자원에 대해서 익명사용자 접근을 허용할 수 있습니다. 기본적으로는 익명사용자는 접근할 수 없습니다.

Resource에 대해서 지정된 경로에 대해서 적용이 가능하므로, 특정 경로를 입력하여도 됩니다.

적용은 S3 SDK 혹은 AWS CLI로 가능합니다.

[Sample Json] – 해당 구문을 AWS CLI 혹은 S3 SDK를 통해 적용

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDownloadBucket",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::{your-bucket-name}/*"
            ]
        }
    ]
}
```

[Sample Request] AWS CLI를 통한 적용

```
aws --profile={profile} --endpoint-url={endpoint} \
s3api put-bucket-policy --bucket {bucket} --policy file://bucket-policy.json
```

(API) Object 별 ACL 설정을 통한 접근 허용/비허용 (Default 비허용) 설정이 가능합니다.

(Example)

예시로 아래 API 설정을 통해서 Object에 대한 접근 설정을 변경할 수 있습니다.

권한들의 리스트는 아래와 같습니다.

Read, Write, Read Permissions, Write Permissions

User 종류는 아래와 같습니다.

AllUsers: 완전히 퍼블릭 오픈, 크롤링 및 무단 접근 위험 존재

AuthenticatedUsers: AWS 계정으로 로그인한 모든 사용자

[Sample Json] - 해당 구문을 AWS CLI 혹은 S3 SDK를 통해 적용

```
{
  "Owner": {
    "ID": "{Canonical ID}"
  },
  "Grants": [
    {
      "Grantee": {
        "Type": "CanonicalUser",
        "ID": "{Canonical ID}"
      },
      "Permission": "FULL_CONTROL"
    },
    {
      "Grantee": {
        "Type": "Group",
        "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
      },
      "Permission": "READ"
    }
  ]
}
```

[Sample Request] AWS CLI를 통한 적용

```
aws --profile={profile} --endpoint-url={endpoint} \
s3api put-object-acl --bucket {bucket} -key {object} --access-control-policy file://acl.xml
```

(API) Presigned URL을 통한, 일시적 접근 허용.

(Example)

미리 서명된 URL을 통해, 특정 자원에 대해 일시적으로 접근 가능하도록 설정합니다.

[Sample Request] AWS CLI를 이용해 생성

```
aws --profile={profile} --endpoint-url={endpoint} \
s3 presign s3://{bucket}/{object} --expires-in 3600
```

4 참고 사항

1 기준

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

2 설명

- 스토리지 목적에 따라 업로드, 다운로드 등의 권한을 세분화하여 적용하여야 한다. S3 API 기반 Object Storage의 경우에는 Bucket Policy를 이용하여 권한을 제어할 수 있다.
  - 예시
    1) 스토리지 객체에 관한 권한(업로드, 다운로드 등)을 세분화하여 목적에 따라 적용하여야 한다.
    2) 스토리지 권한 부여 현황에 대한 모니터링 및 주기적 검토 수행

3 우수 사례

오브젝트 스토리지의 목적에 따라 업로드, 다운로드 권한을 세분화하여 적용할 수 있습니다.

(API) S3 API 기반의 Object Storage는 Bucket Policy를 이용해서 자원에 대해 업로드/다운로드에 대한 권한을 제어할 수 있습니다.

- 스토리지 목적에 따라 업로드, 다운로드 등의 권한을 관리하여야 한다.
  - 예시
    1) 특정 계정에게 다운로드 허용
    2) 특정 계정에게 업로드 허용

(Example)

[Sample Json] – 특정 계정에게 다운로드 허용

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificIPDownload",
      "Effect": "Allow",
      "Principal": "AWS": "arn:aws:iam::123456789012:root",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::{Bucket}/*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "{IpAddress}/32"
        }
      }
    }
  ]
}
```

- "arn:aws:iam::123456789012:root" 유저에게 적용
- "s3:GetObject" Action 을 허용
- "arn:aws:s3:::{Bucket}/*" 특정 버켓 이하 경로 모두 적용
- "Condition": { "IpAddress": { "aws:SourceIp": "{IpAddress}/32" }} 필요 시 IP에 대한 접근제어 추가

[Sample Json] - 특정 계정에게 업로드 허용

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificIPUpload",
      "Effect": "Allow",
      "Principal": "AWS": "arn:aws:iam::123456789012:root",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::{Bucket}/*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "{IpAddress}/32"
        }
      }
    }
  ]
}
```

- "arn:aws:iam::123456789012:root" 유저에게 적용
- "s3:PutObject" Action 을 허용
- "arn:aws:s3:::{Bucket}/*" 특정 버켓 이하 경로 모두 적용
- "Condition": { "IpAddress": { "aws:SourceIp": "{IpAddress}/32" }} 필요 시 IP에 대한 접근제어 추가

[Sample CLI] - AWS CLI를 통해 Bucket Policy 적용

```
aws --profile={profile} --endpoint-url={endpoint} \
s3api put-bucket-policy --bucket {bucket} --policy file://bucket-policy.json
```

4 참고 사항

1 기준

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

2 설명

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

3 우수 사례

(API) S3 API 기반 Object Storage의 경우에는 업로드 가능 파일을 제한할 수 있습니다.
PUT Bucket Policy를 통해 원하는 파일 유형의 확장자를 가진 객체에만 s3:PutObject 작업을 허용하거나 거부합니다.

(Example)
예시로 아래 버킷 정책을 사용하면 .jpg, .png 또는 .gif 파일 확장자를 가진 객체에 대해서 s3:PutObject 작업을 거부할 수 있습니다.

[Sample Request]

```
{
  "Version": "2012-10-17",
  "Id": "MyBucketPolicy",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*.jpg",
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*.png",
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*.gif"
      ]
    }
  ]
}
```

8. 백업 및 이중화 관리

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

8 백업 및 이중화 관리

1 기준

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

2 설명

- 금융회사가 클라우드 이용 시 발생하는 다양한 행위추적성 증적에 대해 백업을 수행(1년이상 보관) 하여야 한다.
  - 예시
    1) 스토리지 서비스를 별도로 생성 및 연동하여 행위 감사로그 백업
    2) 클라우드 웹 콘솔 내 행위 감사로그를 별도의 파일 형태로 다운로드 하여 별도로 보관 등

3 우수 사례

클라우드 행위추적성 로그에 대한 백업저장을 위해 스토리지 서비스를 이용할 수 있으며, 스토리지 서비스중 Object Storage 서비스 기반으로 기술하겠습니다.

Object Stroage 서비스는 파일시스템이 아니므로 Restful API나 별도의 지원 툴을 통해 접근하며 실시간 데이터보다는 장기간 보관하는 데이터 저장에 더욱 적합합니다.

Object Storage 서비스 이용절차는 다음과 같습니다.

- 웹 콘솔 접속 후 Object Storage 〉 Storage 3.0 관리

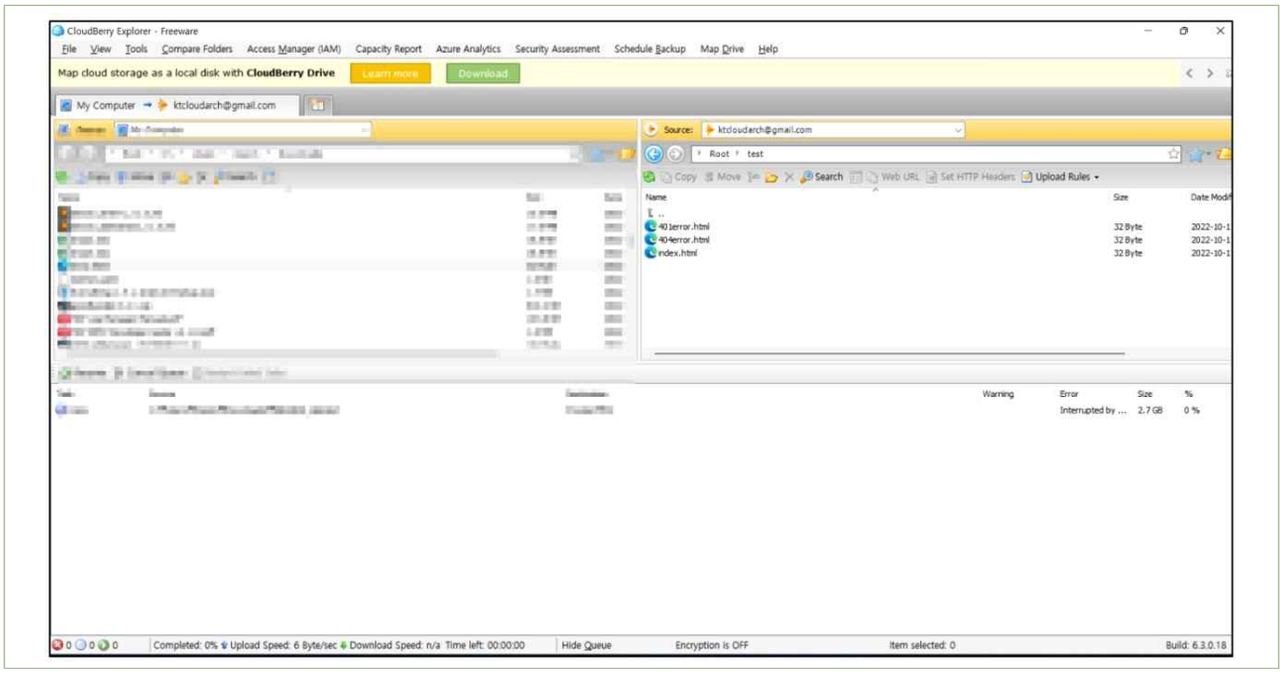
| 그림 8-1-1 | Object Storage 〉 Storage 3.0 관리

- 파일박스 생성 버튼 클릭, 파일박스 이름을 작성 후 파일박스 생성을 클릭합니다.
- 파일박스가 생성되면 Storage 관리화면 상단 파일리스트 기능을 이용해 아래와 같이 해당 파일박스에 대한 파일리스트를 확인할 수 있습니다

| 그림 8-1-2 | 파일 박스 리스트 확인

해당 파일박스에 백업파일의 업로드/다운로드는 Restful API 및 접속 툴을 통해 가능합니다.

Storage 접속 툴 이용 시 Cyberduck, CloudBerry등의 프리웨어 클라이언트 프로그램 사용이 가능하며 관련 설치방법은 4. 참고사항 항목의 관련 링크를 참고해 주시기 바랍니다.



| 그림 8-1-3 | CloudBerry 사용 예시

4 참고 사항

- Object Storage 관련 툴 사용 안내 : https://manual.cloud.kt.com/kt/storagecdn-storage-tool

1 기준

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

2 설명

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

3 우수 사례

kt cloud Backup 시스템 자체적으로 데이터 무결성을 검증하는 기능은 제공되지 않습니다.
고객의 데이터를 백업 받는 방식은 Client OS 내 암호화된 Token 인증 방식을 통하여 고객 Data 원본 그대로 복사·저장하는 구조입니다.
백업 저장 시 Hash 값을 생성하여 고객 Data를 백업 받는 방식이 아니므로, Hash 값을 별도 데이터 형태로 백업 수행 후 복구하여 무결성 하는 방향으로 이용하는 것을 권장 드립니다.

- **고객 무결성 검증 프로세스** (무결성 검증은 고객이 아래 절차에 따라 직접 수행해야 함)
  1. **데이터 복구 신청**: 고객이 클라우드 콘솔에서 복구 요청
  2. **데이터 복원 수행**: KT Cloud에서 고객사 복구 디렉토리로 데이터 Restore
  3. **무결성 검증**: 고객이 복구된 데이터를 기준으로 무결성 및 정합성 확인

| 그림 8-2-1 | **데이터 복구 수행 절차**

통신 채널에 대한 보안은 아래와 같이 제공됩니다.

- NetBackup Appliance 보안 구성
- TLS 기반으로 클라이언트 ↔ 서버 간 통신 암호화
- 각 NetBackup 컴포넌트는 신뢰된 CA(Certificate Authority) 인증서, 자체 서명(Self-signed) 인증서를 통해 상호 인증을 수행합니다.

1 기준

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

2 설명

- 금융회사 클라우드 이용 시 관련 법령(전자금융거래법, 전자금융감독규정 등)에 따라 백업이 필요한 전산자료에 대해서는 백업을 수행하여야 하며, 중요업무인 경우 클라우드 서비스와 관련한 중요 설정파일 및 가상 시스템 이미지도 백업 대상에 포함하여야 한다(중요도에 따라 1년이상 보관).
  - 예시
    1) 클라우드 서비스 제공자가 제공하는 백업 서비스 이름
    2) 전산자료를 별도로 다운받아 금융회사가 관리하는 백업 서버내 보관

3 우수 사례

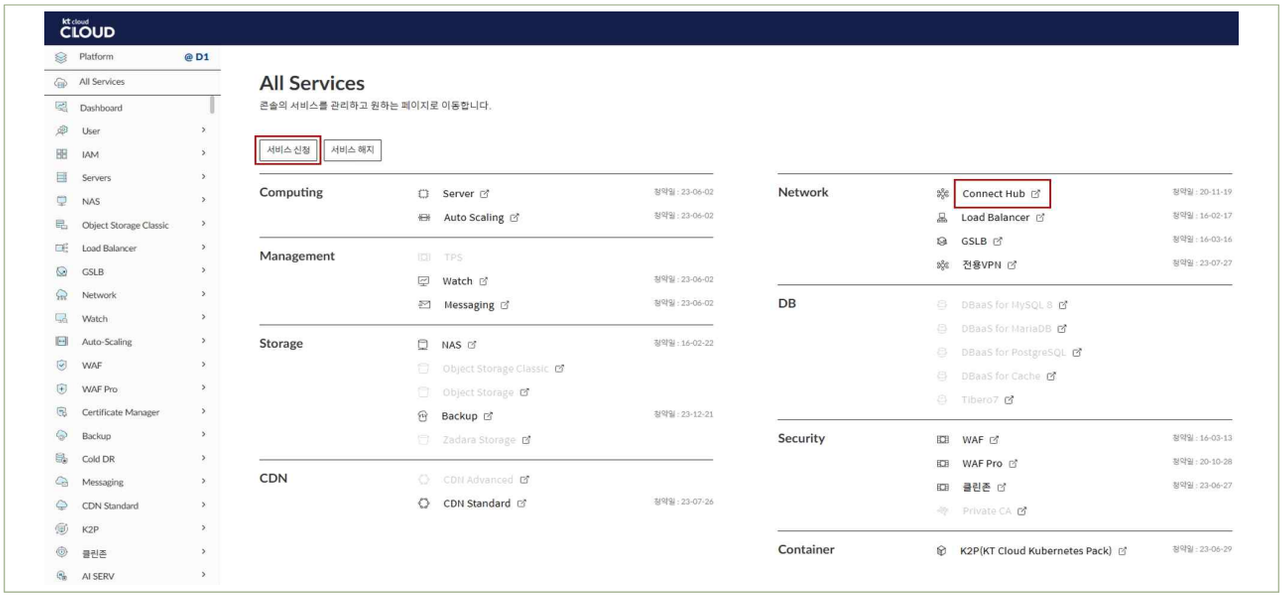
기본적으로 kt cloud에서 제공하는 백업 서비스는 IaaS 가상환경 내 보관 방식이 아닌 백업 전용서버 저장소에 보관/운영되고 있습니다.
기본적인 IPS, IDS 보안 기능과 랜섬웨어 대응이 가능한 Hardening 기술이 적용되어 고객 중요 Data 자산을 암호화 적용되어 보관합니다.
백업 수행을 위한 환경 구성 시 백업 정책 신규 신청부터 이후 정책 변경/삭제/복구에 대한 모든 기능들은 kt cloud 사용자 콘솔에서 이용이 가능합니다. 아래 매뉴얼과 같이 백업서버 간 N/W 연동 후 Backup 인프라 환경 구성을 완료합니다.
이후 고객이 요구하는 정책 기반으로 Scheduler 기능을 통한 자동화 백업 수행을 제공합니다. (G1/G2, D1 플랫폼 모두 제공)

1.1 백업 신청 전 사전 N/W 구성 및 백업 서버간 연동

① kt-cloud D1 or G1/G2 플랫폼에서 Backup 서비스를 이용하기 위해서는 Connect Hub 상품 신청 및 백업서버 간 연동이 필요합니다.

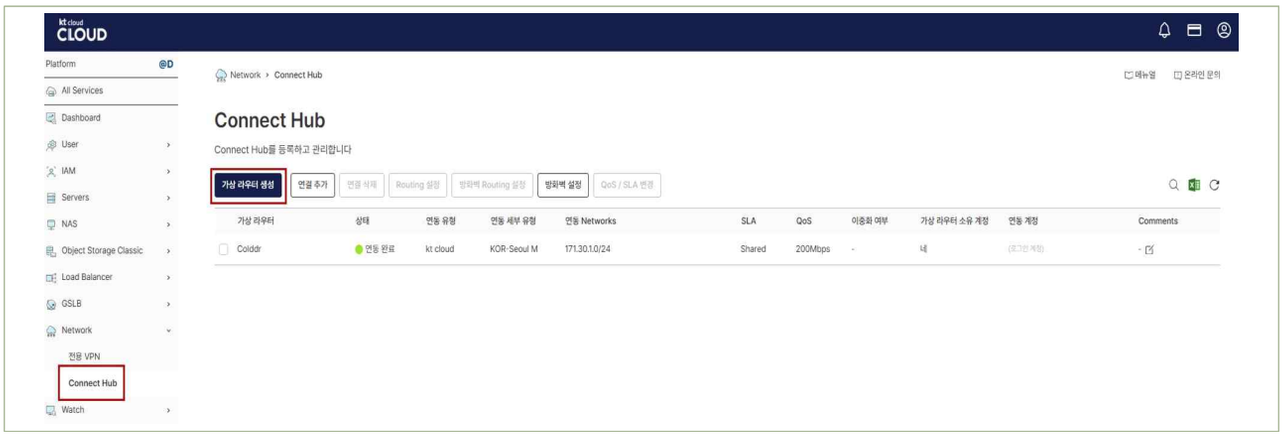
② (콘솔) ‘Network’ ➔ ‘Connect Hub’ 신청 메뉴에서 신청하실 수 있으며, G1/G2 플랫폼 이용 고객은 신청 서 다운로드 후 ‘Backup 서비스 이용을 위한 Connect Hub 신청’ 목적으로 신청 접수 바랍니다

D1플랫폼 이용 고객은 아래 Connect Hub 가상 라우터 생성 매뉴얼을 참고하여 신청 바랍니다.



| 그림 8-3-1 | All Service 메뉴에서 ‘Network’ 〉‘Connect Hub’ 서비스 신청

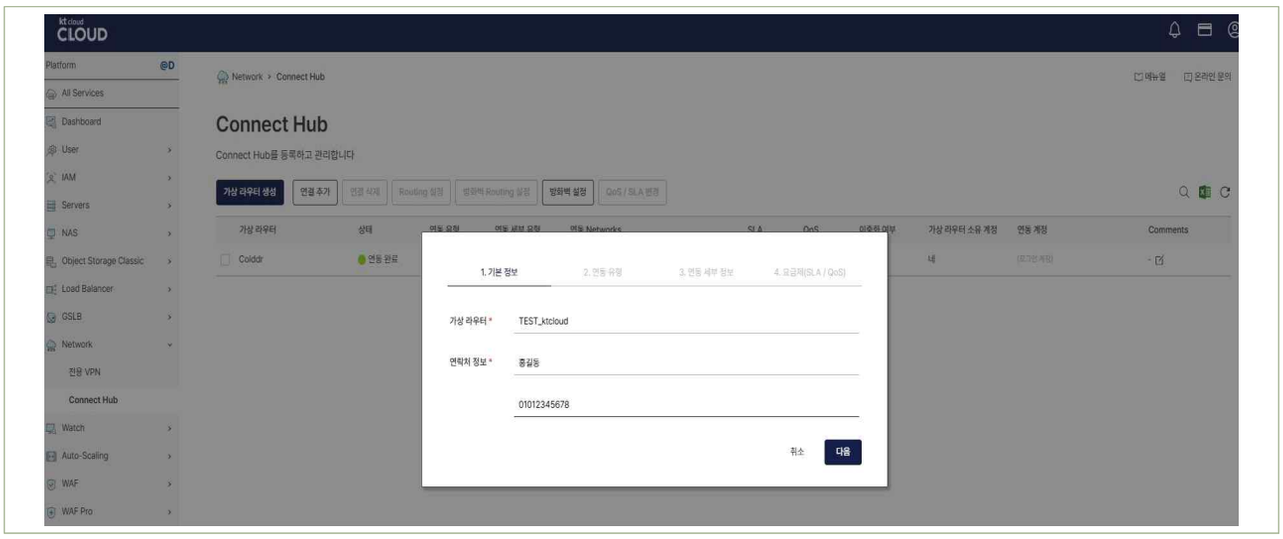
- 청약 신청 완료 후 왼쪽 메뉴에서 Connect Hub 신청 메뉴가 활성화됩니다.



| 그림 8-3-2 | Connect Hub 생성

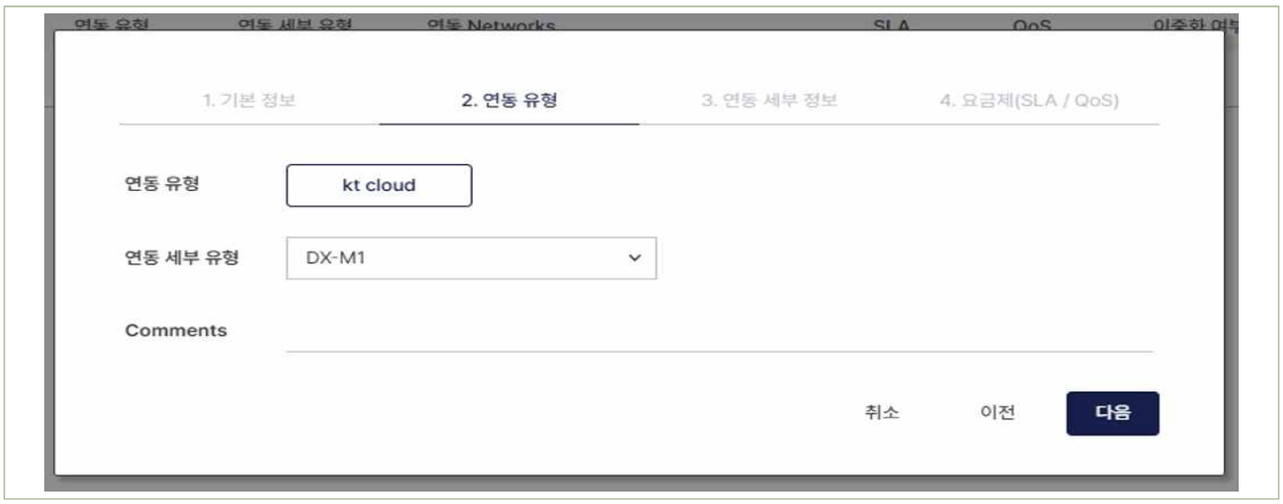
- ‘KT-Cloud 콘솔’ 〉 ‘Network’ 〉 ‘Connect Hub’ 메뉴에서 가상 라우터 생성을 통하여 연동유형에 따라 신청부터 Connect Hub IP 대역 생성 및 Routing 구성을 진행합니다.
- Backup용 Connect Hub IP 대역 할당이 필요하므로 기존에 이용 중인 Connect Hub로는

구성이 불가합니다. 따라서 별도의 Backup용 Connect Hub를 신청하여 구성이 필요합니다.



| 그림 8-3-3 | 기본 정보 입력 단계

- Connect Hub 연동에 사용할 가상 라우터의 이름과 고객 담당자/연락처를 입력합니다.



| 그림 8-3-4 | 연동 유형 입력 단계

- 연동 유형에 [kt cloud] , 연동 세부 유형에 [연동 대상 Zone] 을 선택 후 다음 단계로 이동합니다.

| 그림 8-3-5 | 연동 세부 정보 입력 단계

- 연동할 Network 선택 후 다음 단계로 이동합니다.
  * Central A/B, Seoul M/M2 위치(존)의 경우, 사전에 생성한 Connect Hub 전용 서브넷 선택
  * 타 계정 혹은 Zone의 경우 CIDR 이 서로 다른 경우에만 연동 가능
  * 기본 생성 Tier [DMZ 172.25.0.0/24, Private 172.25.1.0/24]는 연동을 권장하지 않음

| 그림 8-3-6 | 요금제 선택 단계

- 필요한 대역폭 및 SLA 선택 후 최종 신청합니다.

1.2 VM서버와 백업서버 간 1:1 NAT 구성

① D1 플랫폼 이용 고객

- KT-Cloud D1 플랫폼은 vdom을 사용하는 존으로, 백업 서버 간 연동을 위해 1:1 NAT 처리가 필요합니다.

- 생성한 C-Hub IP 대역(10.69.x.x)으로 백업 대상 서버의 사설IP와 1:1 NAT 구성을 진행합니다.
- 예를 들어 백업 대상 서버가 2대일 경우 NAT IP 할당 가능한 범위 내에서 사용하고자 하는 IP를 지정하여 (KT-Cloud 플랫폼 고객일 경우) ent-security@kt.com 메일로 1:1 NAT 처리를 신청합니다. (Ex. 10.69.200.1 ~ 2, 2EA)

※ 1:1 NAT 처리를 위한 메일내용 예시

- Connect Hub 는 C Class 대역으로 할당되므로, 1부터 254 호스트 IP범위 내에서 1:1 NAT 처리 가능합니다.

제목 : kt cloud Backup 서비스 이용을 위한 VM사설IP-Connect Hub 간 1:1 NAT 처리 신청 건

○ 기업명 : ㅇㅇ주식회사
○ 신청자 : 홍길동
○ kt cloud 이용플랫폼 : DX-M1
○ 신청유형 : 백업정책 변경
○ Connect Hub IP 대역 : 10.69.200.0
○ 1:1 NAT 지정 IP

VM서버 사설 IP 주소	1:1 NAT 요청 IP
(1) 172.25.0.169	10.69.200.1
(2) 172.25.0.150	10.69.200.2

② G1/G2 플랫폼 이용 고객

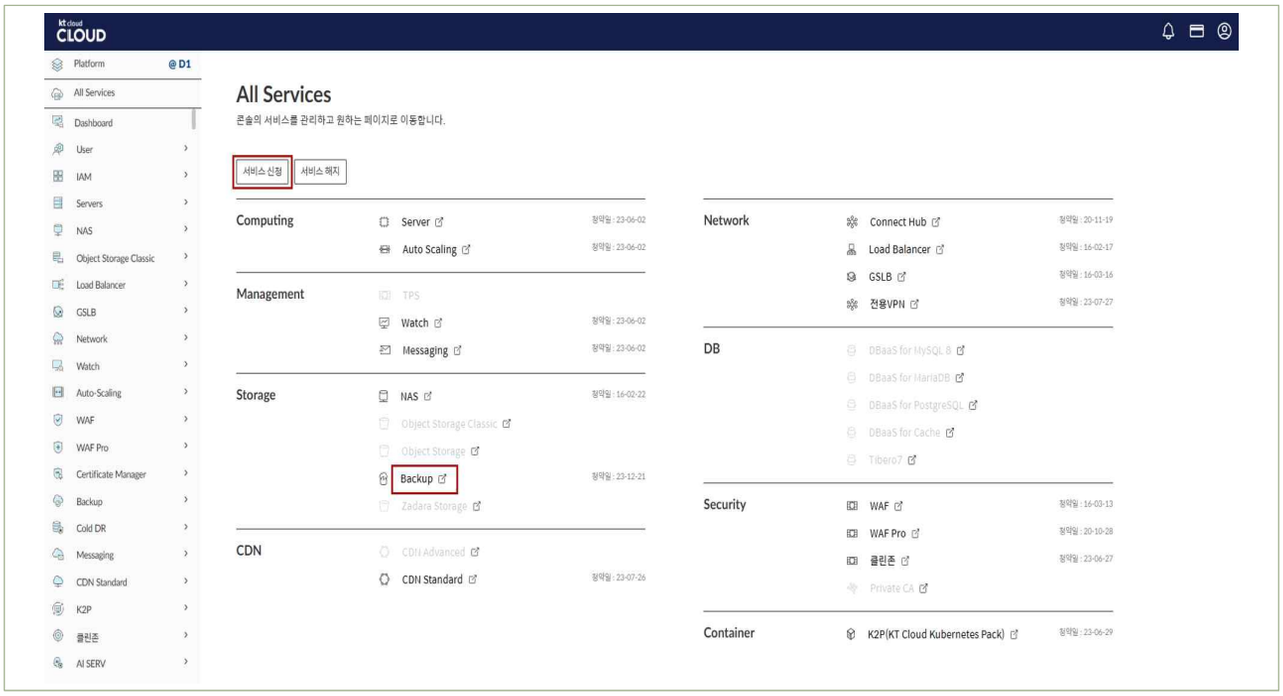
- KT-Cloud G1/G2 플랫폼은 vdom을 사용하지 않는 존으로, 기존 사용하고 있는 /24 CIP(Customer IP 로 Connect Hub 생성하여 백업 서버 간 통신하기 때문에 별도 1:1 NAT 작업 절차는 불필요합니다.

2. Backup 신청 방법

‘1번’의 N/W 구성 및 백업 서버간 연동이 완료되면 Cloud 콘솔에서 백업 신청접수가 가능합니다.

2.1 Backup 서비스 청약 신청

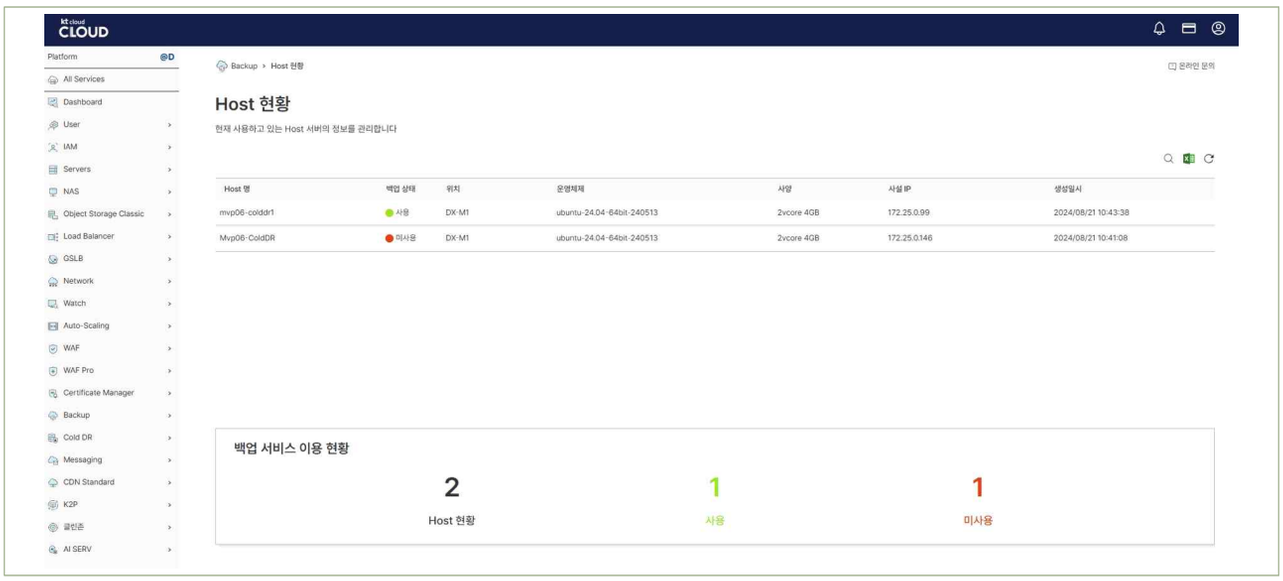
1. (콘솔) All Services 메뉴에서 ‘Storage’ ➔ ‘Backup’ 서비스 신청(청약)
2. 청약 신청 완료 후 왼쪽 메뉴에서 Backup 신청 메뉴 활성화



| 그림 8-3-7 | Backup 서비스 신청

2.2 Backup 호스트 현황

1. 콘솔 로그인 후 Host 현황 메뉴에서 보이는 내용은 현재 사용자가 이용 중인 Host 서버 정보
2. 백업 상태는 Backup 백업 사용 유무에 대한 표시



| 그림 8-3-8 | Backup 호스트 현황

2.3 포트 통신 정상여부 확인

- 아래 네모박스에 기재된 절차에 따라, 수용위치의 백업서버 IP 주소로 포트 통신 테스트를

진행합니다.

- 정상 통신이 되지 않을 경우, 아래 3가지 방안으로 후속 조치 후 다시 수행합니다.

① 본 매뉴얼에 명시된 〈2.1.3 VM서버와 백업서버 간 1:1 NAT 구성〉 단계에서 1:1 NAT 구성이 제대로 되었는지 보안관제팀 (wins.ktcloud@wins21.co.kr)에 문의합니다

② 1:1 NAT 구성이 정상적으로 되었는데도 포트 정상 통신이 안 될 경우에는, kt cloud 테크센터 (techcenter@kt.com)에 문의 접수합니다.

[TCO 포트 정상 통신여부 확인 방법]

가. DX-M1, M2 Ent, Security 등 플랫폼 이용 고객 (수용 위치 : 목동)

① 백업 서버 Host 명
- ktbaas-backup-vtl01

② 방화벽 정책 (IP/Protocol/Port)
- IP : 10.69.x.xx (Connect Hub 연동 IP)
- IP : 210.xxx.xx.x (외부망 연동 시)
- Protocol/Port : TCP 프로토콜, 1556, 13724 Port

③ TOKEN 값 : DXXXXXXXXXXXXXXX

나. Central A/B, DX-Central, DX-DCN-CJ 등 플랫폼 이용 고객 (수용 위치 : 천안)

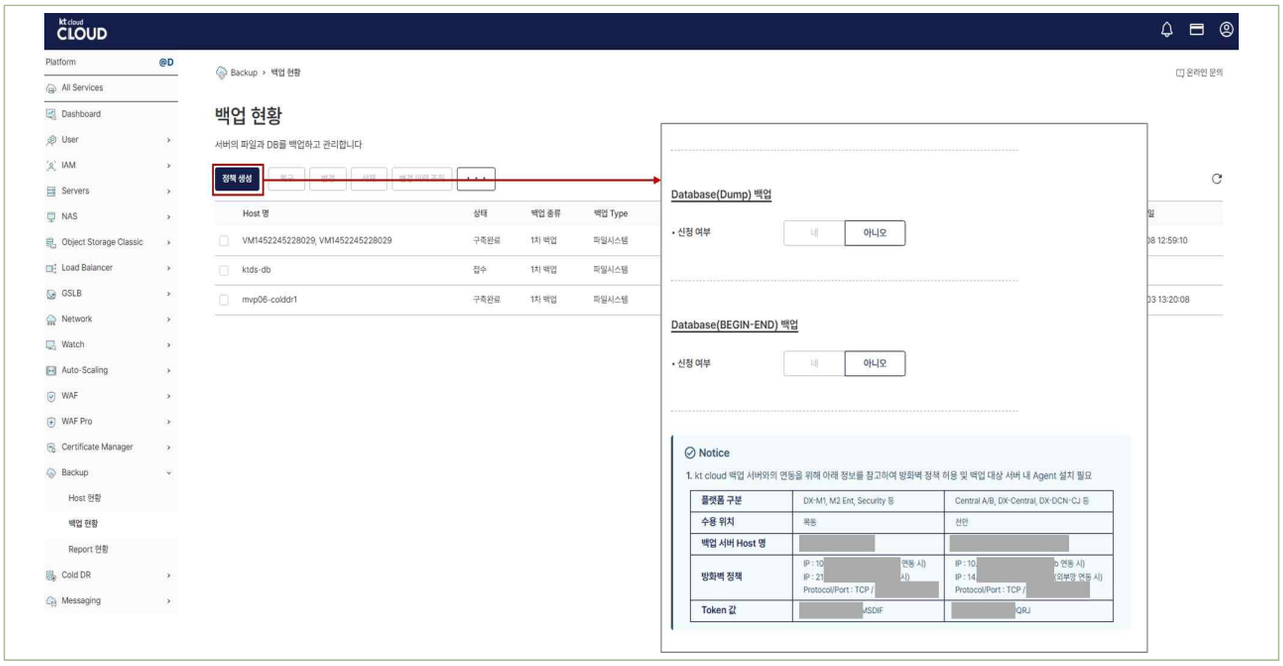
① 백업 서버 Host 명
- P-CA6-Onebackup-Master-01

② 방화벽 정책 (IP/Protocol/Port)
- IP : 10.69.xxx.xx (Connect Hub 연동 IP)
- IP : 14.xx.xxx.xx, 14.xx.xxx.xx (외부망 연동 시)
- Protocol/Port : TCP 프로토콜, 1556, 13724 Port

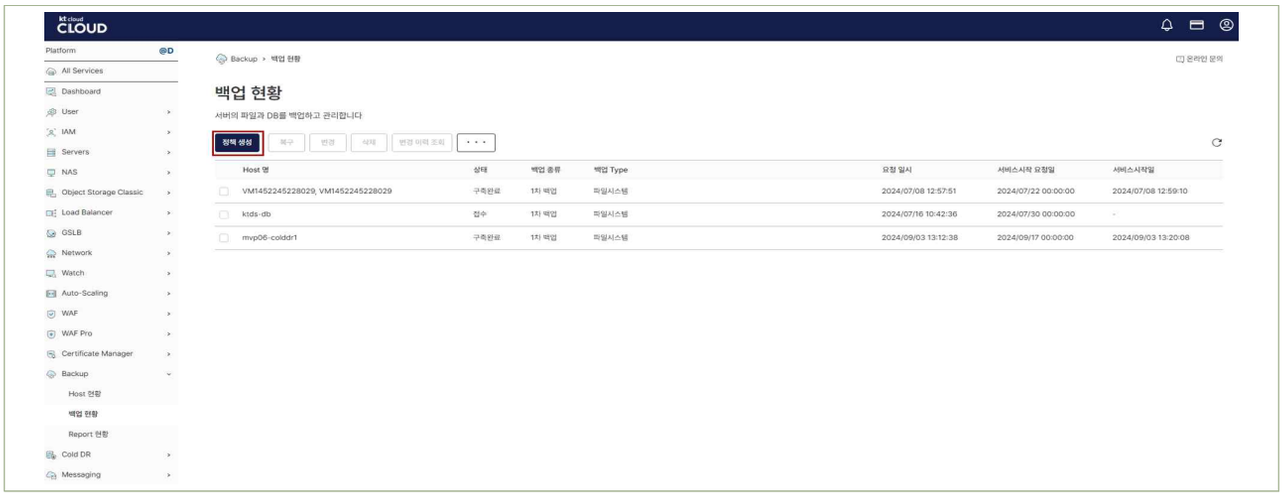
③ TOKEN 값 : NXXXXXXXXXXXXXXX

포트 통신을 위한 백업서버 IP주소 정보 및 TOKEN 값은 아래 접속경로를 통해 확인 가능합니다.

: KT-Cloud 콘솔접속 〉 All Service 〉 Backup 신청 〉 Backup 〉 백업현황 〉 '백업신청' 맨 하단 정보확인



| 그림 8-3-9 | Back up 현황



| 그림 8-3-10 | Backup 정책 신청

- 백업 신규 정책 생성을 위하여 '정책 생성' 메뉴를 클릭합니다.

※ 기본 정보 입력

- 서비스 시작 요청일 : 백업 서비스 수행 일자 선택 후 입력 (신청일 기준 2주 후부터 선택)
  * 빠른 시일 내에 백업 서비스를 수행이 필요한 경우 별도 Tech Center를 통해 접수

| 그림 8-3-11 | 파일 시스템 백업

※ 파일시스템 백업

① 신청 여부 : 파일시스템 백업 유형 서비스 필요 시 선택

② Zone : 이용 중인 kt G-Cloud 플랫폼 중 백업을 희망하는 플랫폼 선택

③ Host 명 : 고객 계정에 생성된 VM 선택 (백업을 희망하는 대상 VM 시스템)

④ 백업 서버 Connect-Hub IP : 백업 서버와 통신 가능한 1:1 NAT IP 입력 (IP 포맷 형태로만 입력 가능)

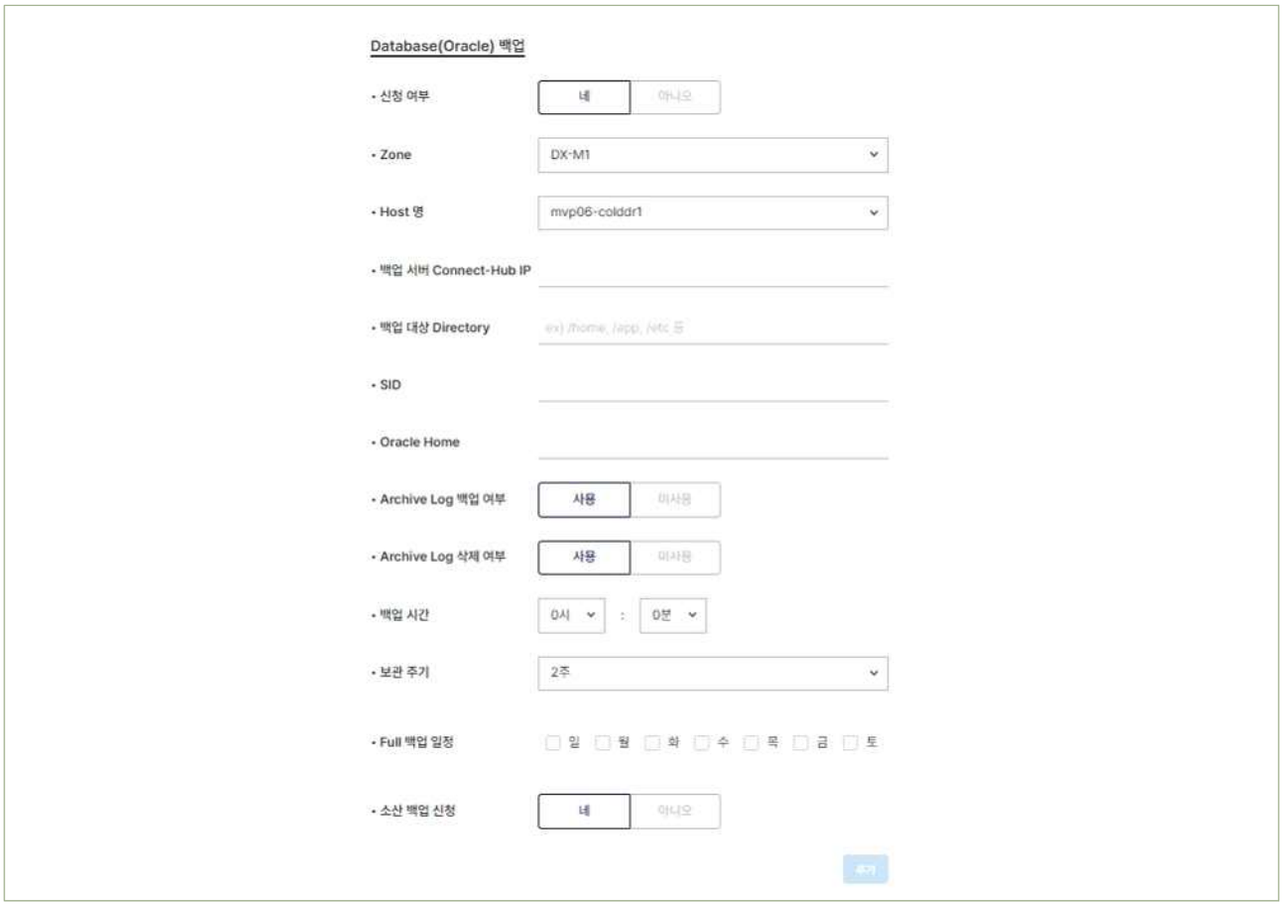
⑤ 백업 대상 Directory : VM 시스템 내 백업 대상 Directory 명 입력

⑥ 백업 시간 : 00:00~23:59 선택

⑦ 보관 주기 : 2주 Default 이며 2주, 3주, 4주, 1개월, 2개월, 3개월, 5개월, 6개월, 12개월 중 택1

⑧ FULL 백업 일정 : 콤보 박스로 다중 선택 가능
(FULL 백업 일정에 체크되지 않는 일정은 자동으로 증분 백업이 수행됩니다)

⑨ 소산 백업 신청 : 이격된 거리에 1벌 더 보관을 원할 경우 선택



| 그림 8-3-12 | Database (Oracle) 백업

※ Database(Oracle) 백업

① 신청 여부 : Database Oracle 백업 유형 서비스 필요 시 선택

② Zone : 이용 중인 kt G-Cloud 플랫폼 중 백업을 희망하는 플랫폼 선택

③ Host 명 : 고객 계정에 생성된 VM 선택 (백업을 희망하는 대상 VM 시스템)

④ 백업 서버 Connect-Hub IP : 백업 서버와 통신 가능한 1:1 NAT IP 입력 (IP 포맷 형태로만 입력 가능)

⑤ 백업 대상 Directory : VM 시스템 내 백업 대상 Directory 명 입력

⑥ SID : 사용자 입력

⑦ Oracle Home : 사용자 입력

⑧ Archive log 백업 여부 : 사용자 선택

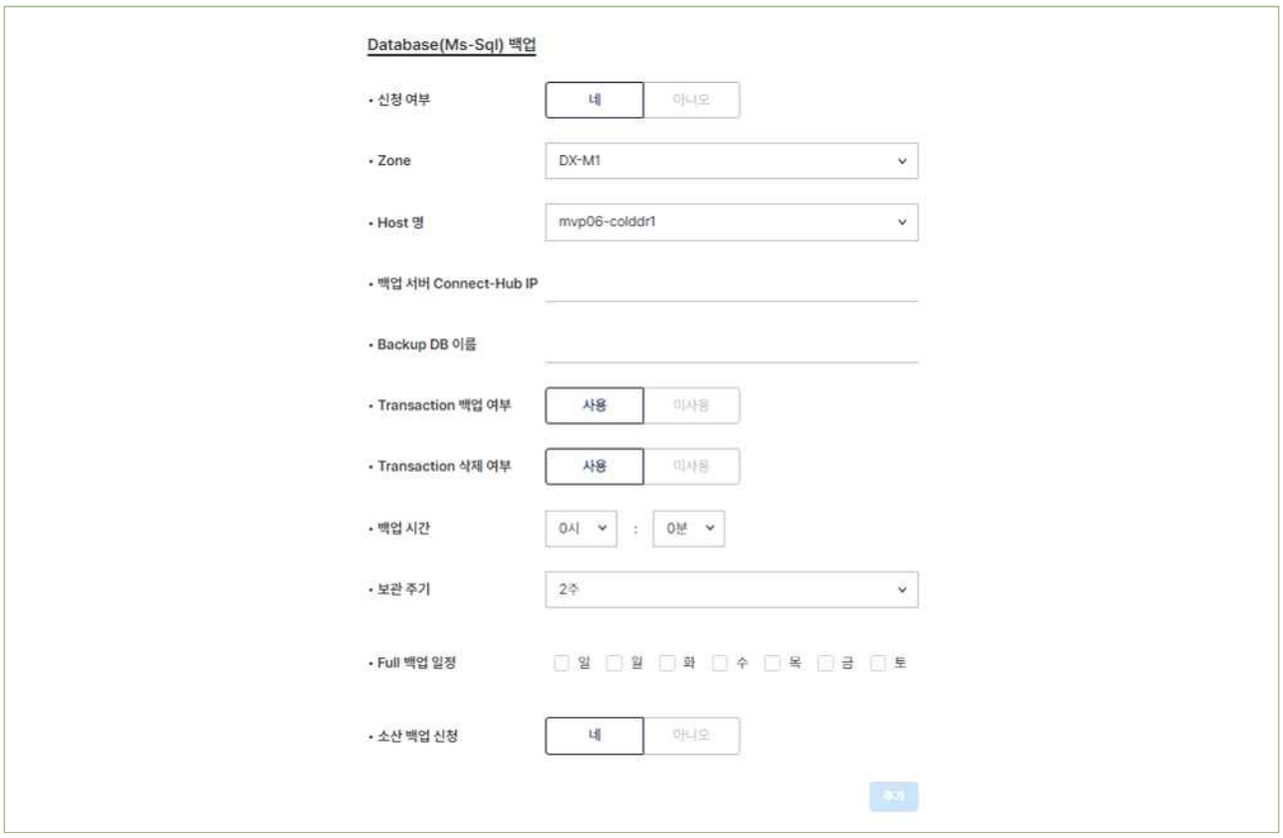
⑨ Archive log 삭제 여부 : 사용자 선택

⑩ 백업 시간 : 00:00~23:59 선택

⑪ 보관 주기 : 2주 Default 이며 2주, 3주, 4주, 1개월, 2개월, 3개월, 5개월, 6개월, 12개월 중 택1

⑫ FULL 백업 일정 : 콤보 박스로 다중 선택 가능
(FULL 백업 일정에 체크되지 않는 일정은 자동으로 증분 백업이 수행됩니다)

⑬ 소산 백업 신청 : 이격된 거리에 1벌 더 보관을 원할 경우 선택



| 그림 8-3-13 | Database(Ms-sql) 백업

※ Database(Ms-sql) 백업

① 신청 여부 : Database Ms-Sql 백업 유형 서비스 필요 시 선택

② Zone : 이용 중인 kt G-Cloud 플랫폼 중 백업을 희망하는 플랫폼 선택

③ Host 명 : 고객 계정에 생성된 VM 선택 (백업을 희망하는 대상 VM 시스템)

④ 백업 서버 Connect-Hub IP : 백업 서버와 통신 가능한 1:1 NAT IP 입력 (IP 포맷 형태로만 입력 가능)

⑤ Backup DB 이름 : 사용자 입력

⑥ transaction 백업 여부 : 사용자 선택

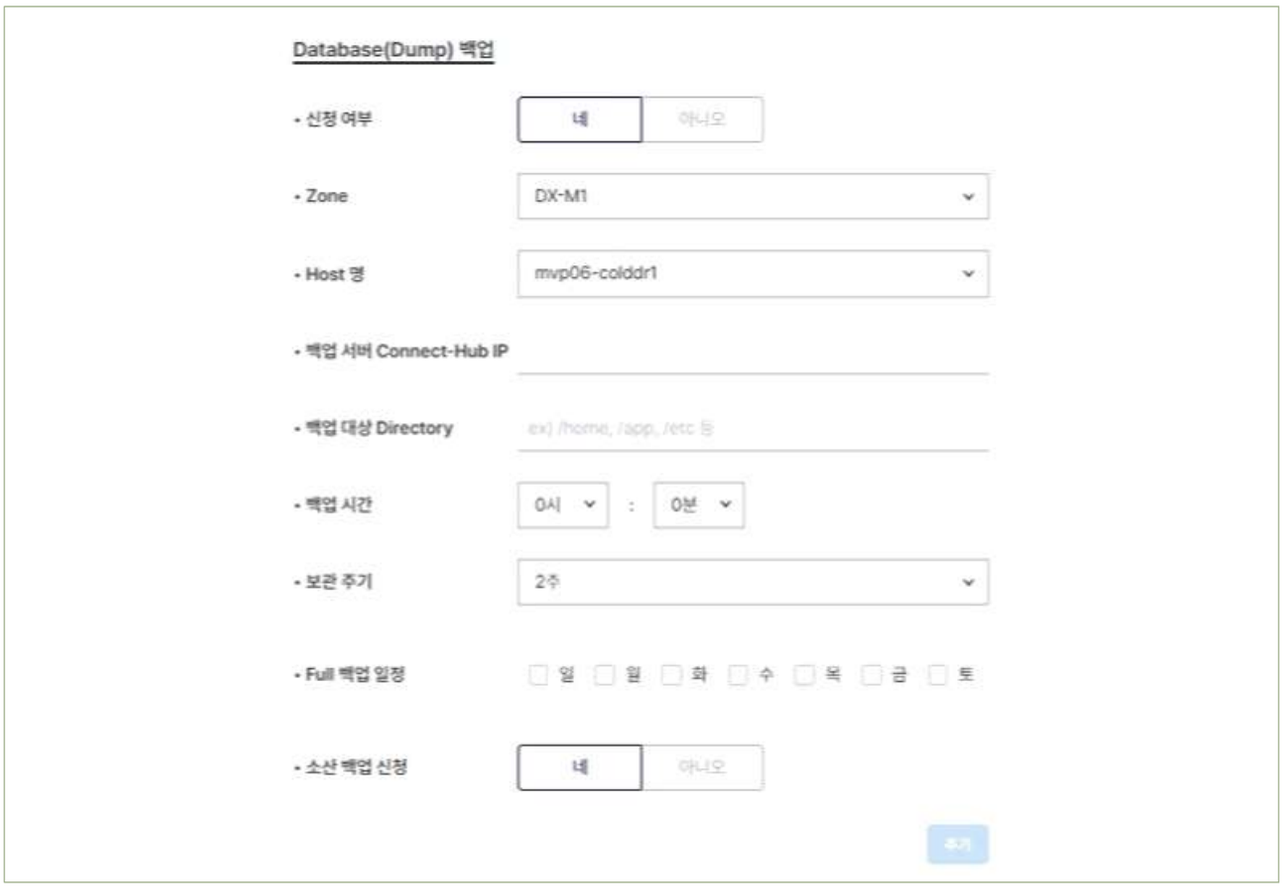
⑦ transaction 삭제 여부 : 사용자 선택

⑧ 백업 시간 : 00:00~23:59 선택

⑨ 보관 주기 : 2주 Default 이며 2주, 3주, 4주, 1개월, 2개월, 3개월, 5개월, 6개월, 12개월 중 택1

⑩ FULL 백업 일정 : 콤보 박스로 다중 선택 가능
(FULL 백업 일정에 체크되지 않는 일정은 자동으로 증분 백업이 수행됩니다)

⑪ 소산 백업 신청 : 이격된 거리에 1벌 더 보관을 원할 경우 선택



| 그림 8-3-14 | Database(Dump) 백업

※ Database(Dump) 백업

① 신청 여부 : Database DUMP 백업 유형 서비스 필요 시 선택

② Zone : 이용 중인 kt G-Cloud 플랫폼 중 백업을 희망하는 플랫폼 선택

③ Host 명 : 고객 계정에 생성된 VM 선택 (백업을 희망하는 대상 VM 시스템)

④ 백업 서버 Connect-Hub IP : 백업 서버와 통신 가능한 1:1 NAT IP 입력 (IP 포맷 형태로만 입력 가능)

⑤ 백업 대상 Directory : VM 시스템 내 백업 대상 Directory 명 입력

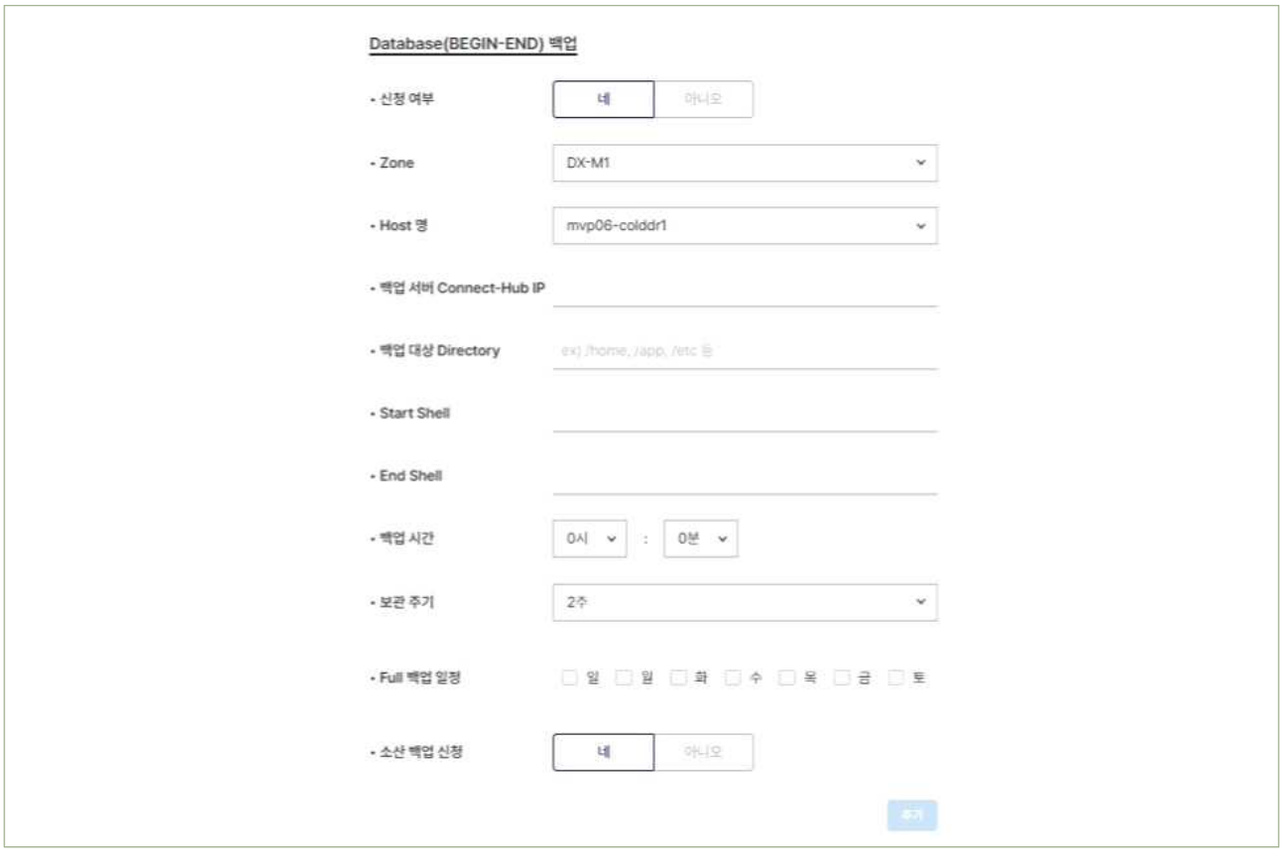
⑥ 백업 시간 : 00:00~23:59 선택

⑦ 보관 주기 : 2주 Default 이며 2주, 3주, 4주, 1개월, 2개월, 3개월, 5개월, 6개월, 12개월 중 택1

⑧ FULL 백업 일정 : 콤보 박스로 다중 선택 가능

(FULL 백업 일정에 체크되지 않는 일정은 자동으로 증분 백업이 수행됩니다)

⑨ 소산 백업 신청 : 이격된 거리에 1벌 더 보관을 원할 경우 선택



| 그림 8-3-15 | Database(BEGIN-END) 백업

※ Database(BEGIN-END) 백업

① 신청 여부 : Database BEGIN-END 백업 유형 서비스 필요 시 선택

② Zone : 이용 중인 kt G-Cloud 플랫폼 중 백업을 희망하는 플랫폼 선택

③ Host 명 : 고객 계정에 생성된 VM 선택 (백업을 희망하는 대상 VM 시스템)

④ 백업 서버 Connect-Hub IP : 백업 서버와 통신 가능한 1:1 NAT IP 입력 (IP 포맷 형태로만 입력 가능)

⑤ 백업 대상 Directory : VM 시스템 내 백업 대상 Directory 명 입력

⑥ Start Shell : 사용자 입력

⑦ End Shell : 사용자 입력

⑧ 백업 시간 : 00:00~23:59 선택

⑨ 보관 주기 : 2주 Default 이며 2주, 3주, 4주, 1개월, 2개월, 3개월, 5개월, 6개월, 12개월 중 택1

⑩ FULL 백업 일정 : 콤보 박스로 다중 선택 가능

(FULL 백업 일정에 체크되지 않는 일정은 자동으로 증분 백업이 수행됩니다)

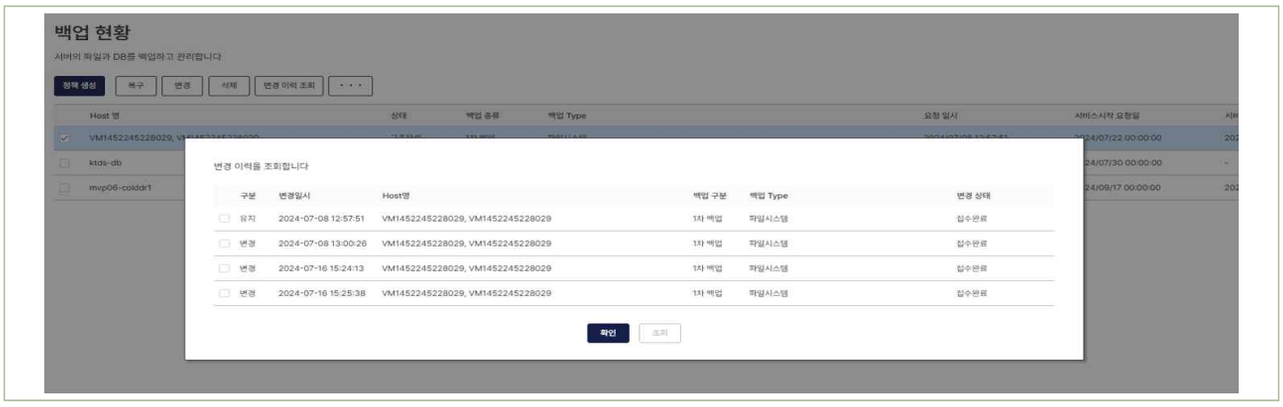
⑪ 소산 백업 신청 : 이격된 거리에 1벌 더 보관을 원할 경우 선택

| 그림 8-3-16 | 백업 현황 조회

① 백업 신청이 완료되면 위와 같이 접수된 내용이 표시됩니다.

② 사용자는 백업 대상 서버에 Agent 설치 진행이 완료가 되면 백업 운영 관리자는 최종 통신 확인 및 이상이 없을 경우 수용을 진행합니다.

③ 최종적으로 정상적인 서비스가 진행되고 난 이후 사용자에게 수용 완료 안내 알림 메일을 발송합니다. (수용 진행 상태는 접수, 검토 중, 구축 중, 구축완료 네 가지로 분류됩니다.)



| 그림 8-3-17 | 신청 이력 조회

① 사용자는 신청이력조회 기능 등을 이용하여 신청한 백업 신규 신청 및 복구/변경 삭제 내역에 대해 확인 및 관리가 가능합니다.

| 그림 8-3-18 | 일단위 Reporting 제공

① 일단위로 수행된 백업 정책 수행 결과는 'Backup' 〉 'Report 현황' 메뉴에서 확인 가능합니다.

4 참고 사항

1 기준

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

2 설명

- 금융회사의 전산자료 백업파일은 무결하게 보관하여야 한다.
  - 예시
    1) 클라우드 서비스 제공자가 제공하는 스토리지로 백업하는 경우 스토리지 내 파일이 훼손될 시 알람을 받을 수 있도록 설정
    2) 금융회사가 운영하는 백업 서버로 백업하는 경우 무결하게 보관

3 우수 사례

kt cloud Backup 서비스는 고객의 데이터를 Client OS 내 암호화된 Token 인증 방식을 통하여 고객의 데이터를 원본 그대로 복사 및 저장합니다. 백업 저장 시 Hash 값을 생성하여 고객 Data를 백업 받는 방식이 아니므로, Hash 값을 별도 데이터 형태로 백업 수행 후 복구하여 무결성 하는 방향으로 이용하는 것을 권장 드립니다.

- **아래 절차에 따라 무결성 검증 수행이 가능합니다.**
  - **데이터 복구 신청**: 고객이 클라우드 콘솔에서 복구 요청
  - **데이터 복원 수행**: KT Cloud에서 고객사 복구 디렉토리로 데이터 Restore
  - **무결성 검증**: 고객이 복구된 데이터를 기준으로 무결성 및 정합성 확인

| 그림 8-4-1 | 데이터 복구 수행 절차

4 참고 사항

1 기준

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

2 설명

- 행위추적성 증적 및 전산자료 등 백업시 백업내역을 기록하고 관리하여야 한다.
  - 예시
    1) 백업대상, 백업주기, 백업담당자 등 정책 수립
    2) 주기적으로 백업 정상여부에 대한 모니터링 및 검토

3 우수 사례

kt cloud 백업 및 복구 서비스는 해당 정책의 희망 백업시간에 자동화 백업이 수행/보관되며 장애가 발생하게 되면 신속한 복구 서비스를 제공합니다.
백업내역에 대한 정책 수행 기록/결과에 대한 이력은 kt cloud 콘솔을 통하여 고객이 직접 확인하고 수행된 결과에 대해 보고서 형태로 일단위로 제공합니다.

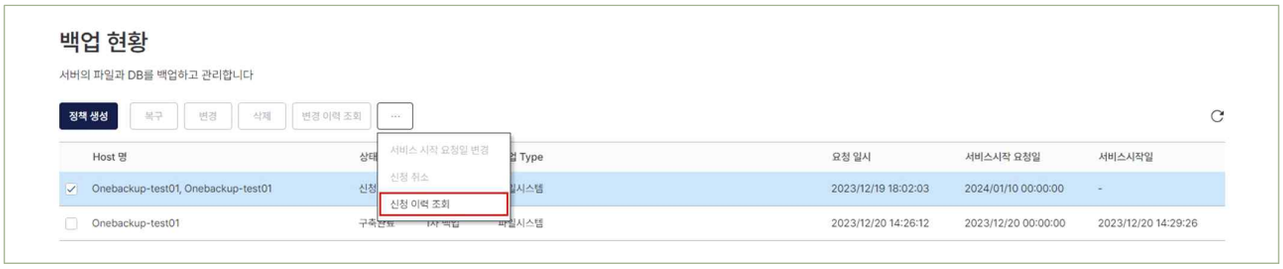
백업 수행 정책/이력 관리 및 일단위 보고서 제공 구성은 아래 기준으로 제공합니다.

- **백업 정책 (Default)**

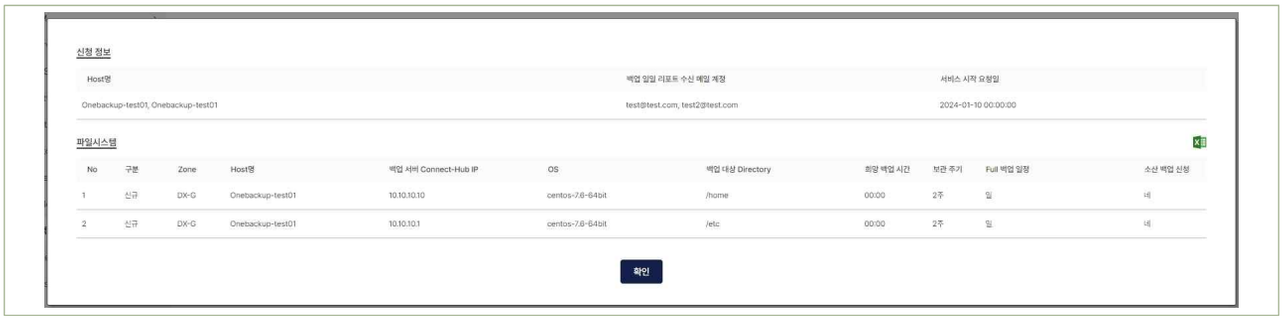
  1. 백업 수행 주기 : 주 1회 Full Backup
  2. 보관 주기 : 최소 2주부터 최대 1년 까지 제공

- **백업 정책 변경 이력 조회/관리**

  (콘솔) Backup ➔ 백업현황 ➔ 백업신청 check ➔ 변경이력 조회



| 그림 8-5-1 | 백업 현황

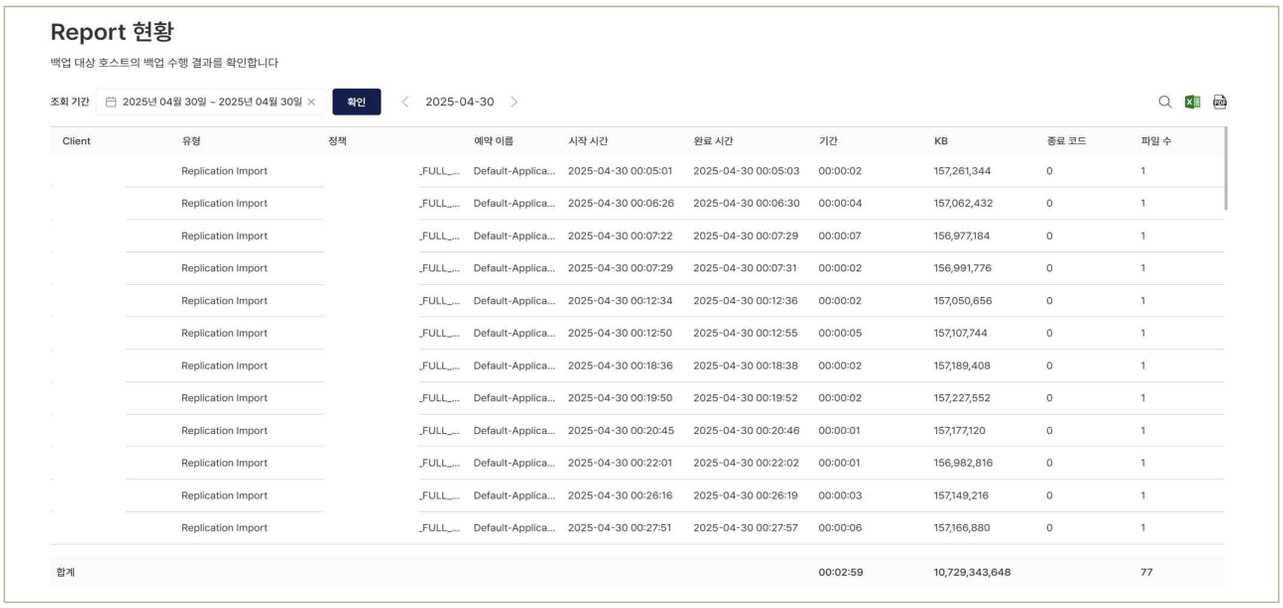


| 그림 8-5-2 | 백업 신청 이력 조회

백업 서비스 이용 중 정책 변경이나 삭제, 복구 서비스를 이용한 이력 확인을 위해서는 Cloud 사용자 콘솔에서 이력 조회 기능을 통하여 확인이 가능합니다.

백업 수행 결과 Report 현황

(콘솔) Backup ➔ Report 현황 ➔ 조회 기간 선택 ➔ 수행결과 확인을 통해 백업 수행 결과를 확인이 가능합니다.



| 그림 8-5-3 | 백업 수행 결과 Report 현황

4 참고 사항

1 기준

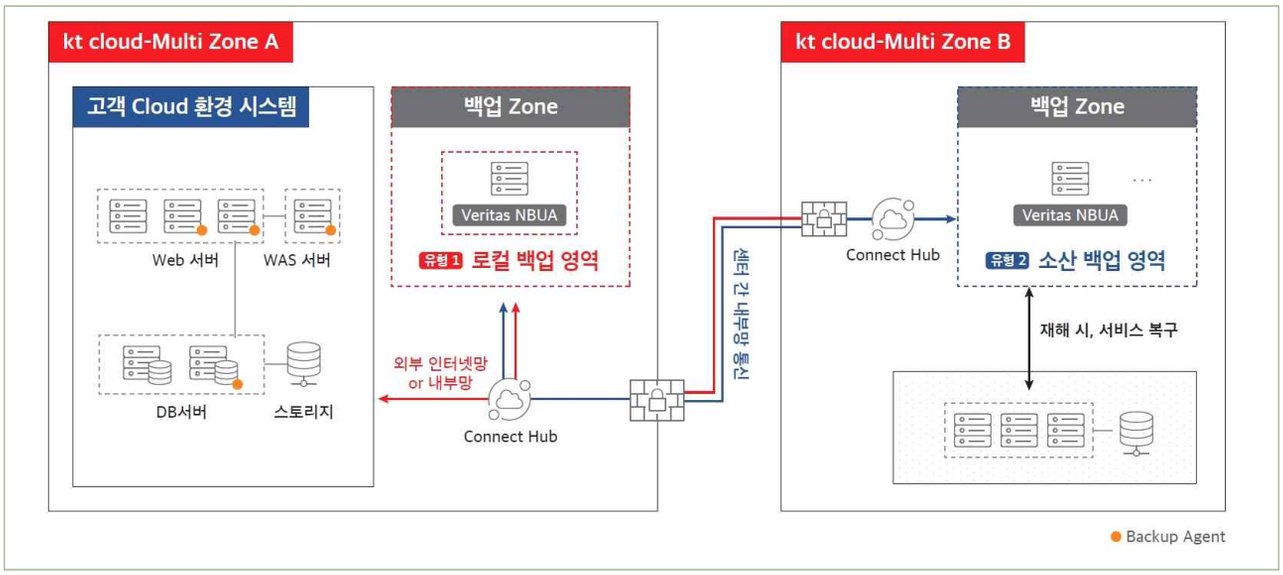
식별번호	기준	내용
8.6.	백업파일 원격 안전지역 보관	금융회사는 전산자료 등 중요도에 따라 중요도가 높은 파일에 대해선 원격 안전지역에 소산하여 보관하여야 한다.

2 설명

- 금융회사는 중요도에 따라 전산자료 등 중요도가 높은 파일에 대해서는 원격 안전지역에 소산하여 보관하여야 한다.
  - 예시
    1) 클라우드 서비스 제공자의 DR 서비스 이용
    2) 금융회사 자체 데이터센터로 소산하여 보관 등

3 우수 사례

kt cloud 에서는 기본적으로 고객 Cloud 환경 내 백업 대상 시스템(File, Database)에 대해 안정적인 로컬 백업 환경 구성을 제공하고 있으며, 파일 손상/유실 또는 재해 재난 사태 발생 대비를 위하여 50km 거리 이상 이격된 DR센터 내 2차 소산 백업 구성을 지원합니다.



| 그림 8-6-1 | 로컬/소산 백업 구성도

Backup 서비스를 신청 중 '소산 백업 신청'을 체크 후 신청하실 경우 50km 거리 이상 이격된 DR 센터 내 2차 소산 백업을 제공합니다.

소산백업 신청 : (콘솔) Backup ➔ 백업현황 ➔ 정책 생성 ➔ 백업유형 별 소산 희망 시 체크 후 신청

- **Managed 서비스**

전문 백업 인력 기반 Full Managed 서비스 제공으로 운영 비용 절감

정상 백업 수행 여부 등 기업의 백업 운영 정책 현황에 대해 일일 리포트 제공

백업 자동화 정책 설정, 백업 모니터링, 데이터 백업 및 복구 수행 대행

4 참고 사항

1 기준

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

2 설명

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

  - 예시

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

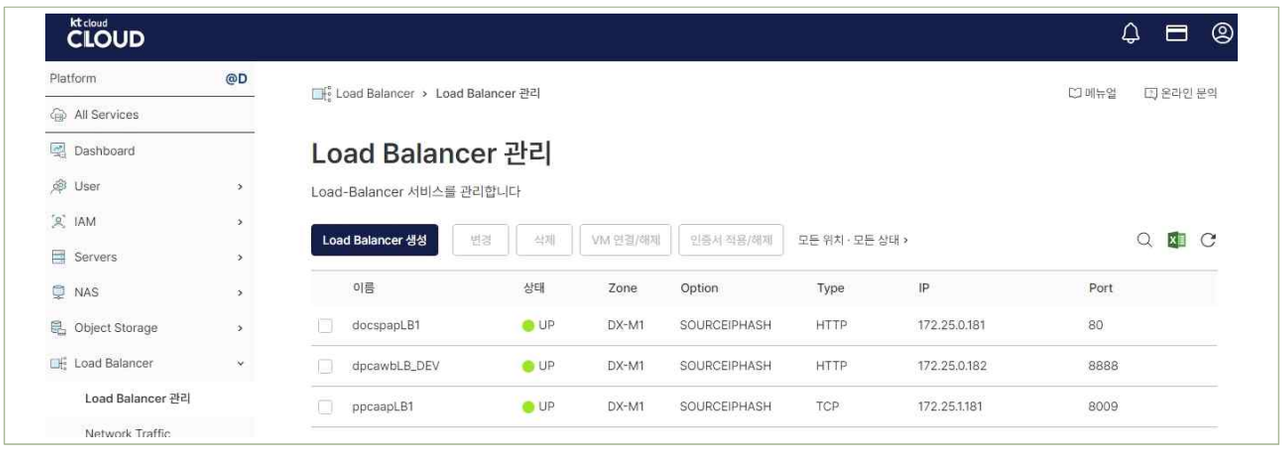
    2) 이중화 구성 시 원격 안전지역 등을 고려

3 우수 사례

웹서버 등 서버의 이중화 구성 시 Load Balancer를 이용하여 구성할 수 있습니다. Load Balancer를통하여 클라이언트의 요청을 단일서버에서 처리하지 않고 서버간 트래픽을 분산하여 가용성을 확보하고 응답시간을 최적화할 수 있습니다.

Load Balancer는 서버의 앞 단에 위치하여 클라이언트의 요청을 수신하면 고객 서비스 영역안에 있는 가상서버(VM)로 분산하여 정보를 처리할 수 있도록 합니다.

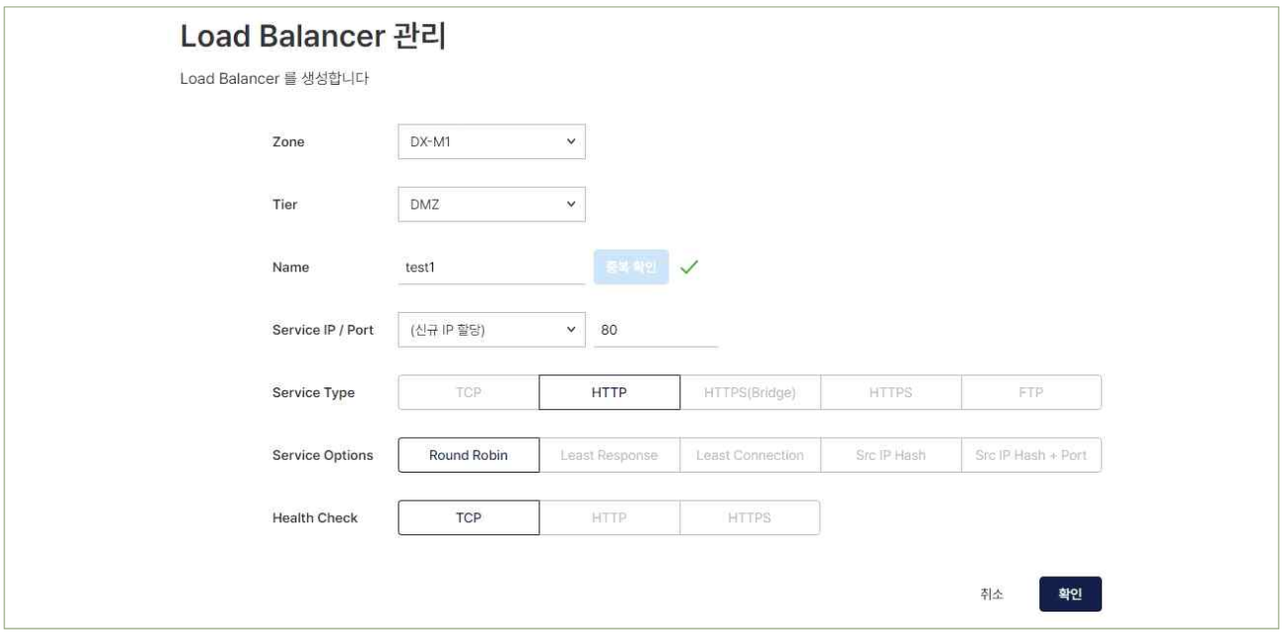
웹 콘솔 접속 Load Balancer 〉 Load Balancer 관리화면에서 Load Balancer 생성을 클릭합니다.



| 그림 8-6-1 | Load Balancer 관리

- Load Balancer 생성 팝업에서 다음 항목을 입력합니다.

1. Zone : LB(Load Balancer) 생성을 위한 대상 존 선택(기존 서버 위치)
2. Tier: LB 생성할 Tier 선택(DMZ/Private/Dev 등)
3. Service IP/Port : 신규IP할당을 선택하여 LB에 사용할 공인IP를 할당, 80/443등 사용포트 입력
4. Service Type : back-end에서 구동되는 서비스 특징에 따라 LB 타입을 지정
   - HTTP : SSL인증서를 사용하지 않는 일반 웹 서버와의 통신을 수행
   - HTTPS(bridge) : SSL인증서는 back-end 서버에 고객이 직접 설치하여 사용, 클라이언트와 웹서버가 ent-to-end로 암호화 통신 수행. LB는 패킷을 바이패스 전송, 웹서버는 CIP 구분불가
   - HTTPS : SSL 인증서를 LB에 설치하여 클라이언트와 LB 구간에서 암호화 통신 수행. LB는 트래픽 복호화 후 back-end 서버로 포워딩함
5. Service Options : 로드밸런싱 방식(알고리즘)을 선택
6. Health Check : back-end 서버의 정상 동작 여부를 확인, HTTP/HTTPS 선택시 유효한 웹페이지주소를 입력해야 함



| 그림 8-6-2 | 로드밸런서 관리

Load Balancer가 정상적으로 생성되었다면 관리 화면에서 목록을 조회할 수 있습니다. 처음 생성시에는 Load Balancer의 상태가 Down으로 표시되며 VM연결 후에는 UP으로 변경됩니다.

Load Balancer 〉 Load Balancer 관리 화면 상단의 VM 연결/해제 버튼을 클릭하여 Load Balancer와 VM을 연결합니다. 팝업화면에서 해당 Tier 및 서버를 선택 및 public port를 입력 후 추가 버튼을 클릭합니다.

4 참고 사항

금융분야 상용 클라우드컴퓨팅서비스 보안 안내서 (KT Cloud)

발 행 일	2026년 8월
발 행 인	금융보안원(원장 박상원)
공 동 발 행 인	KT Cloud
금 융 보 안 원	
클라우드대응부	부장 유재필
클라우드기획팀	팀장 장지현 차장 안성현 대리 최주섭
발 행 처	금융보안원 02-3495-9000 경기도 용인시 수지구 대지로 132

〈비 매 품〉

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

금융분야
상용 클라우드컴퓨팅서비스 보안 안내서