업무참고 2025-클라우드대응-②-63

금융분야
상용 클라우드컴퓨팅서비스 보안 관리 참고서

삼성SDS

금융보안원
FINANCIAL SECURITY INSTITUTE

SAMSUNG SDS

CONTENTS

1. 가상자원 관리

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

1 가상자원 관리

1 기준

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

2 설명

- 이용자 가상자원에 접근하는 계정에 대한 비밀번호 규칙 보안통제 방안을 수립하여야 한다.

  - 예시

    1) 제3자가 쉽게 유추할 수 없는 비밀번호 작성 규칙 수립

3 우수 사례

1) 제3자가 쉽게 유추할 수 없는 비밀번호 작성 규칙 수립

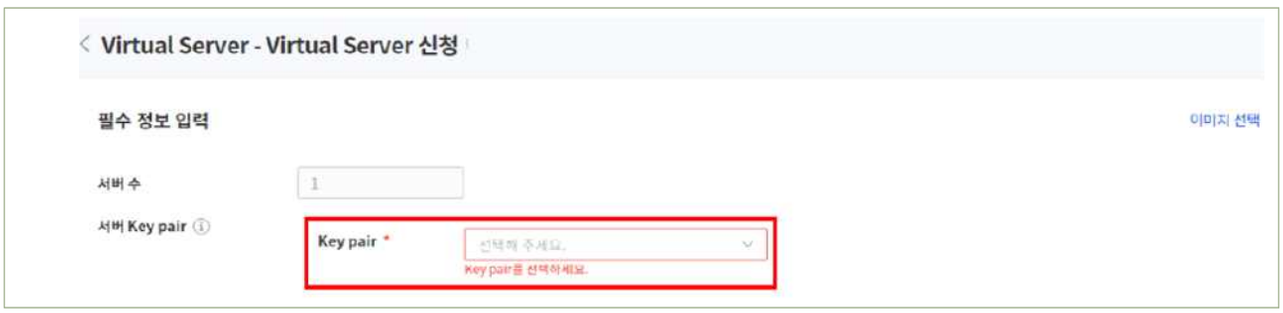
- 가상자원 생성 간 최초 OS 접속은 Key Pair를 활용하며 안전하게 접속할 수 있으며 최초 OS 접속 계정에 대한 개별 비밀번호 설정 불필요

  ① Key pair 신청: 서버 Key pair명 입력→ 완료→ .pem파일 다운로드

| 그림 1.1.1 | 서버 Key pair 신청

② Key Pair를 통한 가상자원 생성

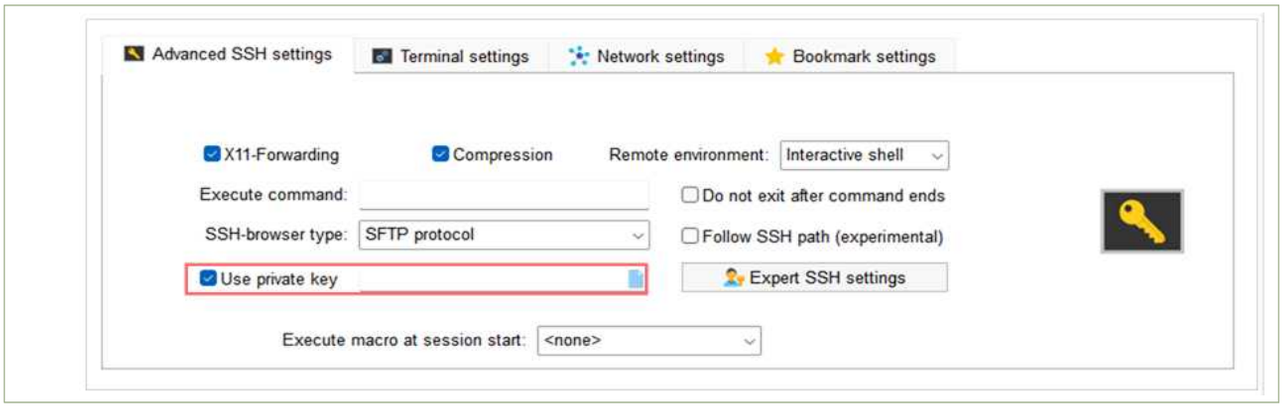
- 신청 경로: Project → 자원관리 → Compute → Virtual Server → Virtual Server → 상품 신청 → 이미지 선택 → 상품구성 선택 및 입력 → 필수정보 입력화면의 Key pair 신규 생성 또는 기존 Key pair 선택



| 그림 1.1.2 | Virtual Server 신청

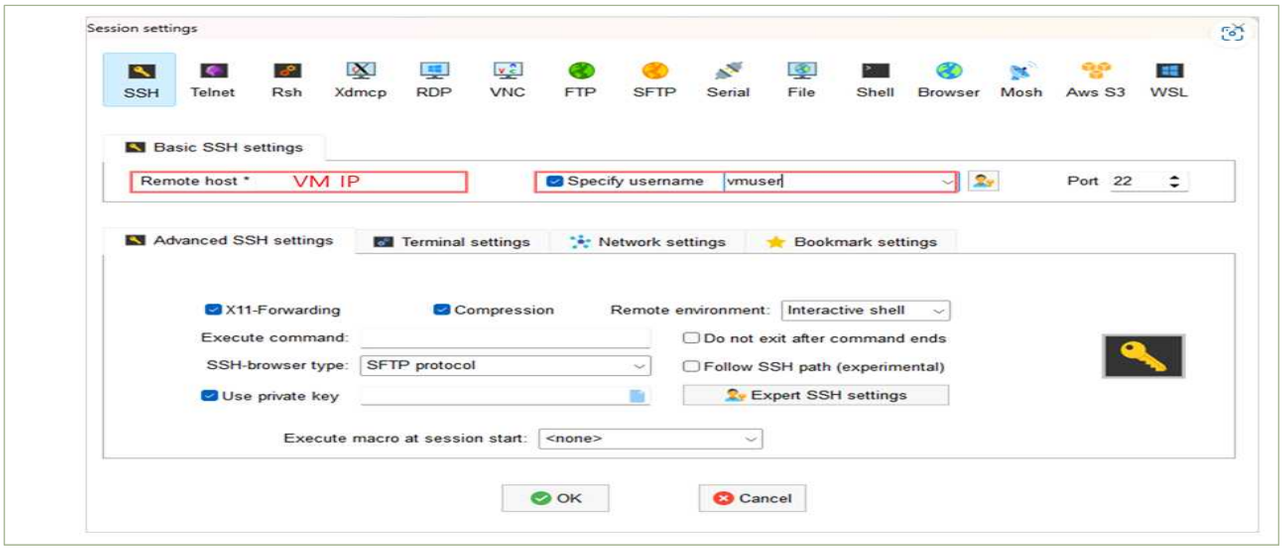
③ Key Pair를 통한 가상자원 접속 (ex. mobaXterm 활용)

- mobaXterm을 실행한 후, Session settings 화면으로 이동
- Advanced SSH settings에서 Use private key를 체크한 후
- 다운로드한 private key 파일(*.pem, *.ppk)을 업로드



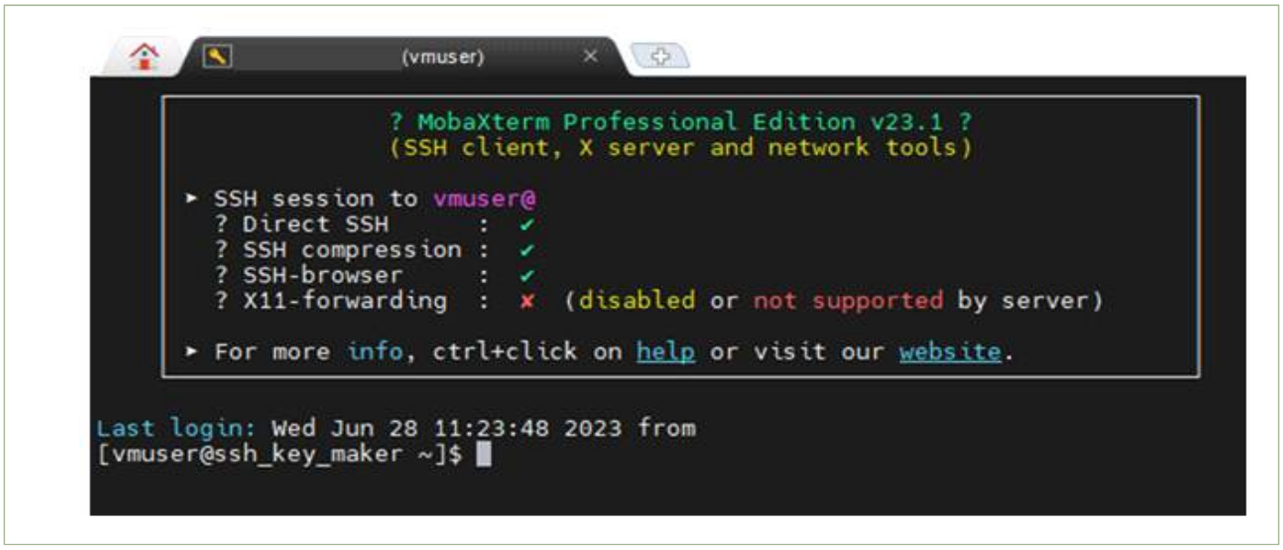
| 그림 1.1.3 | Key pair를 통한 가상자원 접속

- Basic SSH settings 정보를 입력한 후, OK 클릭
- Remote host: 접속할 Virtual Server의 IP 입력
- Specify username: 체크 박스를 클릭한 후, vmuser 입력



| 그림 1.1.4 | Key pair를 통한 가상자원 접속

- vmuser 탭을 클릭하여 Virtual Server 접속 상태 확인



| 그림 1.1.5 | Virtual Server 접속 상태 확인

4 참고 사항

- Key Pair 유출 시 서버에 누구나 접속이 가능하므로 안전하게 보관하고 서버 최초 접속 이후 관리자 패스워드 변경 및 새로운 계정을 생성하여 서버 접속 필요

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(5회 이상 로그인 실패 시 계정 잠김 등)

3 우수 사례

- 이용 고객은 삼성SDS 가상자원 활용 시 서버 내 관련 OS 파일 설정 값 변경을 통해 로그인 규칙 수립

4 참고 사항

- N/A

1 기준

식별번호	기준	내용
1.3.	**가상자원 루트 계정 접근 시 추가 인증수단 적용**	**이용자 가상자원 루트 계정(root, administrator 등) 접근 시 추가 인증 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) 이메일 인증 & 2) SMS 인증

- 로그인 시 이메일 또는 SMS를 통한 OTP 인증 필요

| 그림 1.3.1 | 로그인 인증

4) SSH PEM Key 등을 통한 안전한 로그인 수단 확보 등

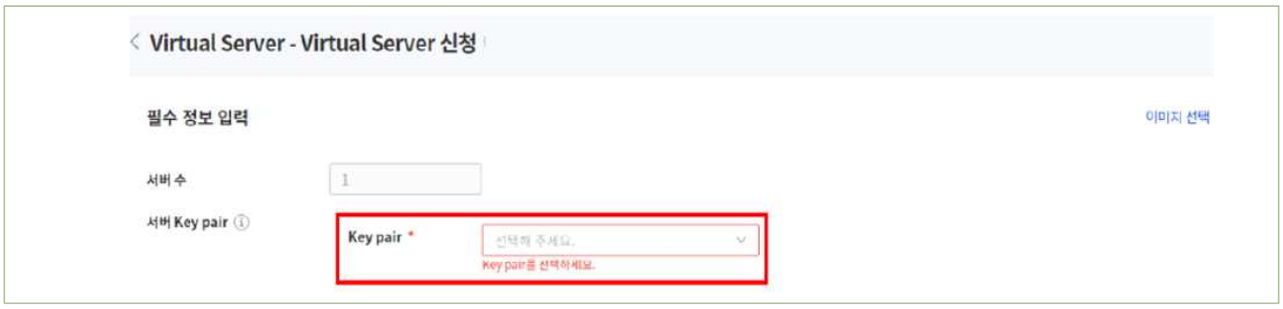
- 가상자원 최초 접속은 Key pair를 활용하여 안전하게 접속 가능

① Key pair 신청: 서버 Key pair명 입력→ 완료→ .pem파일 다운로드

| 그림 1.3.2 | 서버 Key pair 신청

② Key pair를 통한 가상자원 생성

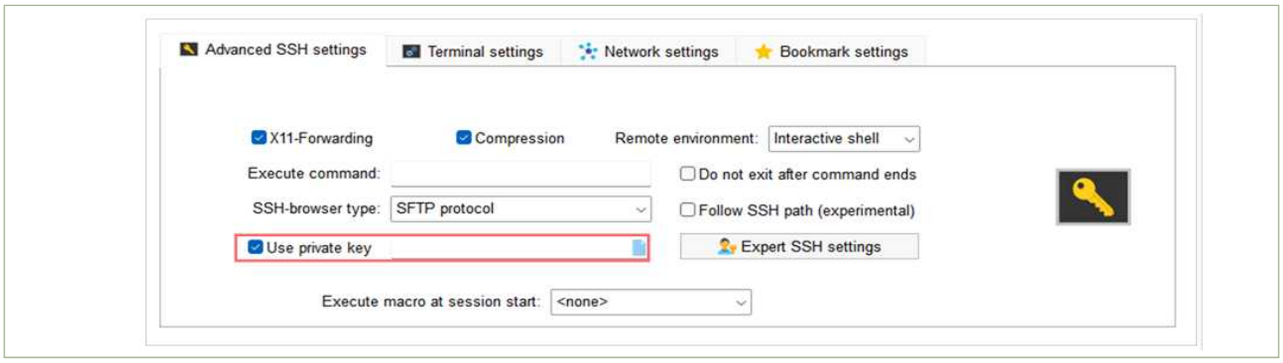
- 신청 경로: Project → 자원관리 → Compute → Virtual Server → Virtual Server → 상품 신청 → 이미지 선택 → 상품구성 선택 및 입력 → 필수정보 입력화면의 Key pair 신규 생성 또는 기존 Key pair 선택



| 그림 1.3.3 | Virtual Server 신청

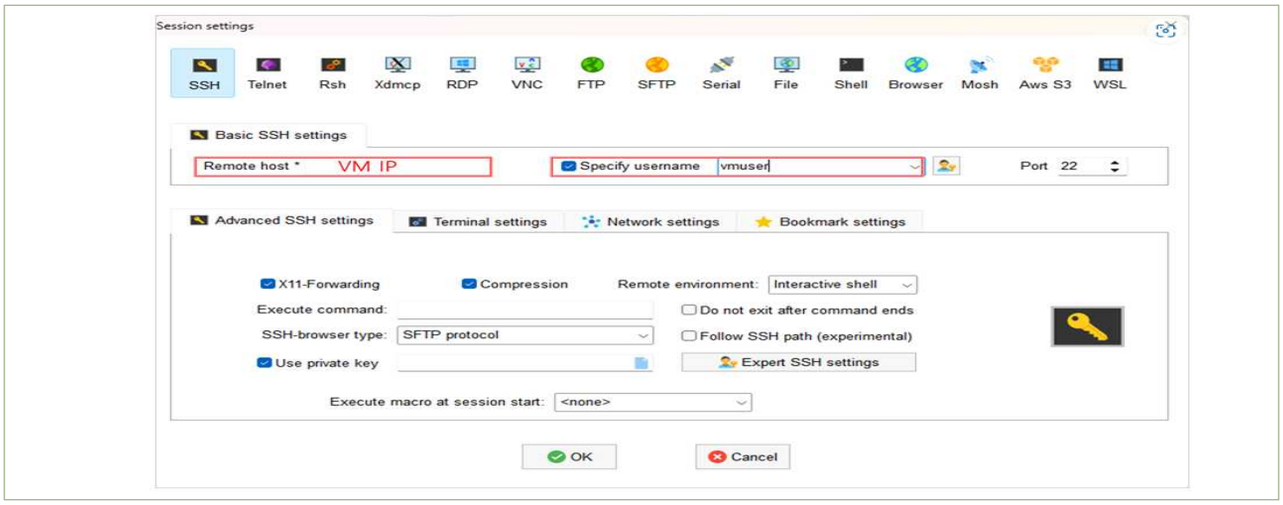
③ Key pair를 통한 가상자원 접속 (ex. mobaXterm 활용)

- mobaXterm을 실행한 후, Session settings 화면으로 이동
- Advanced SSH settings에서 Use private key를 체크한 후
- 다운로드한 private key 파일(*.pem, *.ppk)을 업로드



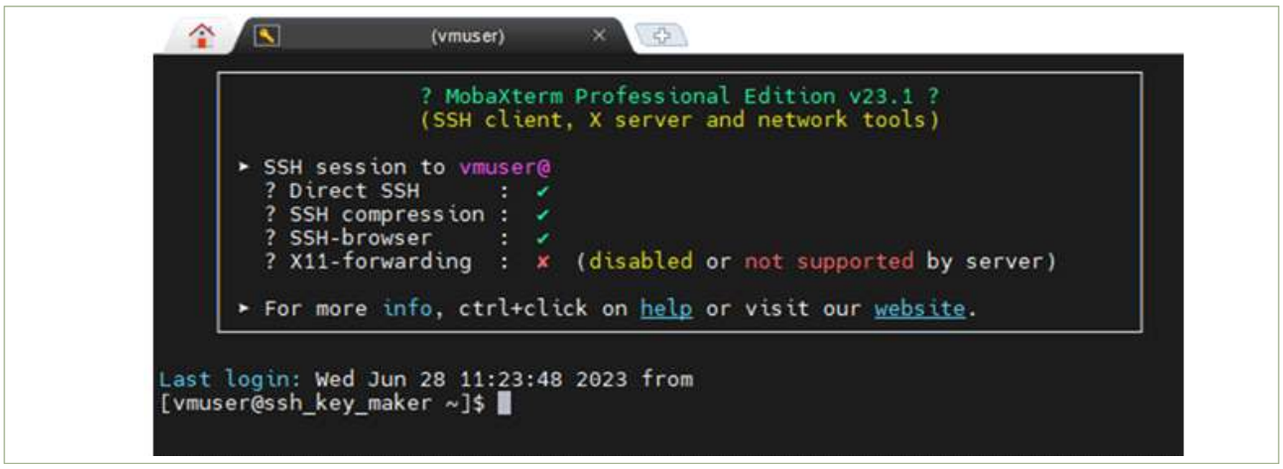
| 그림 1.3.4 | Key pair를 통한 가상자원 접속

- Basic SSH settings 정보를 입력한 후, OK 클릭
- Remote host: 접속할 Virtual Server의 IP 입력
- Specify username: 체크 박스를 클릭한 후, vmuser 입력



| 그림 1.3.5 | Key pair를 통한 가상자원 접속

- vmuser 탭을 클릭하여 Virtual Server 접속 상태 확인



| 그림 1.3.6 | Virtual Server 접속 상태 확인

4 참고 사항

- Key Pair 유출 시 서버에 누구나 접속이 가능하므로 안전하게 보관하고 서버 최초 접속 이후 관리자 패스워드 변경 및 새로운 계정을 생성하여 서버 접속 필요

1 기준

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

2 설명

- 외부에서 직접 접속이 불필요한 경우 내부IP 또는 IP대역에서만 접근할 수 있도록 설정하여야 한다.

  - 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 대역 접근 설정

3 우수 사례

1) 가상자원 접속 가능한 공인IP(외부)대역 점검 및 제거

- 외부에서 직접 접속이 불필요한 경우 Private 네트워크를 구성한다.

  ① Private Subnet 구성

  - 신청경로: 프로젝트 → 모든 상품 → Networking → VPC → Subnet → Subnet 생성

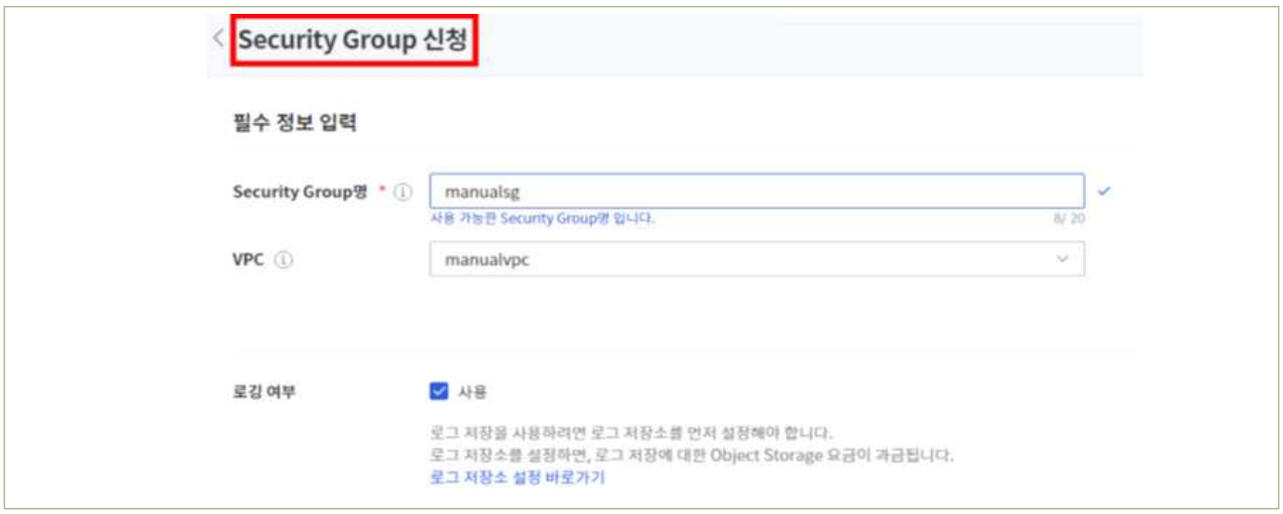
| 그림 1.4.1 | Private Subnet 생성

2) 접근 가능한 IP 또는 IP 대역 대 설정 & 3) VPC 및 보안그룹을 통한 내부 네트워크 대역 접근 설정

- Security Group을 활용하여 가상자원에 접근 가능한 IP 또는 IP 대역대를 설정이 가능하다.

① Security Group 구성

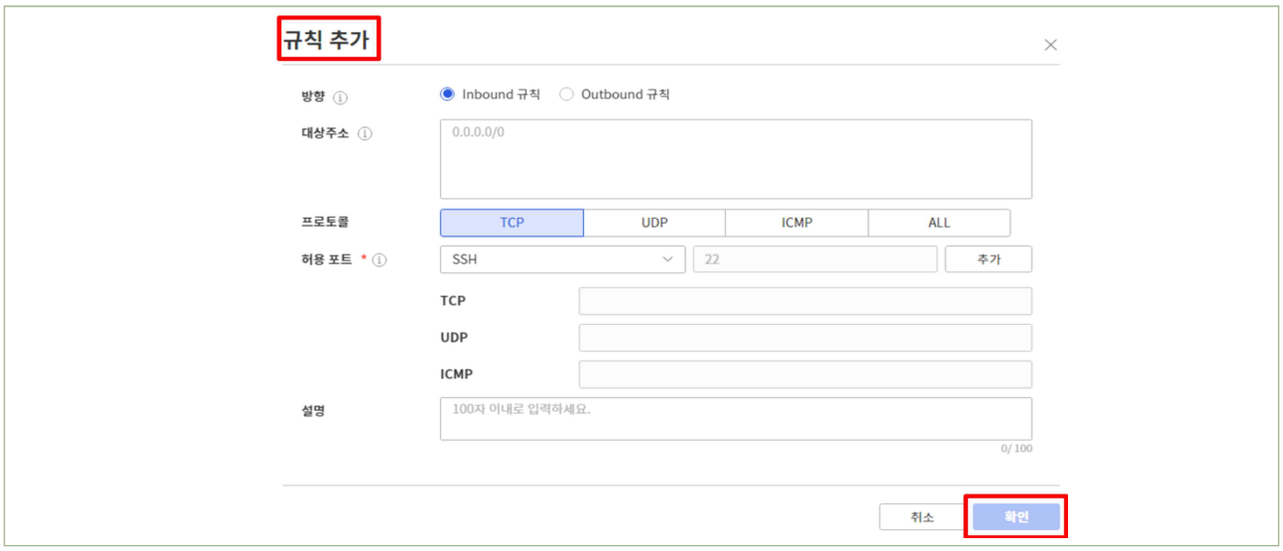
- 신청 경로: Project → 자원관리 → Networking → Security Group → 로깅 여부 체크 후 상품 신청



| 그림 1.4.2 | Security Group 신청

② Security Group 규칙 추가

- 신청 경로: Project → 자원관리 → Networking → Security Group → 규칙 → 규칙 추가 → 접속을 허용할 정보 입력 후 확인



| 그림 1.4.3 | Security Group 규칙 추가

A. 방향: 트래픽의 접근 방향을 설정

- Inbound : 외부 → 서버
- Outbound : 서버 → 외부

B. 대상 주소

- CIDR 형식(IP주소/서브넷마스크) 및 IP영역 또는 단일 주소를 ‘,’와 ‘-’을 사용하여 다수의 주소를 최대 128개까지 한 번에 입력할 수 있습니다. 전체 IP 범위(ANY)를 사용하려면 '0.0.0.0/0'을 입력해야 합니다. ex) 172.0.0.1/24, 10.0.0.1, 20.0.0.1-20.0.0.150

C. 허용 포트

- TCP, UDP 프로토콜을 선택한 경우, 허용 포트를 입력합니다. 허용 범위는 1 ~ 65,535 값이며, ','와 '시작 값-끝 값'을 사용해서 최대 128개까지 한 번에 입력할 수 있습니다. ex) 22, 80, 8001-8100

③ Security Group 규칙 삭제

- 신청 경로: Project → 자원관리 → Networking → Security Group → 규칙 → 삭제할 규칙 우측 클릭 → 규칙 삭제

| 그림 1.4.4 | Security Group 규칙 삭제

4 참고 사항

- N/A

1 기준

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

2 설명

- 이용자의 가상자원(인스턴스) 접속 시 안전한 방식을 통해 접근하여야 한다.

  - 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

1) SSH를 통한 접속 시 안전한 계정관리 수행 (ex. ID/PW 기반이 아닌 Certificate 기반 인증 방식 적용 등)

- 가상자원의 SSH를 통한 OS 최초 접속은 Key pair를 통해 가능하며 최초 접속 이후 관리자 패스워드 변경 및 사용자 계정을 생성하여 서버 접속

  ① Key pair 신청: 서버 Key pair명 입력 → 완료 → .pem파일 다운로드

| 그림 1.5.1 | 서버 Key pair 신청

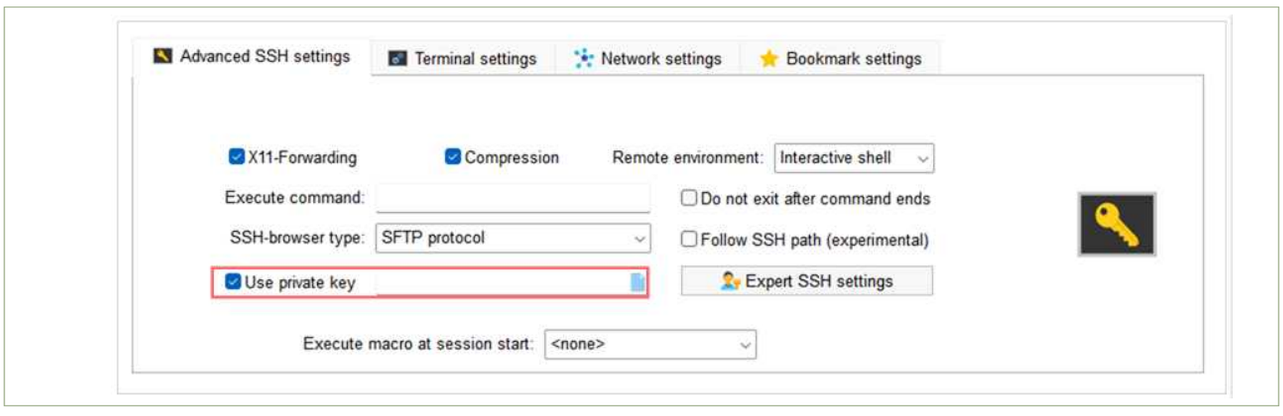
② Key pair를 통한 가상자원 생성

- 신청 경로: Project → 자원관리 → Compute → Virtual Server → Virtual Server → 상품 신청 → 이미지 선택 → 상품구성 선택 및 입력 → 필수정보 입력화면의 Key pair 신규 생성 또는 기존 Key pair 선택

| 그림 1.5.2 | Virtual Server 신청

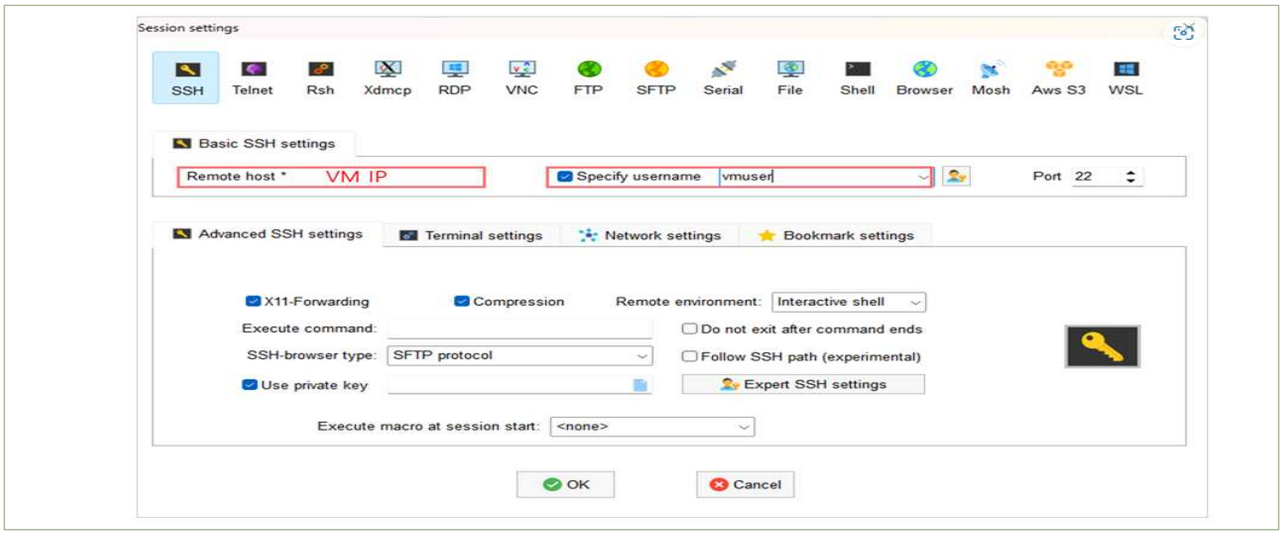
③ Key Pair를 통한 가상자원 접속 (ex. mobaXterm 활용)

- mobaXterm을 실행한 후, Session settings 화면으로 이동
- Advanced SSH settings에서 Use private key를 체크한 후
- 다운로드한 private key 파일(*.pem, *.ppk)을 업로드



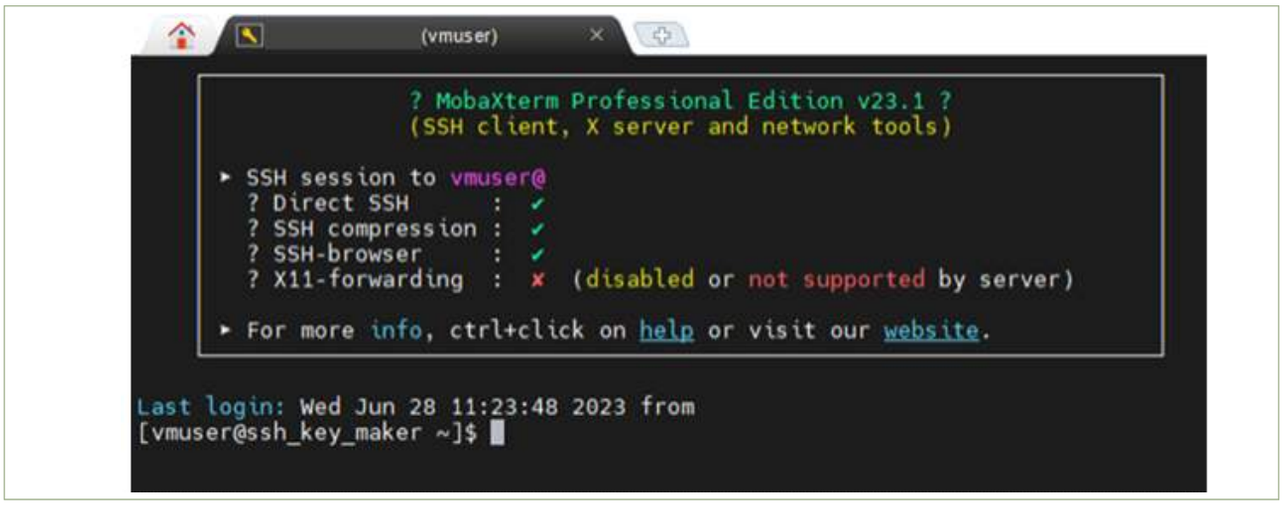
| 그림 1.5.3 | Key pair를 통한 가상자원 접속

- Basic SSH settings 정보를 입력한 후, OK 클릭
- Remote host: 접속할 Virtual Server의 IP 입력
- Specify username: 체크 박스를 클릭한 후, vmuser 입력



| 그림 1.5.4 | Key pair를 통한 가상자원 접속

- vmuser 탭을 클릭하여 Virtual Server 접속 상태 확인



| 그림 1.5.5 | Virtual Server 접속 상태 확인

2) 클라우드 웹 콘솔에서 직접 실행 시 안전한 인증 방식 적용(해당 인스턴스를 호출할 수 있는 권한을 지닌 이용자인지 검증 등)

- 자원 해킹 위협으로부터 안전장치 강화를 위하여 웹 콘솔에서 자원 접속 방식을 허용 하지 않음

4 참고 사항

- Key pair 유출 시 서버에 누구나 접속이 가능하므로 안전하게 보관하고 서버 최초 접속 이후 관리자 패스워드 변경 및 새로운 계정을 생성하여 서버 접속 필요

1 기준

식별번호	기준	내용
1.6.	**이용자 가상자원 별 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.

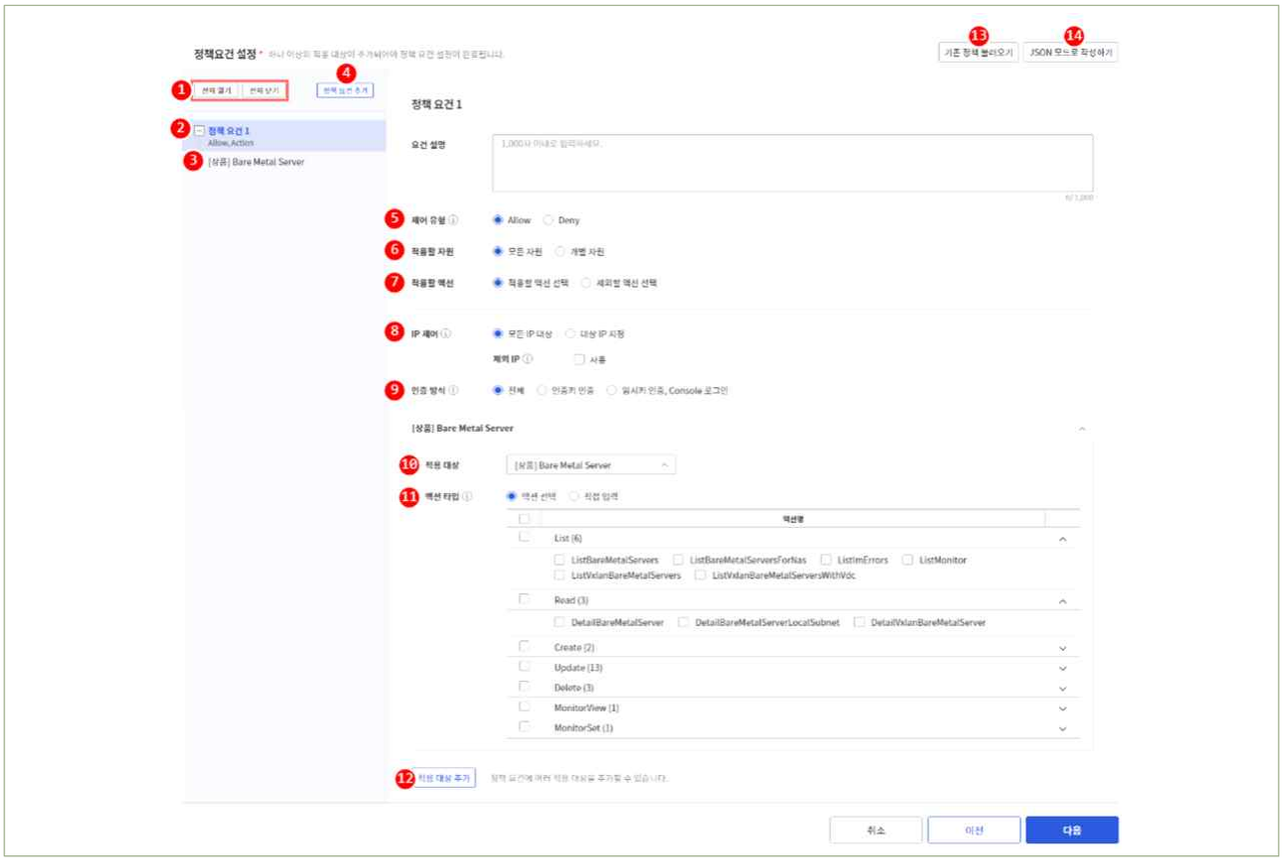
  - 예시

    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

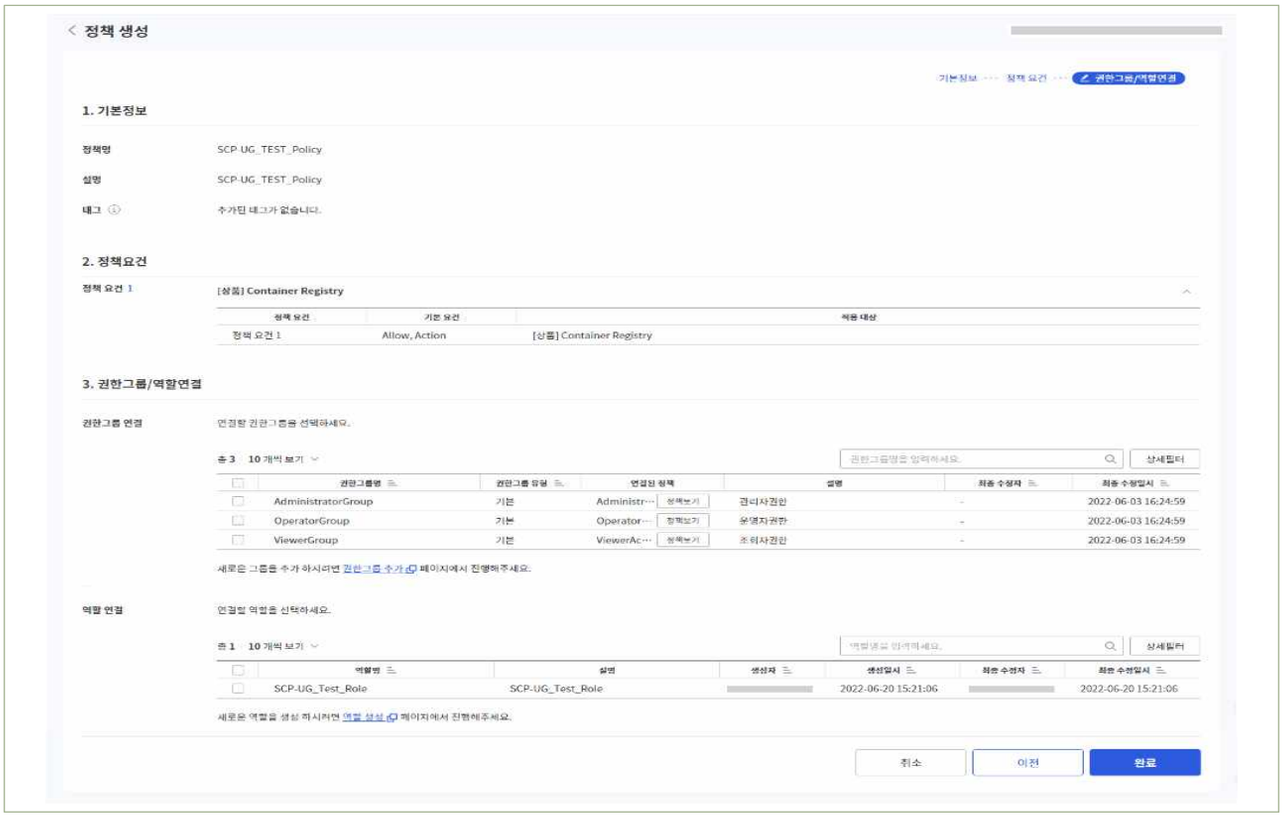
- (권한관리(IAM)) ‘정책’ 탭 → ‘정책 생성’ → ‘정책요건 설정’→ ‘적용 대상’에서 정책에 연결할 적용대상(가상자원)을 선택하여 연결 가능



| 그림 1.6.1 | 정책요건 설정

번호	항목	설명
❶	전체 열기 및 닫기	정책 요건 하위의 적용 대상 목록을 열지거나 닫을 수 있습니다.
❷	정책 요건	정책 하위 세부 사항의 묶음 단위입니다. 클릭하면 해당 정책 요건의 **설명**, **제어 유형**, **적용할 액션**을 표시합니다.
❸	적용 대상	정책 요건을 적용할 대상을 표시합니다. 클릭하면 적용 대상의 세부 사항을 설정할 수 있습니다.
❹	정책 요건 추가	정책 요건을 추가합니다.
❺	제어 유형	정책 적용 대상의 접근 제어 방식을 설정합니다. • **Allow**: 접근을 허용합니다. • **Deny**: 접근을 거부합니다.
❻	적용할 자원	정책이 적용될 대상 자원을 지정합니다. • **모든 자원**: 모든 자원을 대상으로 정책을 적용합니다. • **개별 자원**: 자원 목록을 지정하고 해당 자원에 대해 정책을 적용합니다. **적용할 액션**을 **제외할 액션 선택**으로 설정한 경우에는 선택할 수 없습니다.
❼	적용할 액션	정책에 적용할 액션을 선택하는 방식을 설정합니다. • **적용할 자원**이 **개별 자원**인 경우에는 **제외할 액션 선택**을 설정할 수 없습니다.
❽	IP 제어	정책 요건이 적용될 IP 주소 또는 범위를 설정합니다. • **모든 IP 대상**: 모든 IP를 정책 요건 대상으로 설정합니다. • **대상 IP 지정**: '/'를 이용하여 IP 대역을 지정하는 CIDR 방식으로 표기할 수도 있습니다. • **제외 IP**: 정책 요건의 대상에서 제외할 IP를 등록합니다.
❾	인증 방식	정책을 적용할 사용 대상의 인증 방식을 선택합니다. • **전체**: 인증 방식과 상관없이 적용 • **인증키 인증**: 인증키로 인증한 사용자에게 적용 • **임시키 인증, Console 로그인**: 임시키로 인증한 사용자나 Console 로그인한 사용자에게 적용
❿	적용 대상	정책 요건을 적용할 대상을 선택합니다.
⓫	액션 타입	정책 요건의 내용을 적용할 액션을 목록에서 선택하거나 직접 입력할 수 있습니다.
⓬	적용 대상 추가	정책 요건을 적용할 대상을 추가합니다.
⓭	기존 정책 불러오기	기존에 등록된 정책 중 하나를 복사해 불러올 수 있습니다. • 기존 정책을 불러올 경우, 현재 작성 중이던 항목이 모두 초기화됩니다.
⓮	JSON 모드로 작성하기	JSON 타입 정책문을 에디터 모드에서 직접 수정할 수 있습니다.

| 그림 1.6.2 | 권한그룹과 역할연결



| 그림 1.6.3 | 권한그룹과 역할연결

4 참고 사항

- N/A

1 기준

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

2 설명

- 이용자 가상자원 내 악성코드 통제방안을 수립하여야 한다.

  - 예시

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

3 우수 사례

- 이용 고객은 가상자원 내 악성코드 통제를 위해 가상자원 내 별도의 악성코드 통제 솔루션 설치 및 마켓플레이스 내 네트워크 보호 서비스 등을 이용

4 참고 사항

- N/A

2. 네트워크 관리

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

2 네트워크 관리

1 기준

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

2 설명

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

  - 예시

    1) VPC 등 네트워크 관련 기능을 통한 네트워크 구성 및 통제

    2) 보안그룹(Security group) 또는 NACL(Network ACL) 등의 기능을 통한 네트워크 구성 및 통제(인/아웃바운드 통제 등)

3 우수 사례

1) VPC 등 네트워크 관련 기능을 통한 네트워크 구성 및 통제

- VPC 및 Subnet을 통한 사용자 업무 목적에 따른 네트워크 구성

  ① VPC 구성

  - 신청 경로: 프로젝트 → 모든 상품 → Networking → VPC → 상품 신청

| 그림 2.1.1 | VPC 신청

② Subnet 신청

- 신청 경로: 프로젝트 → 모든 상품 → Networking → VPC → Subnet → 상품 신청

| 그림 2.1.2 | Subnet 생성

A. 사용 용도

- 일반 : VPC내에서 용도에 맞는 네트워크 구성을 위해 신청 가능하며, 서브넷 하위 리소스 중에 공인IP의 여부에 따라 Public과 Private으로 구분됩니다.
- 로컬 : 일반 서브넷과 달리 외부 통신은 되지 않고, 서버 간의 통신만을 위한 서브넷입니다.

B. IP 대역

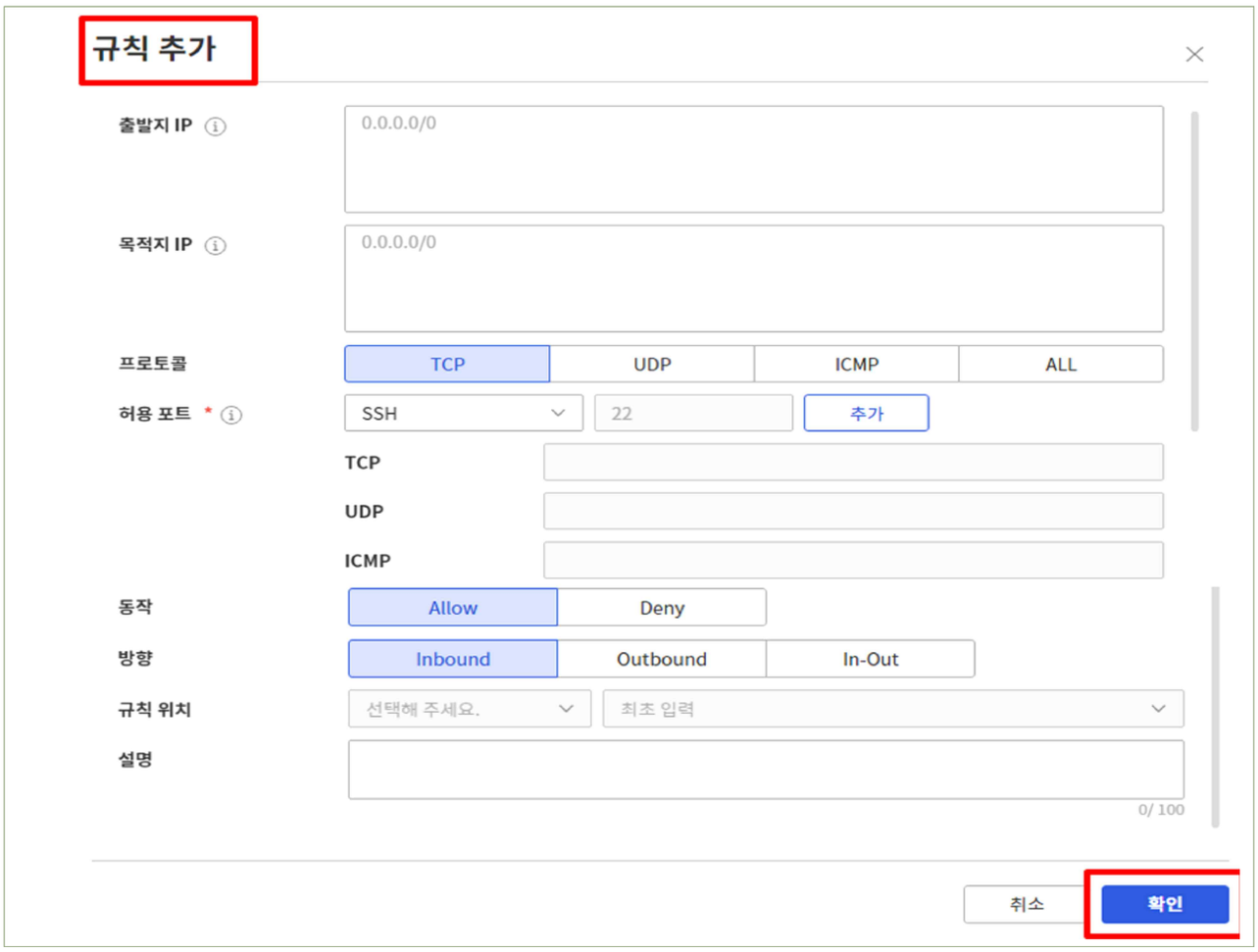
- 서브넷에 사용할 IP대역은 Mask /24~/27범위 내에서 사용자가 입력 가능합니다.
- VPC내 사용중인 IP 대역(다른 서브넷 및 LB상품 IP대역, Routing Table 에 설정한 IP대역, Endpoint IP)과 중복되지 않아야 합니다. 또한, 연결된 다른 VPC 및 고객사 Network의 IP 대역과도 중복되지 않아야 합니다. 일부 IP대역은 관리용으로 사용할 수 없습니다.

2) 보안그룹(Security group) 또는 NACL(Network ACL) 등의 기능을 통한 네트워크 구성 및 통제(인/아웃바운드 통제 등)

- Firewall을 통해 VPC과 인터넷 또는 고객망 간의 네트워크 통제

① Firewall 구성

- 신청 경로: 별도 신청하는 상품이 아니며 Internet Gateway, VPC Peering, Transit Gateway, Direct Connect, Load Balancer 등 VPC 연계 상품 구성 시 자동 생성
- 규칙 추가: 프로젝트 → 자원 관리 → Networking → Firewall → Firewall 선택 → 규칙 → 규칙 추가 or 규칙 일괄 입력



| 그림 2.1.3 | Firewall 규칙 추가

A. 출발지 IP

- CIDR 형식(IP주소/서브넷마스크) 및 IP영역 또는 단일 주소를 ‘,’와 ‘-’을 사용하여 다수의 주소를 최대 128개까지 한 번에 입력할 수 있습니다. 전체 IP 범위(ANY)를 사용하려면 '0.0.0.0/0'을 입력해야 합니다. ex) 172.0.0.1/24, 10.0.0.1, 20.0.0.1-20.0.0.150

B. 목적지 IP

- CIDR 형식(IP주소/서브넷마스크) 및 IP영역 또는 단일 주소를 ‘,’와 ‘-’을 사용하여 다수의 주소를 최대 128개까지 한 번에 입력할 수 있습니다. 전체 IP 범위(ANY)를 사용하려면 '0.0.0.0/0'을 입력해야 합니다. ex) 172.0.0.1/24, 10.0.0.1, 20.0.0.1-20.0.0.150

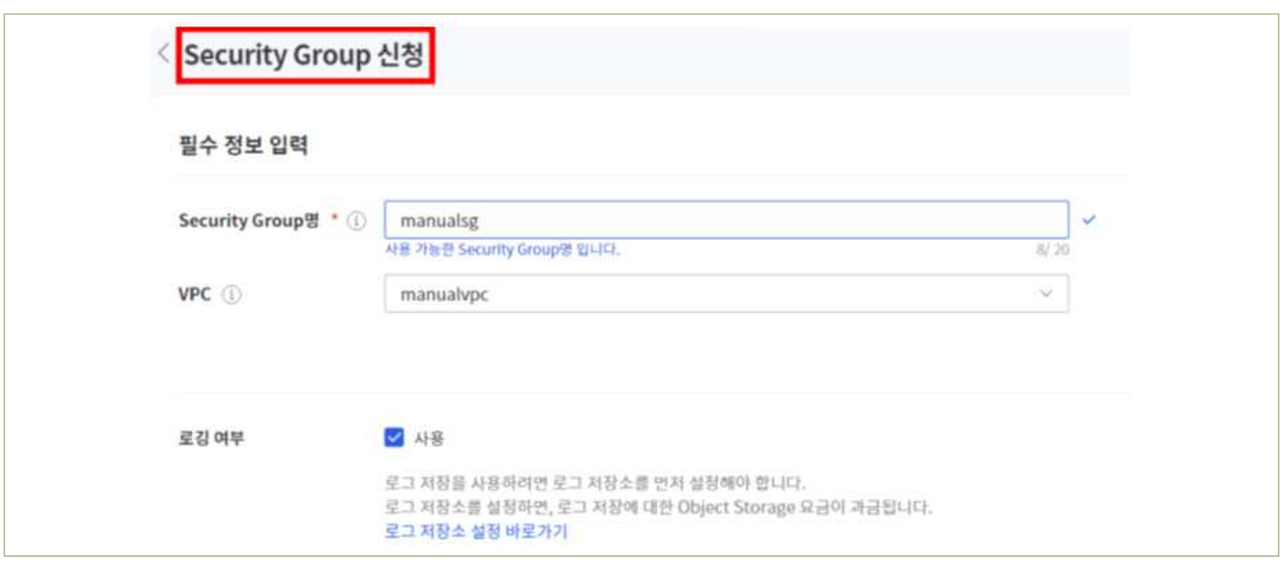
C. 허용 포트

- TCP, UDP 프로토콜을 선택한 경우, 허용 포트를 입력합니다. 허용 범위는 1-65535 값이며, ‘,’와 ‘시작값-끝값’을 사용해서 포트 총합 최대 128개까지 한 번에 입력할 수 있습니다. ex) 22,80,8001-8100

- Security Group을 통해 가상자원의 네트워크 통제

① Security Group 구성

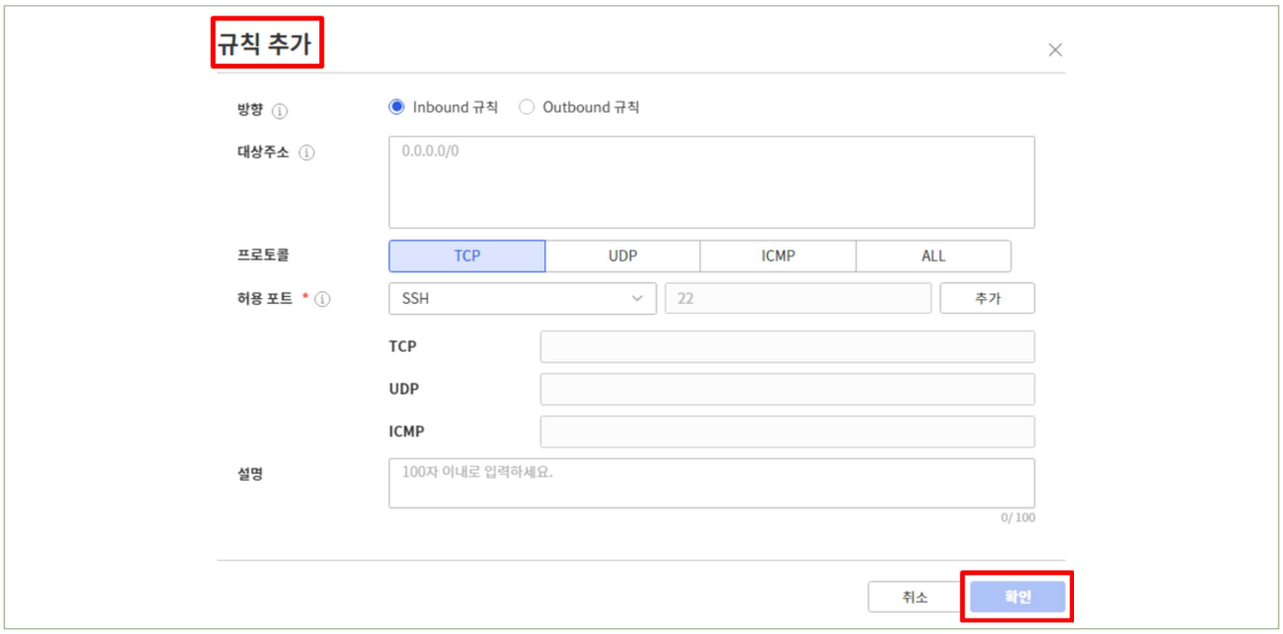
- 신청 경로: Project → 자원관리 → Networking → Security Group → 로깅 여부 체크 후 상품 신청



| 그림 2.1.4 | Security Group 신청

② Security Group 규칙 추가

- 신청 경로: Project → 자원관리 → Networking → Security Group → 규칙 → 규칙 추가 → 접속을 허용할 정보 입력 후 확인



| 그림 2.1.5 | Security Group 규칙 추가

A. 방향: 트래픽의 접근 방향을 설정합니다.

- Inbound : 외부 → 서버
- Outbound : 서버 → 외부

B. 대상 주소

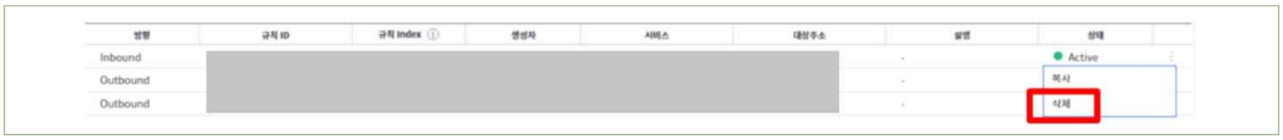
- CIDR 형식(IP주소/서브넷마스크) 및 IP영역 또는 단일 주소를 ‘,’와 ‘-’을 사용하여 다수의 주소를 최대 128개까지 한 번에 입력할 수 있습니다. 전체 IP 범위(ANY)를 사용하려면 '0.0.0.0/0'을 입력해야 합니다. ex) 172.0.0.1/24, 10.0.0.1, 20.0.0.1-20.0.0.150

C. 허용 포트

- TCP, UDP 프로토콜을 선택한 경우, 허용 포트를 입력합니다. 허용 범위는 1-65535 값이며, ','와 '시작 값-끝 값'을 사용해서 최대 128개까지 한 번에 입력할 수 있습니다. ex) 22, 80, 8001-8100

③ Security Group 규칙 삭제

- 신청 경로: Project → 자원관리 → Networking → Security Group → 규칙 → 삭제할 규칙 우측 클릭 → 규칙 삭제



| 그림 2.1.6 | Security Group 규칙 삭제

4 참고 사항

- N/A

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

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

- VPC 및 Private Subnet을 통한 내부망 구성

  ① VPC 구성

  - 신청 경로: 프로젝트 → 모든 상품 → Networking → VPC → 상품 신청

| 그림 2.2.1 | VPC 구성

② Subnet 신청

- 신청 경로: 프로젝트 → 모든 상품 → Networking → VPC → Subnet → 상품 신청

| 그림 2.2.2 | Subnet 생성

A. 사용 용도

- 일반 : VPC내에서 용도에 맞는 네트워크 구성을 위해 신청 가능하며, 서브넷 하위 리소스 중에 공인IP의 여부에 따라 Public과 Private으로 구분됩니다.
- 로컬 : 일반 서브넷과 달리 외부 통신은 되지 않고, 서버 간의 통신만을 위한 서브넷입니다.

B. IP 대역

- 서브넷에 사용할 IP 대역은 Mask /24~/27범위 내에서 사용자가 입력 가능합니다.
- VPC내 사용중인 IP 대역(다른 서브넷 및 LB상품 IP 대역, Routing Table 에 설정한 IP 대역, Endpoint IP)과 중복되지 않아야 합니다. 또한, 연결된 다른 VPC 및 고객사 Network의 IP 대역과도 중복되지 않아야 합니다. 일부 IP 대역은 관리용으로 사용할 수 없습니다.

2) 보안그룹(Security group) 또는 NACL(Network ACL) 등의 기능을 통한 네트워크 구성 및 통제(인/아웃바운드 통제 등)

- Security Group을 통해 가상자원의 네트워크 통제

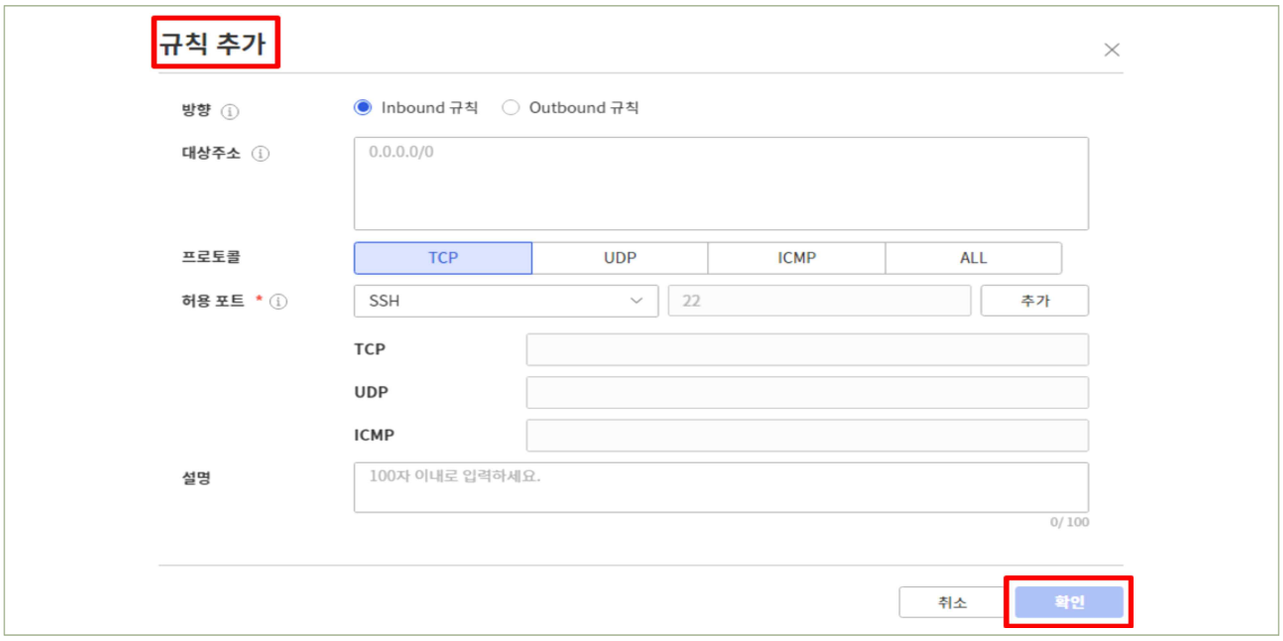
① Security Group 구성

- 신청 경로: Project → 자원관리 → Networking → Security Group → 로깅 여부 체크 후 상품 신청

| 그림 2.2.3 | Security Group 신청

② Security Group 규칙 추가

- 신청 경로: Project → 자원관리 → Networking → Security Group → 규칙 → 규칙 추가 → 접속을 허용할 정보 입력 후 확인



| 그림 2.2.4 | Security Group 규칙 추가

A. 방향: 트래픽의 접근 방향을 설정

- Inbound : 외부 → 서버
- Outbound : 서버 → 외부

B. 대상 주소

- CIDR 형식(IP주소/서브넷마스크) 및 IP영역 또는 단일 주소를 ‘,’와 ‘-’을 사용하여 다수의 주소를 최대 128개까지 한 번에 입력할 수 있습니다. 전체 IP 범위(ANY)를 사용하려면 '0.0.0.0/0'을 입력해야 합니다. ex) 172.0.0.1/24, 10.0.0.1, 20.0.0.1-20.0.0.150

C. 허용 포트

- TCP, UDP 프로토콜을 선택한 경우, 허용 포트를 입력합니다. 허용 범위는 1-65535 값이며, ','와 '시작 값-끝 값'을 사용해서 최대 128개까지 한 번에 입력할 수 있습니다. ex) 22, 80, 8001-8100

③ Security Group 규칙 삭제

- 신청 경로: Project → 자원관리 → Networking → Security Group → 규칙 → 삭제할 규칙 우측 클릭 → 규칙 삭제

| 그림 2.2.5 | Security Group 규칙 삭제

3) 내부망으로 구현한 가상자원(서버, 데이터베이스 등)에 공인 IP 미 할당

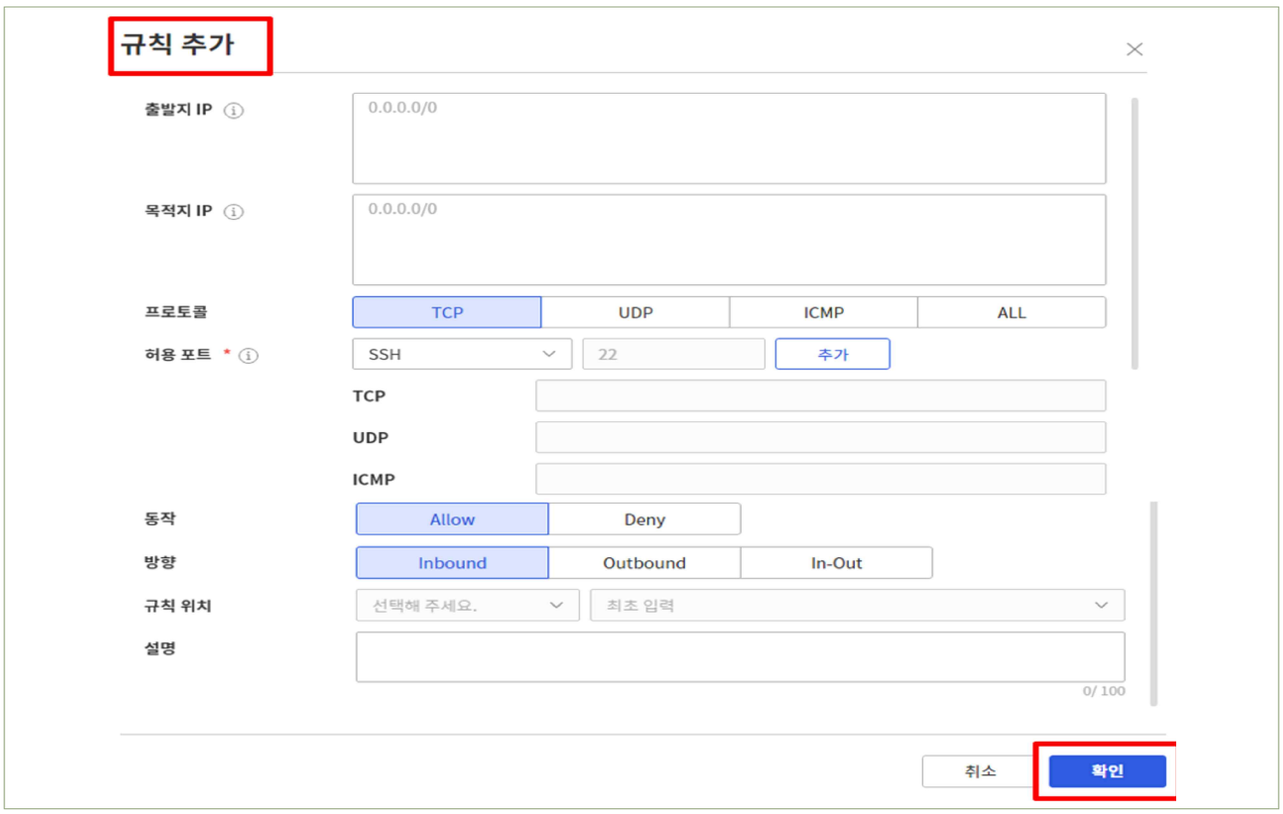
- Private Subnet 구성 시 인터넷 통신을 위한 공인 IP(NAT IP) 미 할당
- Public Subnet 구성 시에만 인터넷 통신을 위한 공인 IP(NAT IP) 할당

4) 방화벽 서비스를 통한 IP 통제 등

- Firewall을 통해 VPC과 인터넷 또는 고객망 간의 네트워크 통제

① Firewall 구성

- 신청 경로: 별도 신청하는 상품이 아니며 Internet Gateway, VPC Peering, Transit Gateway, Direct Connect, Load Balancer 등 VPC 연계 상품 구성 시 자동 생성
- 규칙 추가: 프로젝트 → 자원 관리 → Networking → Firewall → Firewall 선택 → 규칙 → 규칙 추가 or 규칙 일괄 입력



| 그림 2.2.6 | Firewall 규칙 추가

A. 출발지 IP

- CIDR 형식(IP주소/서브넷마스크) 및 IP영역 또는 단일 주소를 ‘,’와 ‘-’을 사용하여 다수의 주소를 최대 128개까지 한 번에 입력할 수 있습니다. 전체 IP 범위(ANY)를 사용하려면 '0.0.0.0/0'을 입력해야 합니다. ex) 172.0.0.1/24, 10.0.0.1, 20.0.0.1-20.0.0.150

B. 목적지 IP

- CIDR 형식(IP주소/서브넷마스크) 및 IP영역 또는 단일 주소를 ‘,’와 ‘-’을 사용하여 다수의 주소를 최대 128개까지 한 번에 입력할 수 있습니다. 전체 IP 범위(ANY)를 사용하려면 '0.0.0.0/0'을 입력해야 합니다. ex) 172.0.0.1/24, 10.0.0.1, 20.0.0.1-20.0.0.150

C. 허용 포트

- TCP, UDP 프로토콜을 선택한 경우, 허용 포트를 입력합니다. 허용 범위는 1-65535 값이며, ‘,’와 ‘시작값-끝값’을 사용해서 포트 총합 최대 128개까지 한 번에 입력할 수 있습니다. ex) 22,80,8001-8100

4 참고 사항

- N/A

1 기준

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

2 설명

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

  - 예시

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

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

3 우수 사례

1) 금융권 통합 보안관제 수행을 위한 지원 체계가 마련되어 있음

- Tap 장비를 이용하여 Mirroring 구성으로 보안관제 적용 가능

4 참고 사항

- N/A

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 웹서버 구현 시 내부통신망과 분리하여 내부통신망과 외부통신망 사이 별도의 독립된 통신망("이하 DMZ")을 구현하고 안전하게 보호하여야 한다.

  - 예시

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

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

3 우수 사례

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

- VPC, Internet Gateway 및 Public Subnet을 통한 DMZ 네트워크 구성

  ① VPC 구성

  - 신청 경로: 프로젝트 → 모든 상품 → Networking → VPC → 상품 신청

| 그림 2.4.1 | VPC 구성

② VPC – Internet Gateway 생성

- 신청 경로: Project → 자원관리 → Networking → VPC → Internet Gateway →IGW 생성 (인터넷 연결이 필요한 VPC 선택) → 구분에 Internet Gateway 선택 → Firewall 사용 및 로깅 여부 체크

| 그림 2.4.2 | Internet Gateway 생성

③ Subnet 구성

- 신청 경로: 프로젝트 → 모든 상품 → Networking → VPC → Subnet → 상품 신청 → 사용 용도 'Public' 선택

| 그림 2.4.3 | Public Subnet 생성

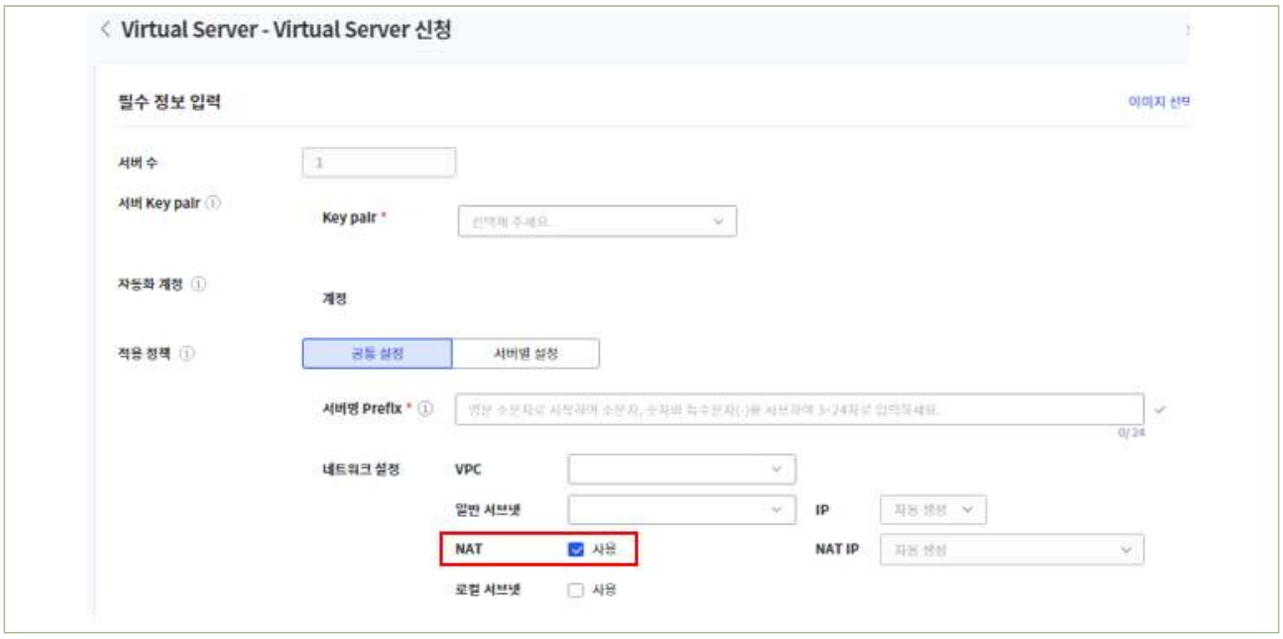
A. 사용 용도

- 일반 : VPC 내에서 용도에 맞는 네트워크 구성을 위해 신청 가능하며, 서브넷 하위 리소스 중에 공인 IP의 여부에 따라 Public과 Private으로 구분됩니다.
- 로컬 : 일반 서브넷과 달리 외부 통신은 되지 않고, 서버 간의 통신만을 위한 서브넷입니다.

B. IP 대역

- 서브넷에 사용할 IP 대역은 Mask /24~/27범위 내에서 사용자가 입력 가능합니다.
- VPC내 사용중인 IP 대역(다른 서브넷 및 LB상품 IP 대역, Routing Table 에 설정한 IP 대역, Endpoint IP)과 중복되지 않아야 합니다. 또한, 연결된 다른 VPC 및 고객사 Network의 IP 대역과도 중복되지 않아야 합니다. 일부 IP 대역은 관리용으로 사용할 수 없습니다.

- DMZ 네트워크 내 가상자원 생성
  - ① 가상자원 생성
    - 신청 경로: Project → 자원관리→ Compute → Virtual Server → Virtual Server → 상품 신청 → 이미지 선택 → 상품 구성 선택 → 필수정보입력 → NAT 사용 체크



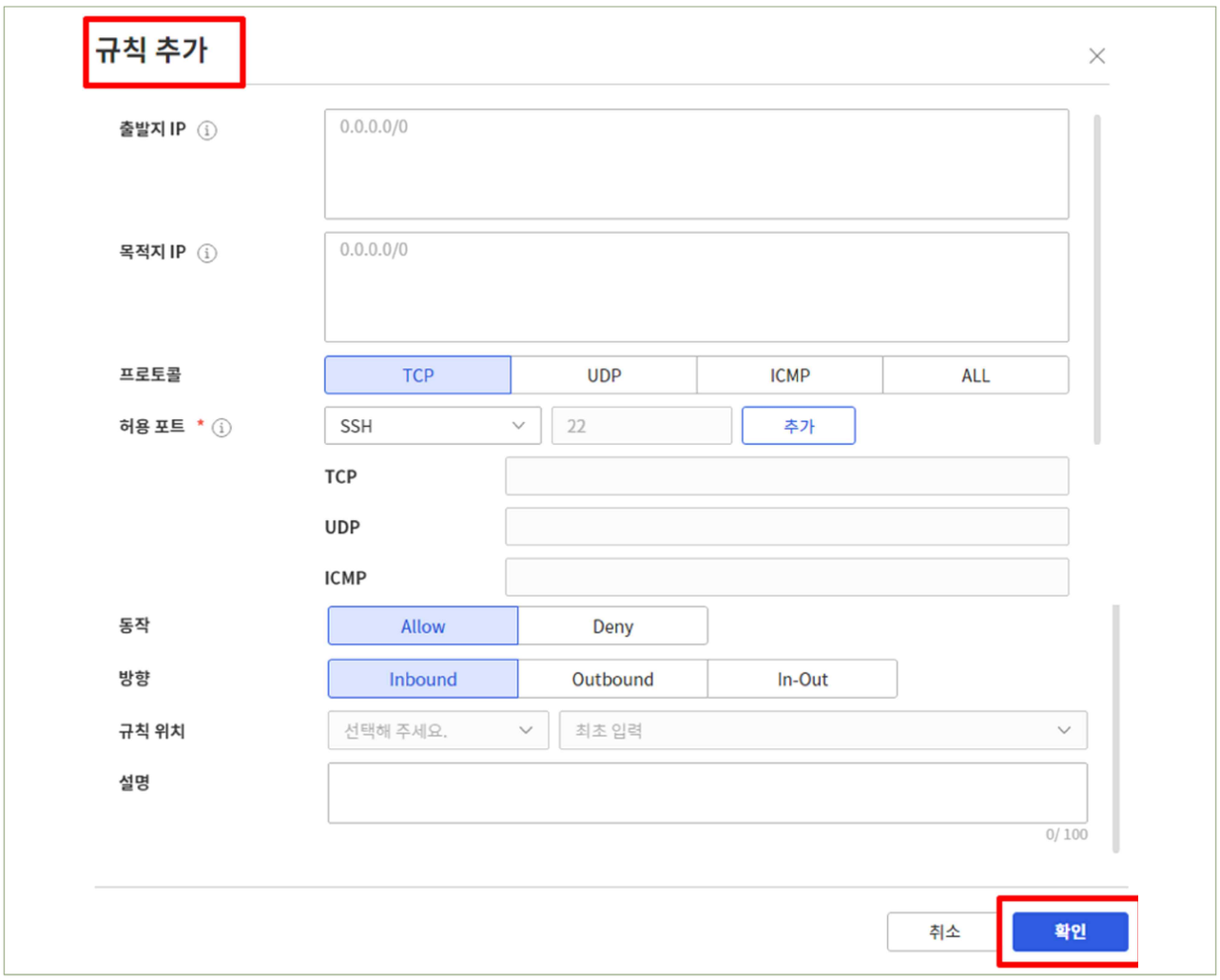
| 그림 2.4.4 | Virtual Server 신청

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

- Firewall을 통해 VPC과 인터넷 또는 고객망 간의 네트워크 통제

① Firewall 구성

- 신청 경로: 별도 신청하는 상품이 아니며 Internet Gateway, VPC Peering, Transit Gateway, Direct Connect, Load Balancer 등 VPC 연계 상품 구성 시 자동 생성
- 규칙 추가: 프로젝트 → 자원 관리 → Networking → Firewall → Firewall 선택 → 규칙 → 규칙 추가 or 규칙 일괄 입력



| 그림 2.4.5 | Firewall 규칙 추가

A. 출발지 IP

- CIDR 형식(IP주소/서브넷마스크) 및 IP 영역 또는 단일 주소를 ‘,’와 ‘-’을 사용하여 다수의 주소를 최대 128개까지 한 번에 입력할 수 있습니다. 전체 IP 범위(ANY)를 사용하려면 '0.0.0.0/0'을 입력해야 합니다. ex) 172.0.0.1/24, 10.0.0.1,

20.0.0.1-20.0.0.150

B. 목적지 IP

- CIDR 형식(IP주소/서브넷마스크) 및 IP 영역 또는 단일 주소를 ‘,’와 ‘-’을 사용하여 다수의 주소를 최대 128개까지 한 번에 입력할 수 있습니다. 전체 IP 범위(ANY)를 사용하려면 '0.0.0.0/0'을 입력해야 합니다. ex) 172.0.0.1/24, 10.0.0.1, 20.0.0.1-20.0.0.150

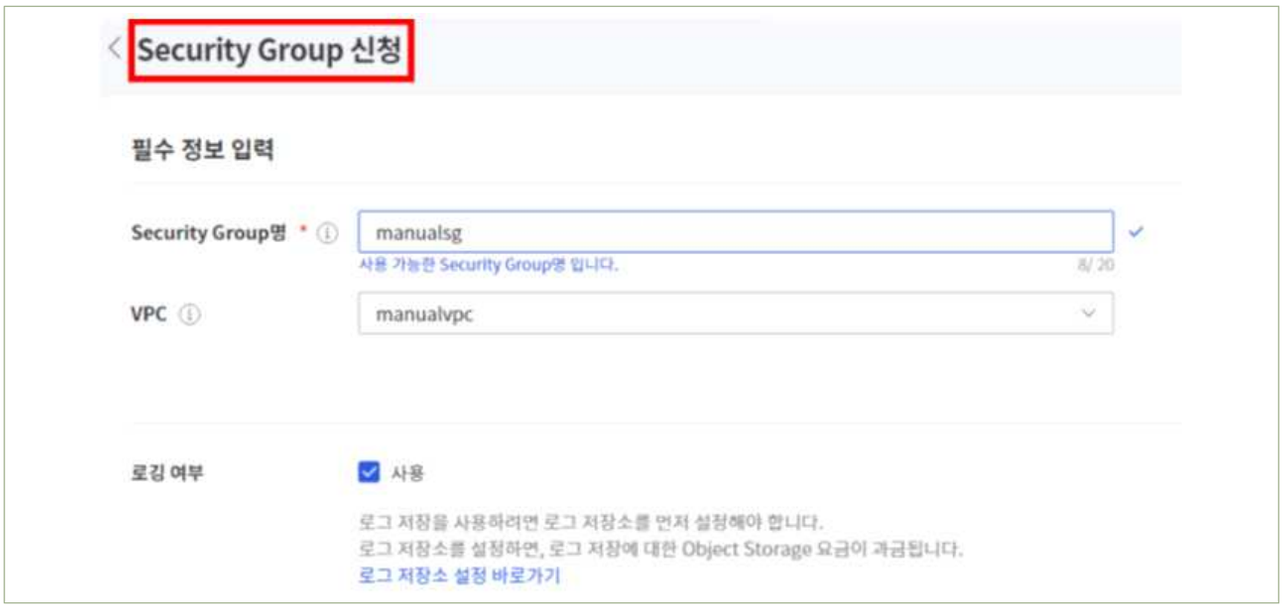
C. 허용 포트

- TCP, UDP 프로토콜을 선택한 경우, 허용 포트를 입력합니다. 허용 범위는 1-65535 값이며, ‘,’와 ‘시작값-끝값’을 사용해서 포트 총합 최대 128개까지 한 번에 입력할 수 있습니다. ex) 22,80,8001-8100

- Security Group을 통해 가상자원의 네트워크 통제

① Security Group 구성

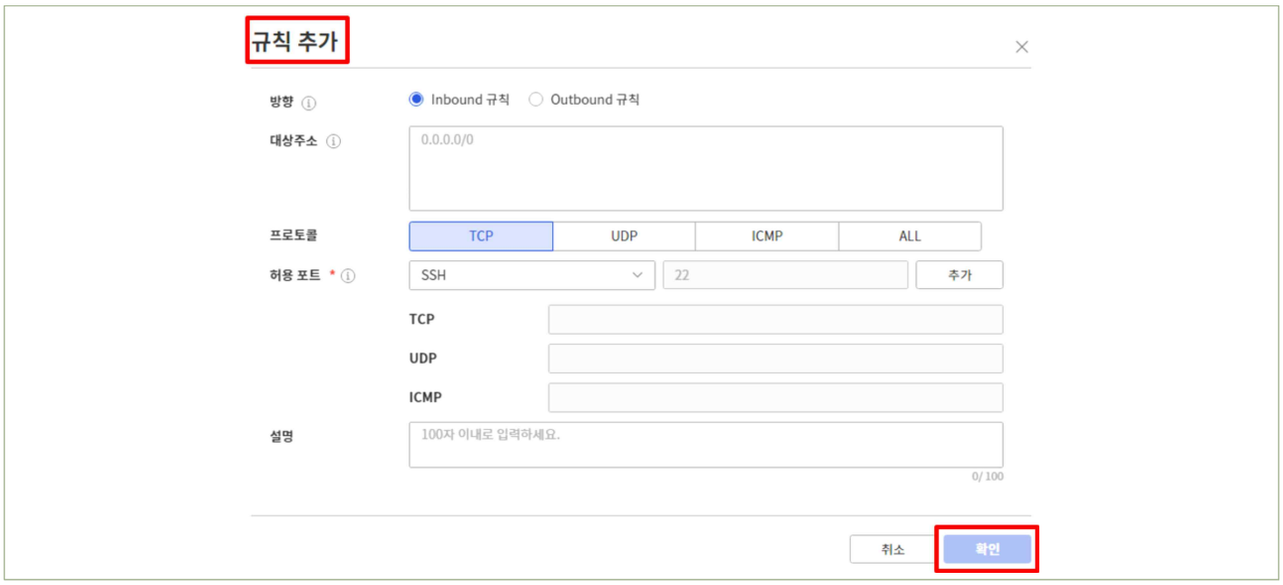
- 신청 경로: Project → 자원관리 → Networking → Security Group → 로깅 여부 체크 후 상품 신청



| 그림 2.4.6 | Security Group 신청

② Security Group 규칙 추가

- 신청 경로: Project → 자원관리 → Networking → Security Group → 규칙 → 규칙 추가 → 접속을 허용할 정보 입력 후 확인



| 그림 2.4.7 | Security Group 규칙 추가

A. 방향: 트래픽의 접근 방향을 설정합니다.

- Inbound : 외부 → 서버
- Outbound : 서버 → 외부

B. 대상 주소

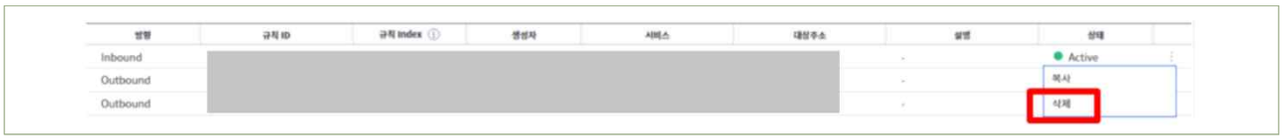
- CIDR 형식(IP주소/서브넷마스크) 및 IP 영역 또는 단일 주소를 ‘,’와 ‘-’을 사용하여 다수의 주소를 최대 128개까지 한 번에 입력할 수 있습니다. 전체 IP 범위(ANY)를 사용하려면 '0.0.0.0/0'을 입력해야 합니다. ex) 172.0.0.1/24, 10.0.0.1, 20.0.0.1-20.0.0.150

C. 허용 포트

- TCP, UDP 프로토콜을 선택한 경우, 허용 포트를 입력합니다. 허용 범위는 1-65535 값이며, ','와 '시작 값-끝 값'을 사용해서 최대 128개까지 한 번에 입력할 수 있습니다. ex) 22, 80, 8001-8100

③ Security Group 규칙 삭제

- 신청 경로: Project → 자원관리 → Networking → Security Group → 규칙 → 삭제할 규칙 우측 클릭 → 규칙 삭제



| 그림 2.4.8 | Security Group 규칙 삭제

4 참고 사항

- N/A

1 기준

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

2 설명

- 클라우드 환경 내 내부망 네트워크 구현 시 사설 IP를 부여하고 주기적으로 현황을 검토하여야 한다.

  – 예시

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

  2) 사설 IP 할당 현황에 대한 주기적 검토 수행

3 우수 사례

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

- Subnet을 통한 내부망 네트워크 사설 IP 부여 및 관리

  ① Subnet 구성을 통한 사설 IP 부여

  – 신청 경로: 프로젝트 → 모든 상품 → Networking → VPC → Subnet → 상품 신청 → 사용 용도 'Private' 선택

| 그림 2.5.1 | Subnet 생성

② Subnet 관리

- 관리 경로: 프로젝트 → 자원 관리 → Networking → VPC → Subnet → Subnet 상세 → IP 대역

| 그림 2.5.2 | Subnet 관리

2) 사설 IP 할당 현황에 대한 주기적 검토 수행

- Subnet 상세 화면을 통해 주기적 검토 수행 가능

4 참고 사항

- N/A

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 수행하여야 한다.

  - ‘2. 네트워크 관리’ 분야 내 내용을 참고하여 내부에서 방화벽, ACL, 보안그룹 등에 대해 검토

4 참고 사항

- N/A

3. 계정 및 권한 관리

3.1. 클라우드 계정 권한 관리
3.2. 이용자별 인증 수단 부여
3.3. 인사변경 사항 발생 시 계정 관리
3.4. 클라우드 가상자원 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, MFA 등 추가 인증 방식을 구현하고 접속 IP를 제한하는 등 강화된 보안환경 구성

3 우수 사례

1) 사전에 정의된 행위만이 가능하도록 역할을 생성

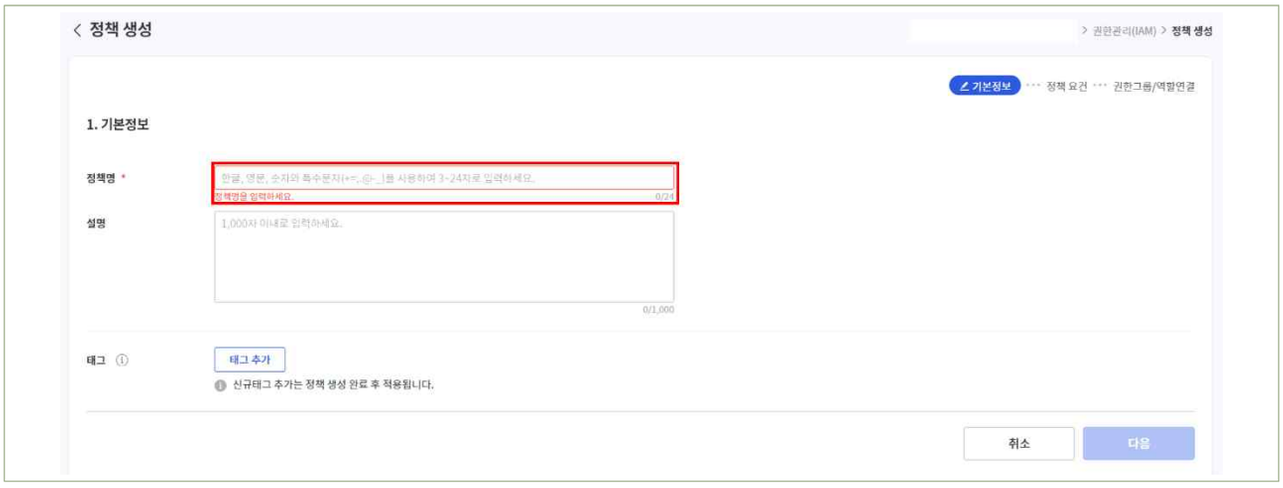
- 정책요건 설정을 통한 계정 권한 관리

① 정책요건 설정

- 권한관리(IAM) → 정책 탭 → 정책 생성 → 정책요건 설정에서 사전에 정의된 행위만 가능하도록 정책을 생성할 수 있습니다.

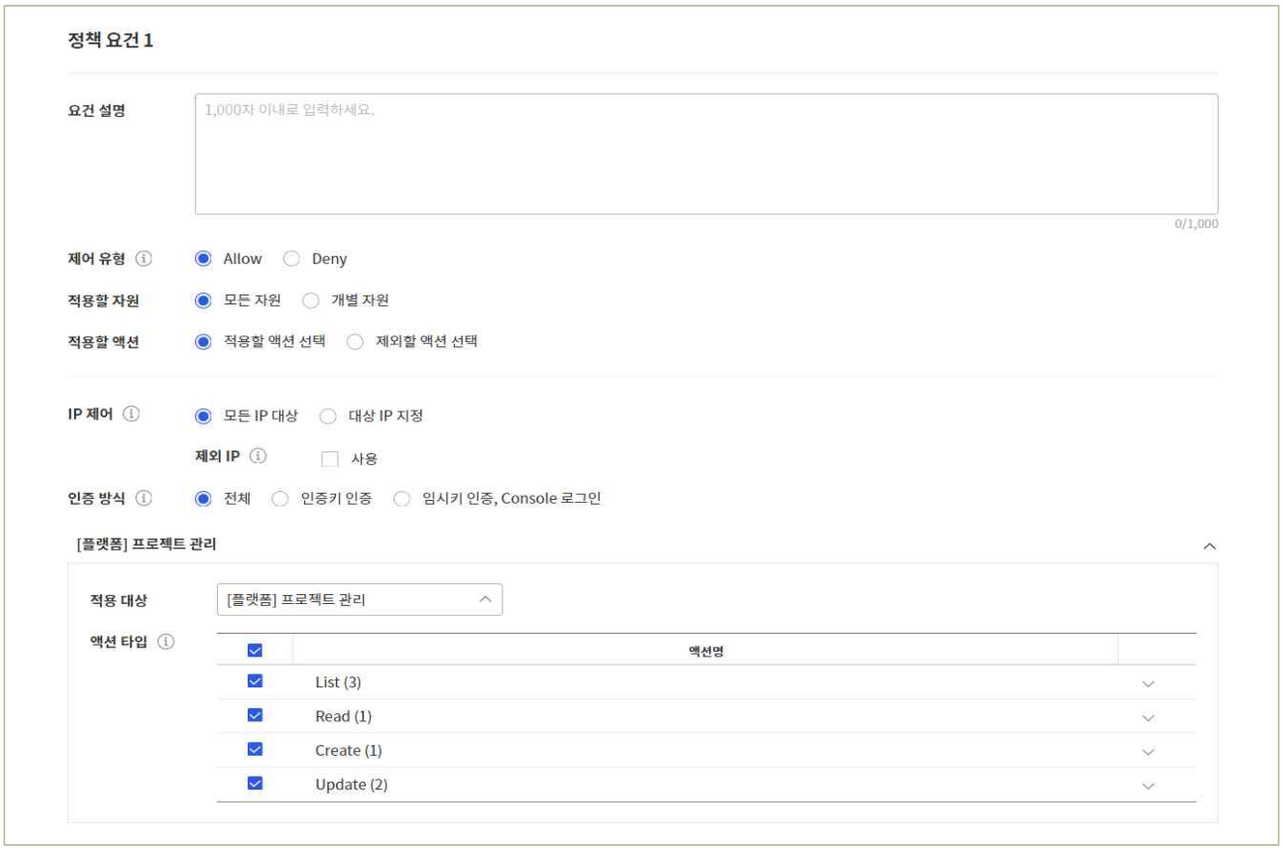
| 그림 3.1.1 | 정책 생성

- 정책명을 입력하고 '다음' 버튼을 클릭하여 정책요건 설정 화면으로 이동합니다.



| 그림 3.1.2 | 정책 기본정보 입력

- 정책요건 설정 화면에서 제어 유형, 적용할 자원, 적용할 액션, IP 제어, 인증 방식, 적용 대상을 선택한 후 '다음' 버튼을 클릭합니다.



| 그림 3.1.3 | 정책요건 설정

- 권한그룹/역할 연결 화면에서 연결할 권한그룹 또는 역할을 선택한 후 '완료' 버튼을 클릭하여 정책 생성을 완료합니다.

| 그림 3.1.4 | 권한그룹과 역할 연결

4 참고 사항

- SCP에서의 '역할'은 사용자의 본래 계정 대신 임시 자격 증명을 통해 프로젝트에 접근할 수 있게 하는 기능으로, 사전에 정의된 행위만이 가능하도록 권한을 관리할 때에는 '정책'을 생성하여 사용해야 합니다.
- 자세한 사항은 Samsung Cloud Platform 콘솔의 '사용자 가이드'를 참고하시기 바랍니다.
  https://cloud.samsungsds.com/manual/ko/scp_user_guide.html#e397ba9859bbae01

1 기준

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

2 설명

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

  - 예시

    1) IAM(Identity and Access Management) 기능 등을 이용하여 이용자별 인증수단 적용

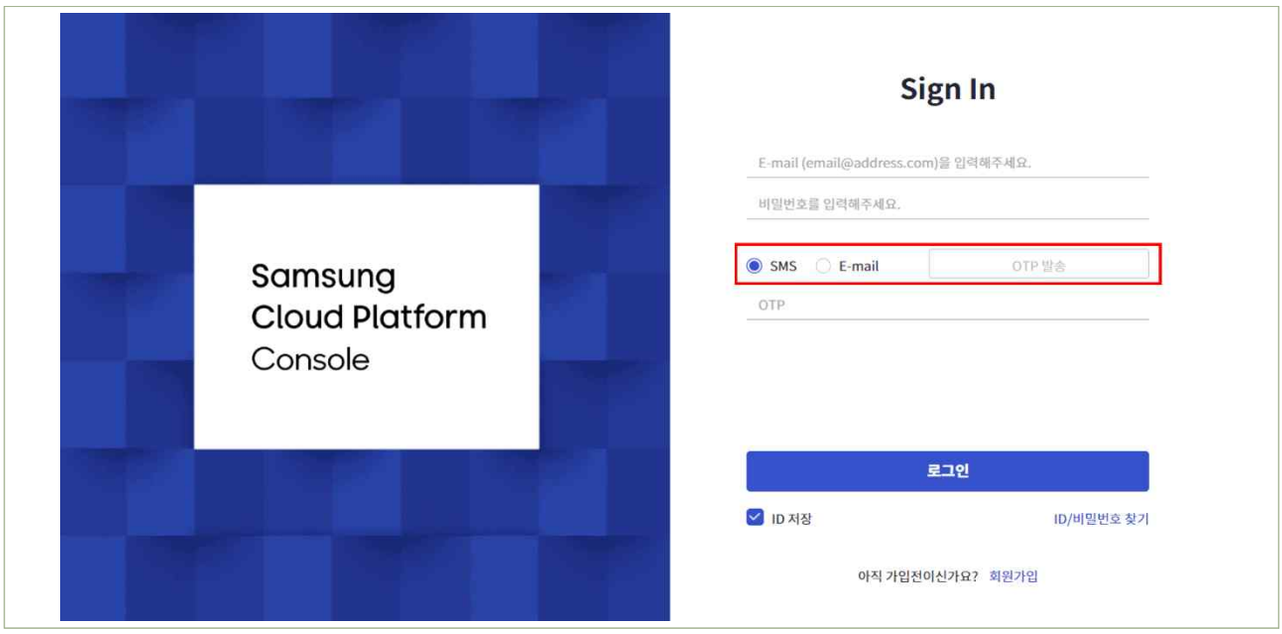
    2) 업무 중요도에 따른 MFA 추가 인증(OTP, 바이오인증 등) 고려

3 우수 사례

1) 업무 중요도에 따른 MFA 추가 인증(OTP, 바이오인증 등) 고려

- 로그인

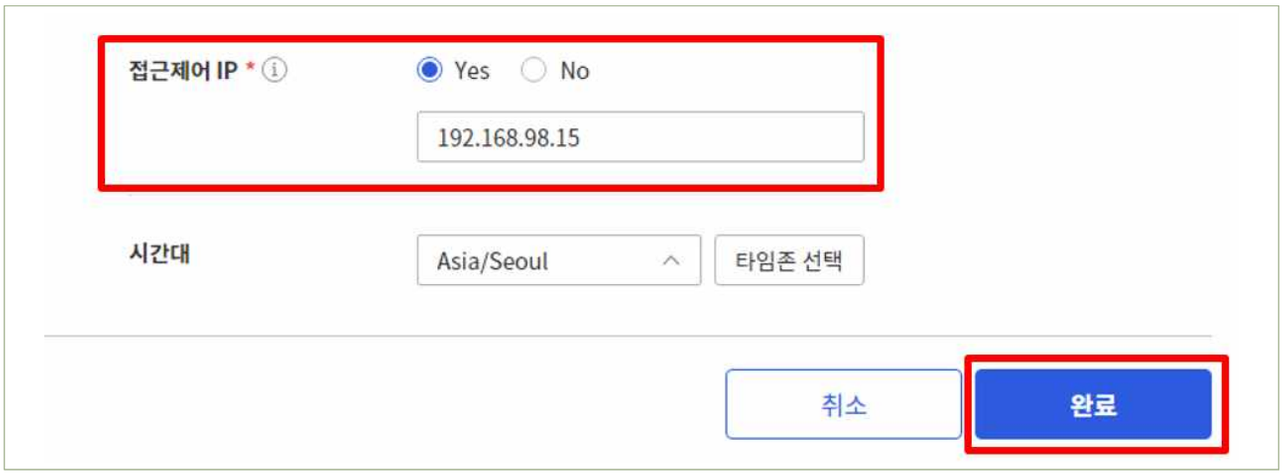
  ① 로그인 시 계정 정보를 입력한 후, SMS 또는 이메일 주소로 OTP를 받아 로그인해야 합니다.



| 그림 3.2.1 | 로그인 시 OTP 인증

- 접근제어 IP 설정을 통한 추가 인증

  ② My 메뉴 → 사용자 정보 설정 → 사용자 정보 탭 → 접근제어 IP 항목을 설정하여 인가받지 않은 사용자의 접근을 차단할 수 있습니다.



| 그림 3.2.2 | 접근제어 IP 설정

4 참고 사항

- 접근제어 IP는 '|'로 구분하여 여러 건을 입력할 수 있습니다.
  (ex. 1.1.1.1|2.2.2.2)
- 접근제어 IP 설정은 일반적인 IPv4 형식과 CIDR 포맷을 허용합니다.

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

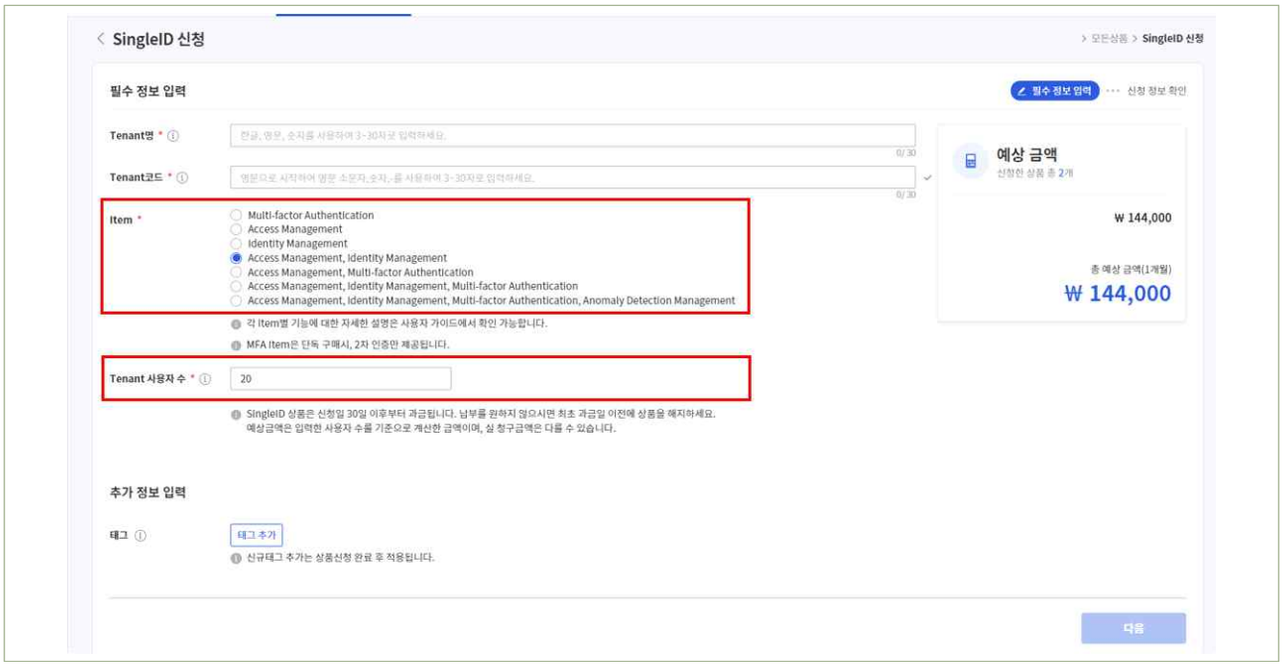
3 우수 사례

1) 인사변경이 발생한 이용자의 계정 삭제 또는 중지

- SCP SingleID를 활용한 계정 관리

  ① 인사변경 사항 발생 시 계정 관리는 고객사 또는 MSP 수행영역이나, SCP의 상품(SCP SingleID)을 활용하여 해당 요건 수행 시 활용 가능

  - SingleID 신청: Security → SingleID → AM, IM



| 그림 3.3.1 | SingleID 예시

[Item] 기능별 Sales Item 선택(7개)

- Multi-Factor Authentication
- Access Management
- Identity Management
- Access Management, Identity Management
- Access Management, Multi-Factor Authentication
- Access Management, Identity Management, Multi-Factor Authentication
- Access Management, Identity Management, Multi-Factor Authentication, Anomaly Detection Management

[Tenant 사용자 수] 과금이 청구되는 기준으로, 항목별 최소 사용자수를 입력

- Multi-Factor Authentication 선택 : 50명 이상 입력
- 그 외 상품 : 20명 이상 입력

4 참고 사항

- SingleID 관련 문의사항은 서포트 센터 〉 1:1 문의를 이용하시기 바랍니다.

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

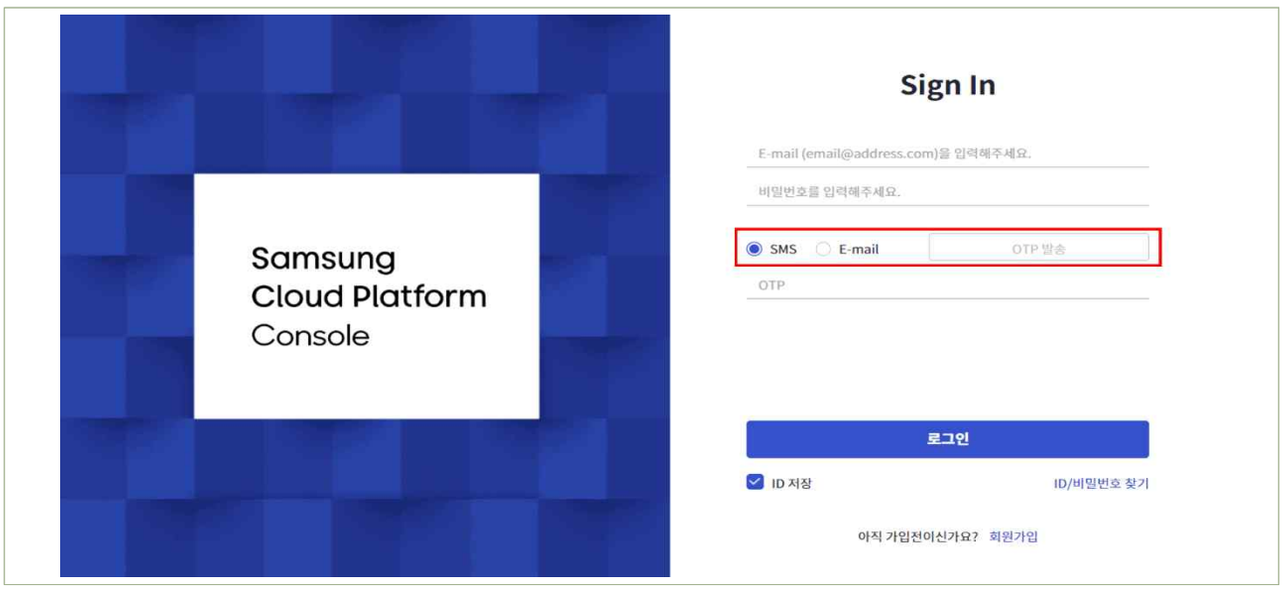
3 우수 사례

1) 이메일 인증 & 2) SMS 인증

- 관리자 로그인

  ① 관리자 로그인 시 SMS 또는 이메일 주소를 통한 OTP 인증이 필요합니다.

  - [관리자], [사용자] 모두 ID/PW 외 추가 OTP 인증을 적용



| 그림 3.4.1 | 관리자 로그인 시 OTP 인증

4 참고 사항

- N/A

1 기준

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

2 설명

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

  - 예시

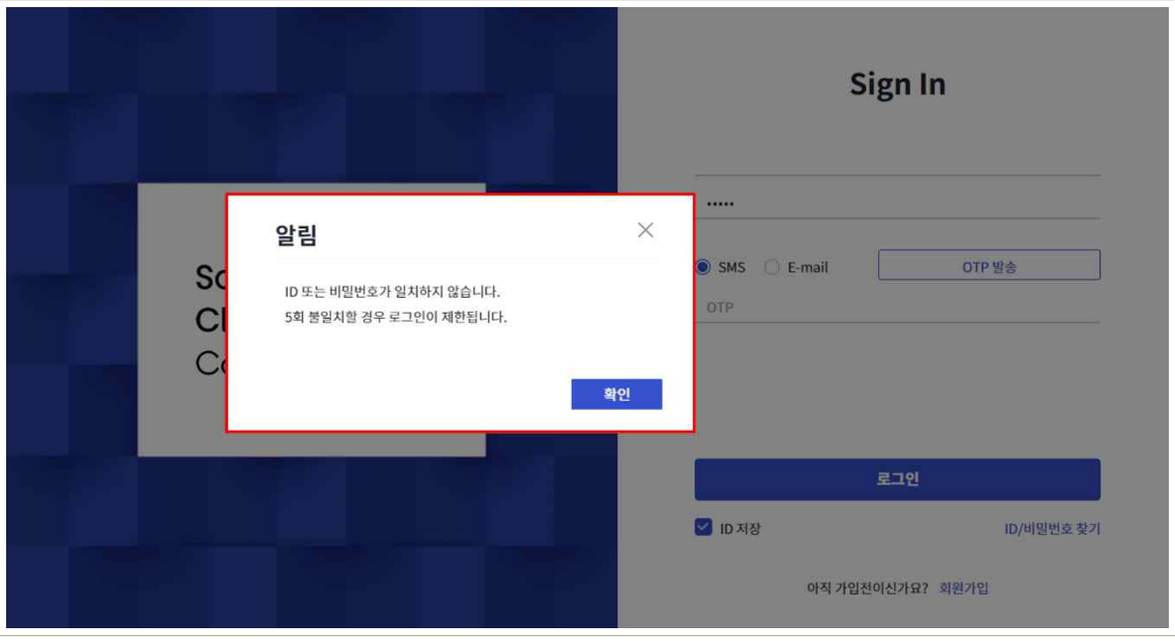
    1) 로그인 오류에 따른 보안통제 방안 수립 등

3 우수 사례

1) 로그인 오류에 따른 보안통제 방안 수립 등

- 로그인 오류 시 보안통제

  ① 로그인 페이지에서 5회 이상 잘못된 ID 또는 비밀번호를 입력할 경우 로그인이 제한됩니다.



| 그림 3.5.1 | 로그인 오류 시 보안통제

② My 메뉴 → 사용자 정보 설정 → 사용자 정보 탭 → 비밀번호 재사용 제한에서 최근 사용한 비밀번호를 재사용하지 못하도록 비밀번호 히스토리를 체크할 수 있습니다.

| 그림 3.5.2 | 비밀번호 재사용 제한 설정

4 참고 사항

- N/A

1 기준

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

2 설명

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

  - 예시

    1) 제3자가 쉽게 유추할 수 없는 비밀번호 작성 규칙 수립

3 우수 사례

1) 제3자가 쉽게 유추할 수 없는 비밀번호 작성 규칙 수립

- 비밀번호 변경

  ① My 메뉴 → 사용자 정보 설정 → 비밀번호 변경에서 아래와 같은 비밀번호 규칙을 적용하여 비밀번호를 설정합니다.

| 그림 3.6.1 | 비밀번호 변경

4 참고 사항

- N/A

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.

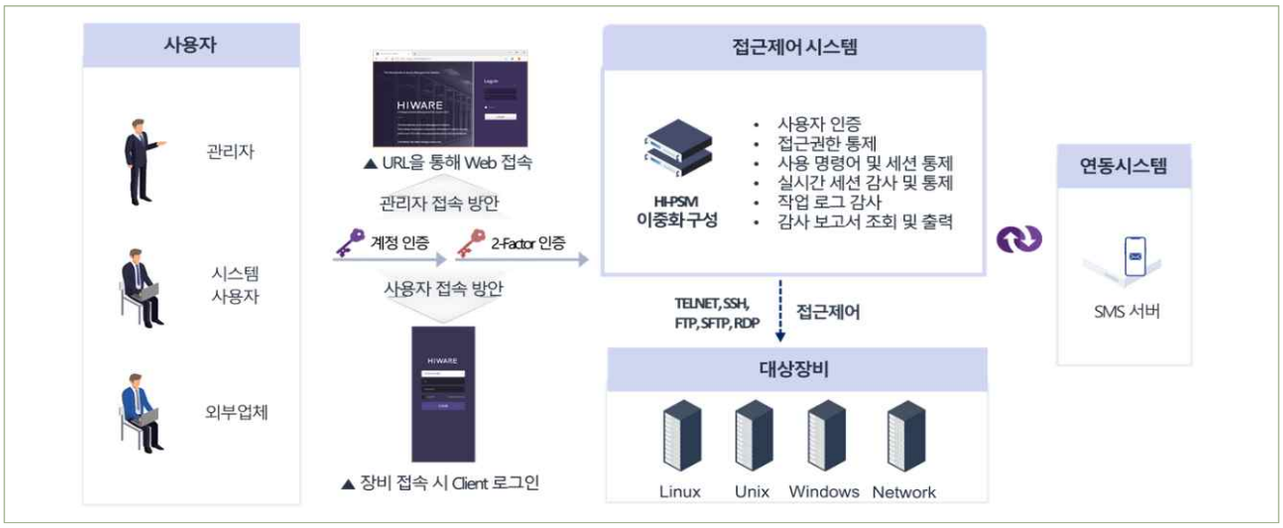
  - 예시

    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

- 공개용 웹서버 접근 계정 제한 관리는 고객사 또는 MSP 수행영역이나, SCP의 특정 상품(3rd Party 솔루션, HI-PSM)을 활용하여 해당 요건수행 시 활용 가능.
- (Samsung Cloud Platform 포탈) 마켓플레이스 → 'HI-PSM'



| 그림 3.7.1 | HI-PSM 활용 사례

[HIWARE Privileged Session Management]

① 원격 접속 프로토콜(Telnet, SSH, FTP, SFTP, RDP)을 이용하여 서버 및 네트워크에 접근하는 사용자의 모든 접속과 작업에 대해 사전 인증 및 접근 권한을 관리

② 인적 실수 또는 장애 발생 시 명백한 감사 자료를 통해 보다 효율적이고 보안성이 강화된 관리 환경을 제공

4 참고 사항

- HIWARE 제품 문의 및 기술지원 창구
  - Website : https://www.netand.co.kr

4. 암호키 관리

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

4 암호키 관리

1 기준

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

2 설명

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

  – 예시

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

3 우수 사례

1) 클라우드의 키 관리 서비스를 통해 CSP 사업자의 관리형 Key로 암호화

- 가상자원(서버)에 대한 암호화 기능 적용

① Compute 생성 시 Key pair를 활용하여 서버 접속 및 관리(Virtual Server, GPU Server)

- Key pair 유출시 서버에 누구나 접속이 가능하므로 안전하게 보관하고 서버 최초 접속 이후 관리자 패스워드 변경 및 새로운 계정을 생성하여 서버에 접속
- 신청 경로: (Compute) 'Project' → '자원관리' → 'Compute' → 'Virtual Server' → '상품 신청' → 이미지 선택 → 상품 구성 선택 및 입력 → 필수 정보 입력 화면의 'Key pair 신규 생성' 또는 '기존 Key pair' 선택

| 그림 4.1.1 | Compute 생성 시 Key pair 활용

A. 최초 1회에 대해서만 Key를 다운로드 가능.
재발급은 제공되지 않으니, 반드시 다운로드 파일 확인 필요

B. 다운로드 받으신 Private Key는 반드시 안전한 곳에 저장

C. 윈도우 OS는 기본 관리자 계정을 사용하기 때문에 최초 접속 시 사용자 계정을 생성하여 사용

D. 리눅스 OS는 최초 접속 시 관리자 계정 비밀번호를 설정

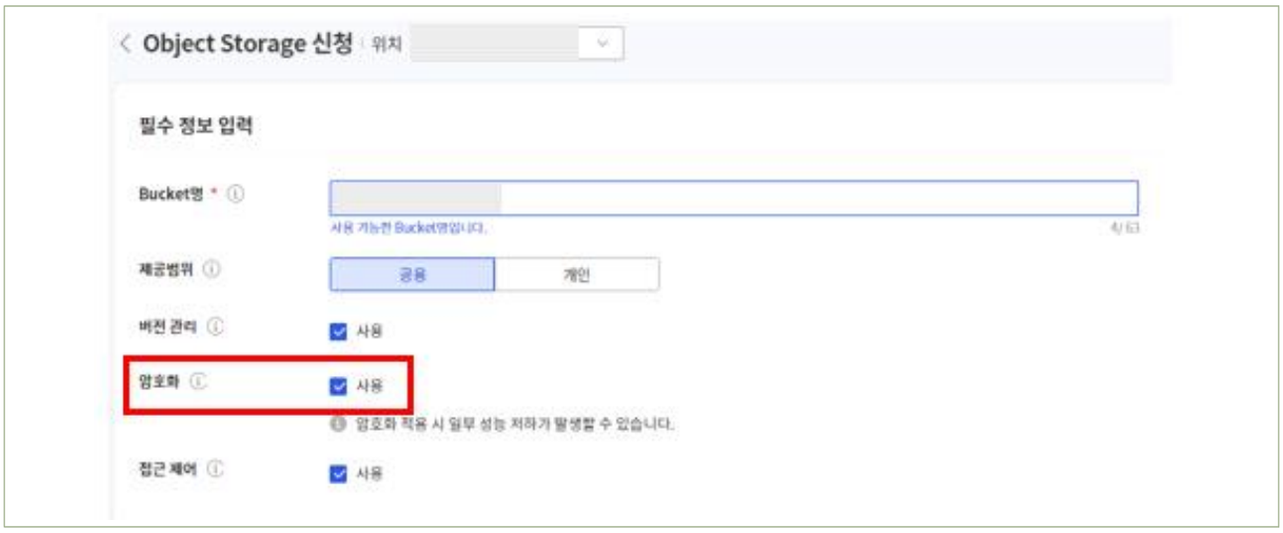
E. Key 공유 시 권한이 있는 사람에게 안전하게 전달

2) 클라우드의 키 관리 서비스를 통해 CSP 사업자의 관리형 Key로 암호화

- 가상자원(스토리지)에 대한 암호화 기능 적용

① Storage 관련 암호화 알고리즘 기능 제공

- SSE-S3(Server Side Encryption-S3)방식으로 제공하고 있으며, bucket 단위로 암호화하여 데이터를 안전하게 보관
- AES-256 방식의 암호화 알고리즘을 통해 데이터가 안전하게 저장
- 신청 경로: (Storage) 'Object Storage' → '상품 신청' → 'Object Storage 신청' 메뉴 이동 → 필수정보 입력 → '암호화'체크



| 그림 4.1.2 | Object Storage 신청 시 암호화 확인

A. 암호화 기능을 SSE-S3(Server Side Encryption-S3)방식으로 제공하고 있으며, bucket 단위로 암호화하여 데이터를 안전하게 보관

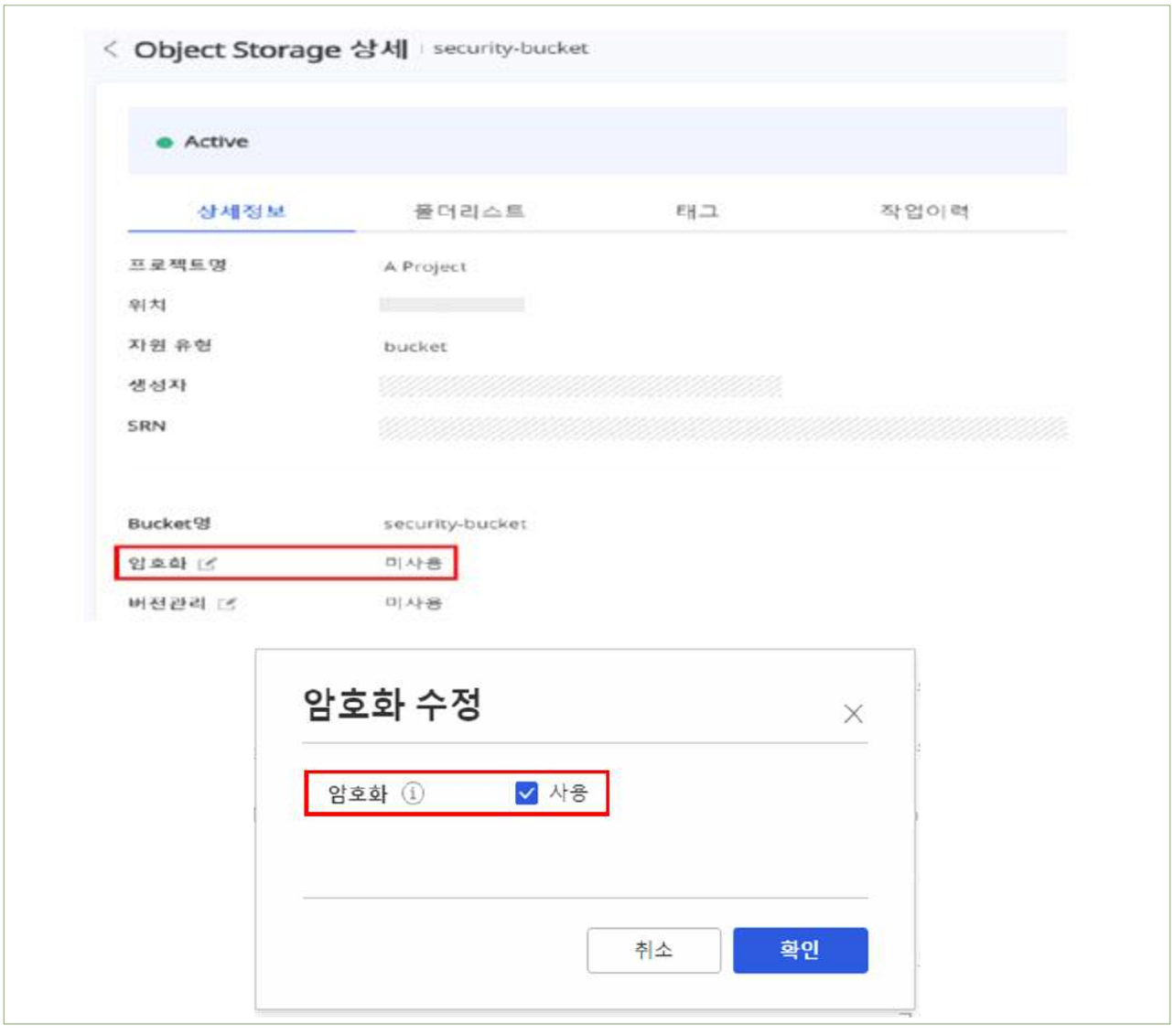
B. AES-256 방식의 암호화 알고리즘을 통해 데이터가 안전하게 저장 및 다운로드 되며, 저장된 데이터는 여러 단계의 보안장비로 안전하게 보호

C. Object Storage Bucket에 저장되는 객체에 대하여 암호화 설정이 필요시 암호화 설정 적용

D. Bucket에 암호화 동작을 설정하여 객체가 Bucket에 저장될 때 암호화

② Object Storage 수정 시

- 신청 경로: ‘Project’ → ‘자원관리’ → ‘Storage’ → ‘Object Storage Bucket’클릭 → 상세정보 확인 → ‘암호화 수정’ → 사용 체크



| 그림 4.1.3 | Object Storage 사용 시 암호화 수정

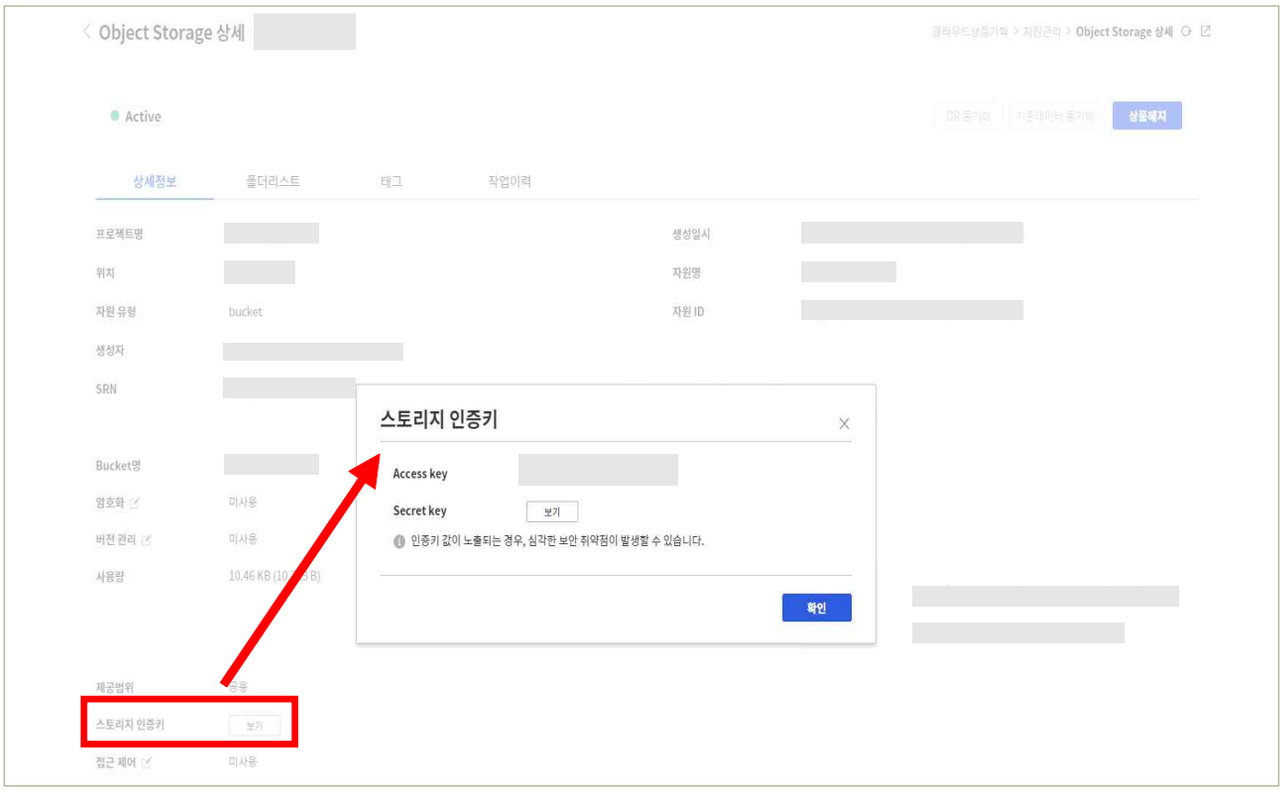
A. 암호화 사용을 선택하면 SSE-S3 암호화 키 방식 및 AES256 암호화 알고리즘 적용

B. Bucket에 암호화 동작을 설정하여 객체가 Bucket에 저장될 때 암호화

C. Object Storage Bucket에 저장되는 객체에 대하여 암호화 설정이 필요시 암호화 설정을 적용

③ Object Storage 사전 작업 조치

- API를 활용하여 Object Storage의 인증키 값이 노출될 경우 심각한 보안취약점이 발생할 수 있어 Key 정보를 안전하게 보관하여 Bucket의 데이터를 안전하게 보호
- 신청 경로: 스토리지 인증키 내 Key 정보 확인 → 'Project' → '자원관리' → 'Storage' → 'Object Storage' → Bucket 클릭 → 상세정보 확인 → 스토리지 인증키 보기 클릭



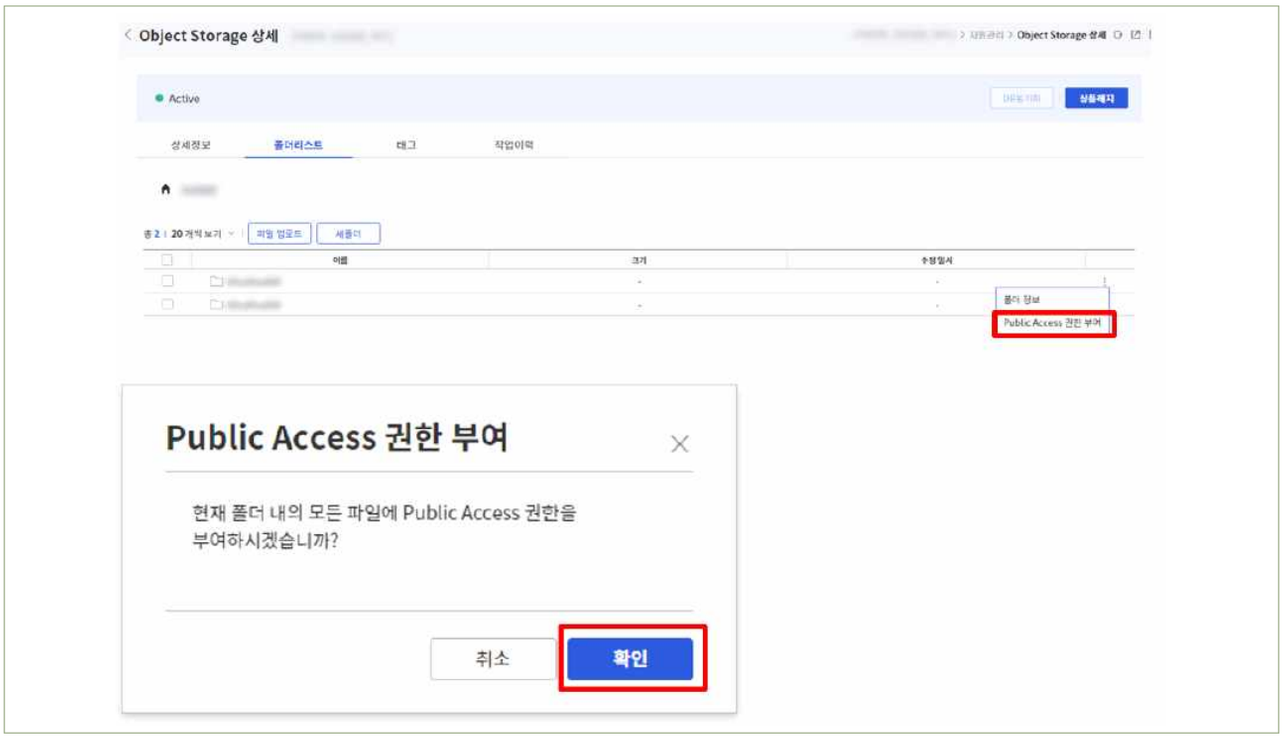
| 그림 4.1.4 | 스토리지 인증키 보기

A. API를 활용하여 Object Storage 활용 시 안전한 Key 관리, 필요 폴더에 한하여 퍼블릭 권한을 부여하여, Bucket의 데이터를 안전하게 보호

B. Object Storage의 인증키 값이 노출될 경우 심각한 보안취약점이 발생할 수 있어 Key 정보를 안전하게 보관하여, Bucket의 데이터를 안전하게 보호

④ 폴더 파일리스트 Public Access 권한 부여

- Public Access 권한을 부여한 폴더의 경우 Key 없이 폴더 접근 가능. 안전한 사용을 위해 Public 권한 부여 사용은 자제하고 필요한 폴더에 한하여 접근제어를 적용한 후 사용 권고
- 신청 경로: (Storage) → 'Object Storage' → 'Object Storage 자원 관리하기' → 폴더 관리하기



| 그림 4.1.5 | Public Access 권한 부여

※ 공용 Access Key와 Secret Key는 각 Samsung Cloud Platform의 AZ별로 Project 단위로 1개씩 발급

※ 개인 Access Key와 Secret Key는 각 Samsung Cloud Platform의 AZ별로 사용자 단위로 1개씩 발급

⑤ Block Storage 암호화

- Block Storage(VM) 신청 시
  - 신청 경로: ‘Project’ → ‘자원관리’ → ‘Storage’ → ‘Block Storage(VM)’ → ‘상품 신청’ → 암호화 체크 후 생성

| 그림 4.1.6 | Block Storage 암호화

- Block Storage(BM) 신청 시
  - 신청 경로: ‘Project’ → ‘자원관리’ → ‘Storage’ → ‘Block Storage(BM)’ → ‘상품 신청’→ 암호화 체크 후 생성

| 그림 4.1.7 | Block Storage 암호화 적용

A. Block Storage 생성 시 암호화를 설정하여 Block Storage Volume을 암호화
B. Block Storage 생성 시 설정한 암호화 사용 여부는 수정 불가능

4 참고 사항

- 「Samsung Cloud Platform 보안가이드」에서는 VPN을 통한 보안 침해 방지를 위하여 송수신 되는 데이터를 안전한 암호화 알고리즘으로 암호화하는 방법에 대해 소개되어 있으므로, 더 자세한 내용은 해당 가이드 참조
  (https://cloud.samsungsds.com/manual/ko/scp_user_guide.html#96a737e02d536b95)

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

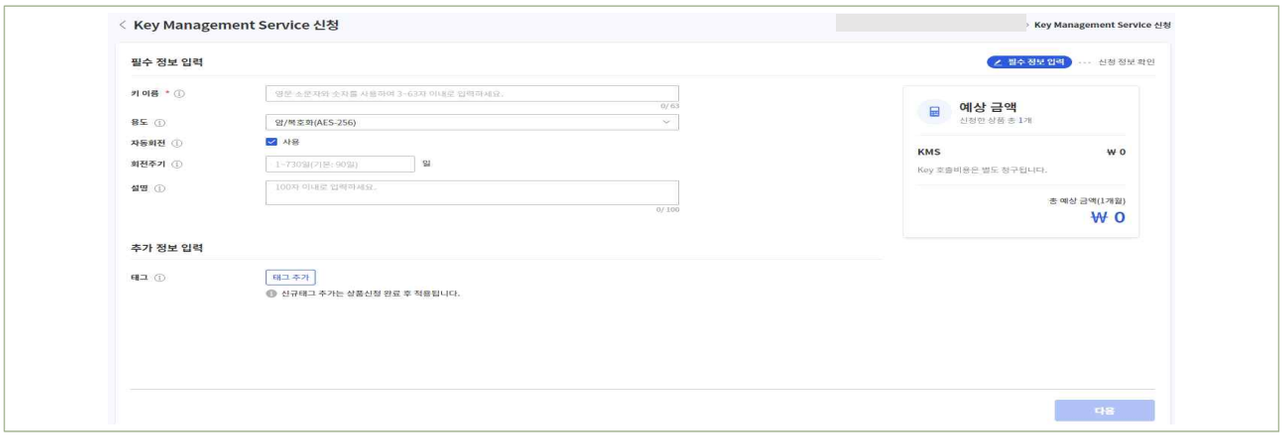
    1) KMS(Key Management Service)를 통한 암호키 방안 수립(생성, 변경, 폐기 등)
    2) 클라우드 서비스 제공자가 직접 제공하는 암호키 이용 시 적절한 관리방안 수립
    3) 키 사용기간 수립 및 암호키 유출 등에 대응할 수 있도록 키 삭제 및 재적용 관련 기능 수립
    4) 생성된 암호키를 안전하게 보관할 수 있는 방안 수립 등

3 우수 사례

1) KMS를 통한 암호키 방안 수립(생성, 변경, 폐기 등)

- KMS는 암호키를 편리하게 생성하고 안전하게 보호하는 키 관리 서비스로 암호키의 보안을 위해 주기적으로 키 회전을 실행하고, 사용 권한 및 접근 권한 관리 가능

  ① KMS 신청



| 그림 4.2.1 | KMS 상품 신청

A. 키의 용도 및 암호화 방식 선택

- 암호화/복호화(AES-256) : 대칭 키 방식의 AES-256 키를 생성해 최대 32 KB 데이터 암호화에 이용
- 암호화/복호화 및 서명/검증(RSA-2048) : 비대칭 키 방식의 RSA(2048 bit) 키를 생성해 최대 190B 데이터 암호화 또는 8KB 서명에 이용.
- 서명/검증(ECDSA) : 비대칭 키 방식의 ECDSA 키를 생성해 최대 8KB 데이터 서명에 이용

[KMS 키(Master Key)]

- 사용자가 Key Management Service 상품에서 생성한 키이며, 생성 및 회전, 삭제, 권한 관리까지 모두 사용자의 관리 하에 운영
- Key Management Service 상품 관리자나 Key Manager 권한을 가진 사용자는 Samsung Cloud Platform에서 편리하게 키 관리 가능
- KMS 키가 데이터 키를 생성 및 보호하는데 사용되기 때문에 Master Key로 명명
- 일반적으로 대칭 암호화 KMS 키를 사용하지만 서명 및 검증에 비대칭 KMS 키 사용 가능

[데이터 암호화]

- 데이터 암호화는 KMS 키 또는 데이터 키를 사용하여 평문 데이터를 해석이 불가능한 암호화된 데이터로 변환하는 것을 의미
- 암호화된 데이터는 키를 통해서만 복호화 가능

[데이터 키(Data Key)]

- 데이터 암/복호화에 직접 이용되는 키로 사용자가 직접 관리 영역에 안전하게 보관 필요
- KMS의 CreateDataKey API를 이용하여 데이터 키를 생성
- KMS에서 생성한 KMS 키를 통해 데이터 키를 보호한다면 관리적 측면에서 부담 감소
- API를 이용하면 즉시 사용할 수 있는 일반 텍스트 키와 이를 KMS 키로 암호화된 형태 확보
  A. 키의 자동회전 사용을 선택하면 설정한 회전주기마다 생성한 키의 내부 알고리즘을 다른 값으로 변환하여 적용
  B. 키의 회전주기는 1~730일 사이의 값을 입력할 수 있으며, 회전주기를 입력하지 않으면 90일로 자동 설정

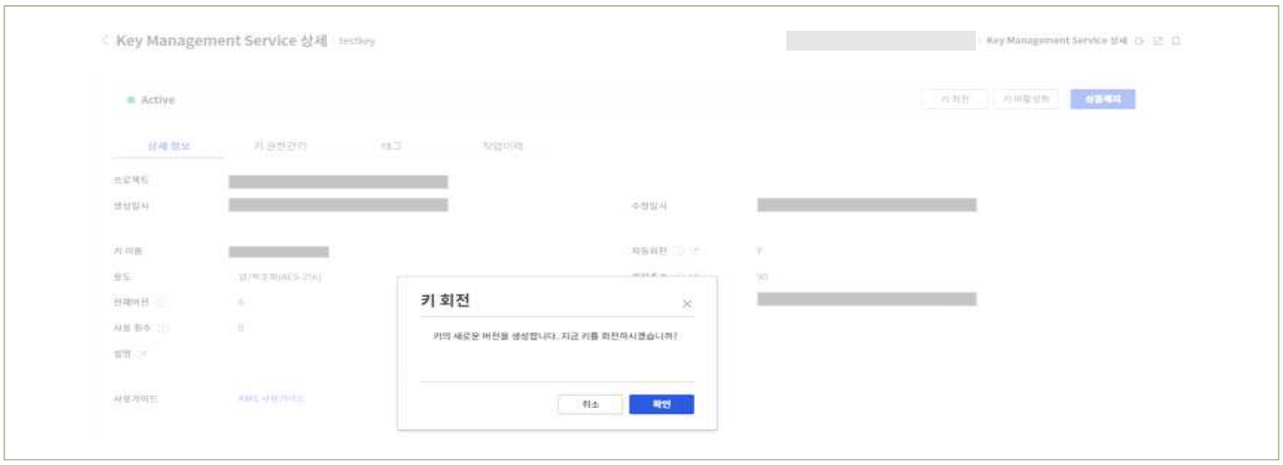
2) 클라우드 서비스 제공자가 직접 제공하는 암호키 이용 시 적절한 관리방안 수립

- 키 회전 이후 버전이 변경되는 경우, 현재 버전 이전의 키는 더 이상 암호화에 사용 불가(복호화 용도로만 사용 가능)

① KMS 신청 및 키 변경(키 회전)

- 신청 경로 : (KMS) → '자원관리' → Security 탭에서 'Key Management

② Service' → KMS 상세 페이지로 이동 → '키 회전'



| 그림 4.2.2 | KMS 변경(키 회전)

A. 회전주기: 자동회전 사용 시 회전주기를 표시

B. 현재버전: 키의 현재 버전을 표시하며, 키가 회전할 때마다 자동으로 버전이 1씩 증가

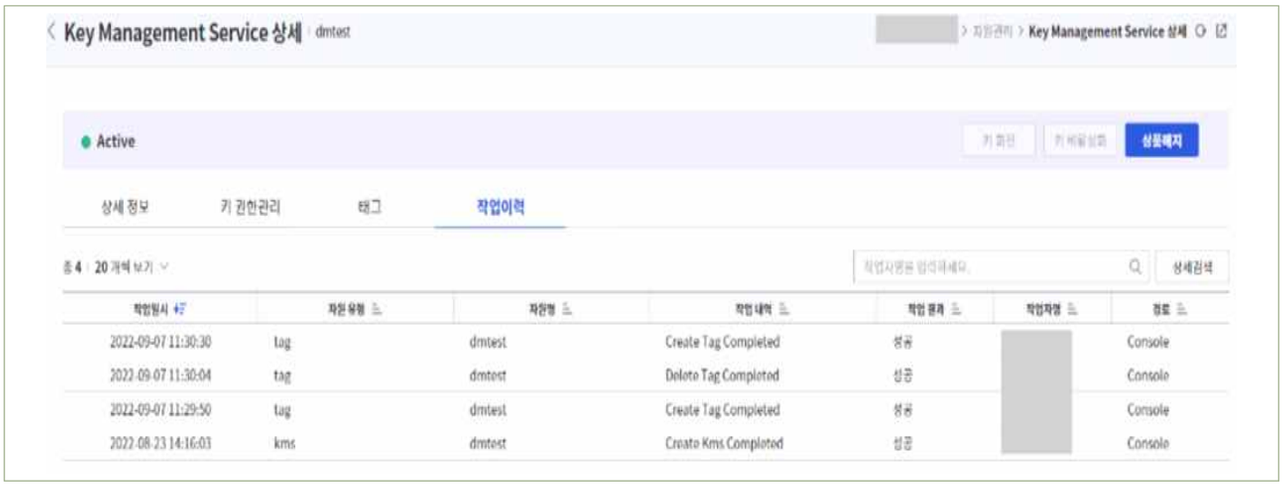
C. 다음회전일: 키의 다음 회전일을 표시하며, 해당 날짜에 자동으로 키 회전 실행

3) 키 사용기간 수립 및 암호키 유출 등에 대응할 수 있도록 키 삭제 및 재적용 관련 기능 수립

- 키를 해지하면 KMS의 모든 요청 및 기능을 사용할 수 없으며, 72시간 후 영구적으로 삭제

① 키 해지

- 신청 경로: (KMS) → '자원관리' → 'Security'탭에서 'Key Management Service' → KMS 상세 페이지로 이동 → '상품해지'에서 '키 해지'



| 그림 4.2.3 | Key Management Service 폐기(해지)

A. KMS 상세 페이지 상단의 상품해지를 클릭해도 선택한 항목 해지 가능

B. 상품 해지를 취소하려면 KMS 목록 페이지 또는 상세 페이지에서 해지취소 버튼 클릭

※ 상품 해지 취소 팝업창에서 확인을 클릭하면 선택한 키는 삭제되지 않고 비활성화 상태로 복구

※ 키를 다시 사용하려면 상세 페이지에서 키 활성화 버튼을 클릭

① 키 해지 취소

- 키 해지 취소 선택 시, 선택한 키는 삭제되지 않고 비활성화 상태로 복구되며, ‘키 활성화’ 클릭시 키 재적용으로 사용가능한 상태로 변경
- 신청 경로: (KMS) → ‘자원관리’ → ‘Security’ → ‘Key Management Service’ → KMS 상세 페이지로 이동 → ‘상품해지’ → ‘해지취소’

| 그림 4.2.4 | 키 삭제 및 재적용(해지취소)

A. 상품 해지 취소 팝업창에서 확인을 클릭하면 선택한 키는 삭제되지 않고 비활성화 상태로 복구

B. 키를 재사용하려면, 상세 페이지에서 키 활성화 버튼을 클릭

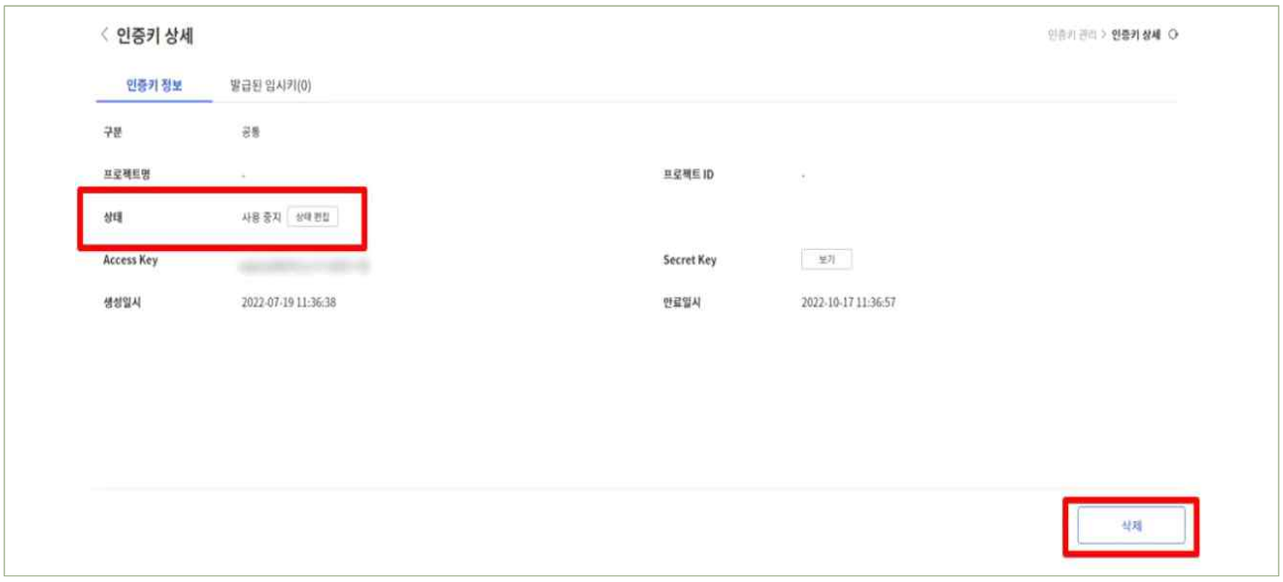
4) 생성된 암호키를 안전하게 보관할 수 있는 방안 수립

- 암호키를 안전하게 보관할 수 있는 방안은 프로젝트 관리자 권한을 가진 계정의 프로그래밍 방식 사용을 제한하기 위해 인증키/임시키 발급이력 현황 확인
  - ① 인증키 생성 일시 확인 후 주기적으로 인증키 교체
    - 신청 경로: (Management) '인증키 관리 → 사용자 계정 로그인 → 우측 상단 사용자 아이콘 → 인증키 관리 → 인증키 발급 현황 확인

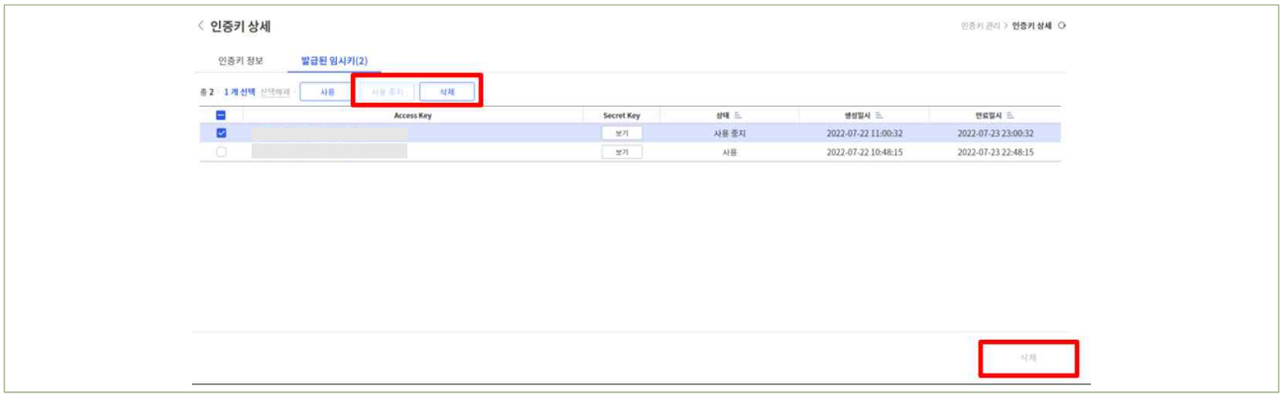
| 그림 4.2.5 | 인증키 발급 현황 확인

② 인증키 삭제: 인증키/임시키에 IP기반의 접근제어를 수행하여 인가받지 않은 사용자의 접근 차단

- 신청 경로: (Management) '인증키 관리' → 인증키 선택 → 삭제 또는 사용중지 상태로 변경



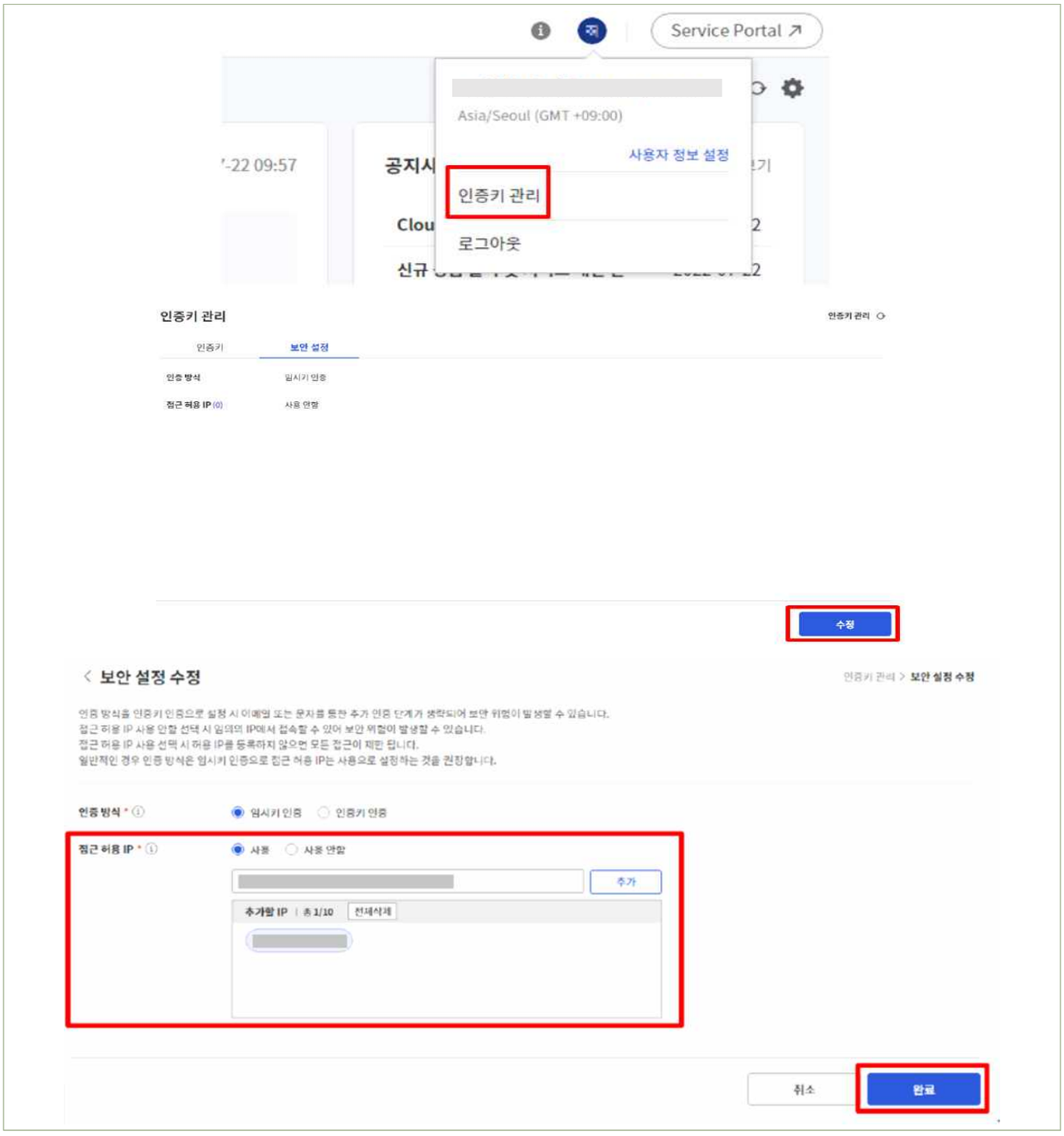
| 그림 4.2.6 | 인증키 사용중지



| 그림 4.2.7 | 인증키 삭제

③ 인증키/임시키에 대해 사용자 IP 기반의 접근제어

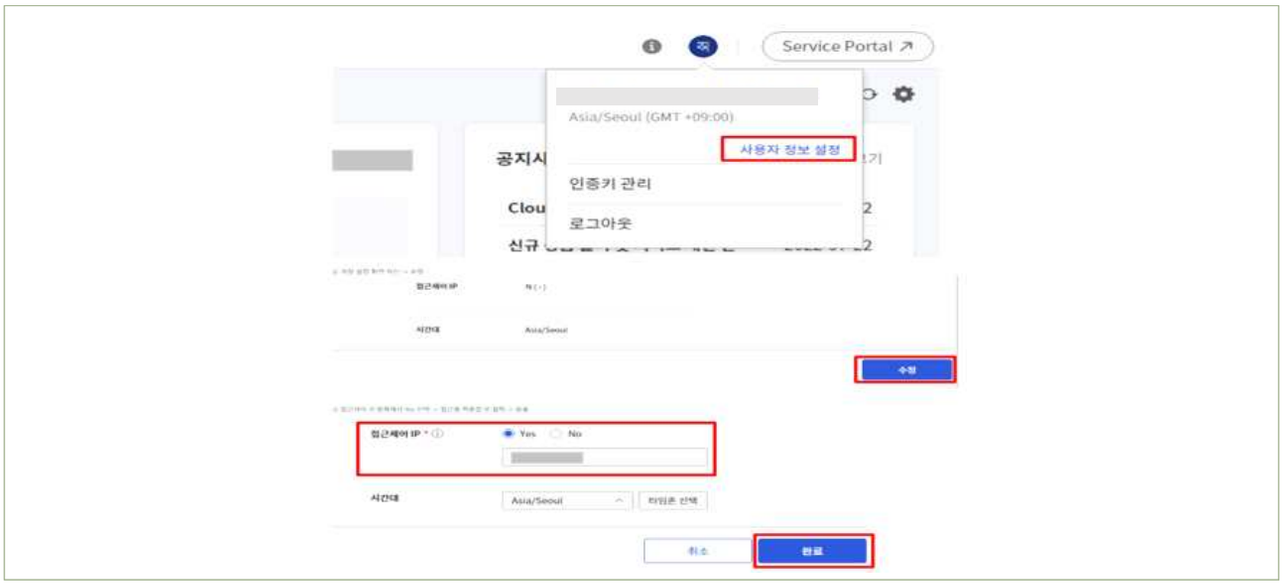
- 인증키/임시키에 IP 기반의 접근제어를 수행하여 인가 받지 않은 사용자의 접근을 차단하여, 인증키/임시키에 대해 사용자 IP 기반의 접근제어 수행
- 신청 경로: (Management) '인증키 관리' → '보안 설정 확인하기'
  - 사용자 계정 로그인 → 우측 상단 사용자 아이콘 → 인증키 관리
  - 보안 설정 탭 → 수정
  - 보안 설정 수정 → 접근 허용 IP 사용 체크 후 IP 추가 → 완료



| 그림 4.2.8 | 인증키/임시키 관련, 사용자 IP 기반의 접근제어

A. 사용 설정 시 특정 IP의 접근만 허용(최대 10개까지 등록)
※ 사용 안 함 설정 시, 전체 IP 접근 허용
B. 사용 설정 후 IP 미등록 시 모든 IP 접근 거부

④ 인증키/임시키에 대해 사용자 IP 기반의 접근 차단
- SCP 콘솔 계정에 대해 사용자 IP 기반의 접근제어 수행을 위해, 콘솔 사용자 IP 기반의 접근제어를 수행하여 인가 받지 않은 사용자의 접근 차단
- 신청 경로: (Management) '인증키 관리'→ '보안 설정 수정하기'→ 접근제어 IP 입력

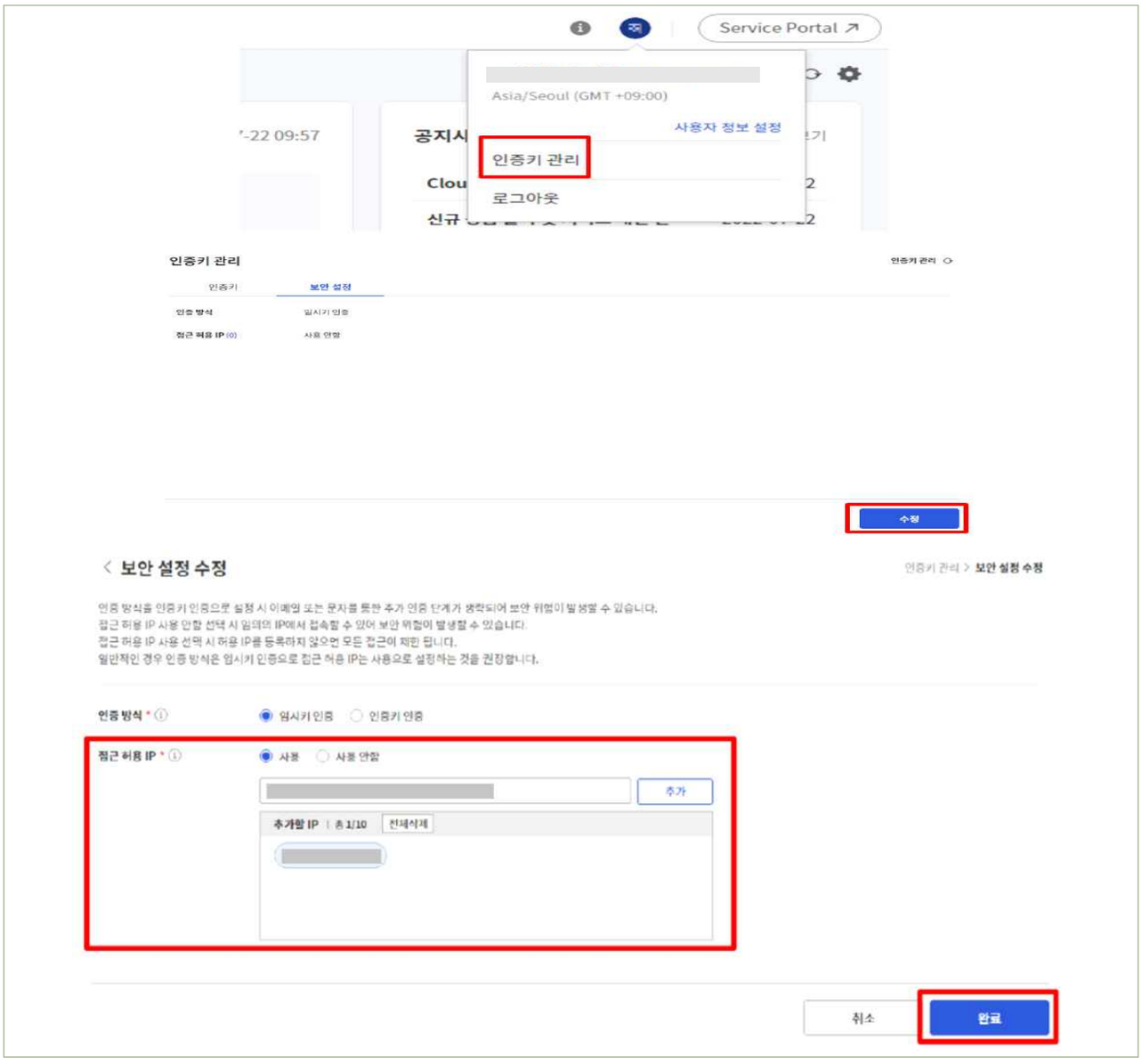


| 그림 4.2.9 | 보안 설정(접속제어 IP 지정)

A. 사용자 계정 로그인 → 우측 상단 사용자 아이콘 → 사용자 정보 설정
B. 계정 설정 화면 하단 → 수정
C. 접근제어 IP 항목에서 Yes 선택 → 접근 허용 IP 입력 → 완료
D. 접근제어 IP를 설정하면, 설정한 IP만 접근 허용
※ 접근제어 IP는 '|' 로 구분하여 여러 건 입력
※ 접근제어 IP 설정: 일반적인 IPv4 형식과 CIDR 포맷 허용

⑤ 임시키 인증방식으로 설정 시 MFA(SMS, E-mail 추가인증) 적용

- 인증키를 이용한 API 호출 차단 및 API 호출 시 임시키를 이용한 방식만 허용하기 위해, 임시키 인증방식으로 설정 시 MFA(SMS, E-mail 추가인증)적용 되어 인증키 인증방식보다 안전한 사용 가능
- 신청 경로: (Management) '인증키 관리' → '보안 설정 수정하기' → 접근허용 IP 입력



| 그림 4.2.10 | 보안 설정(접속허용 IP 지정)

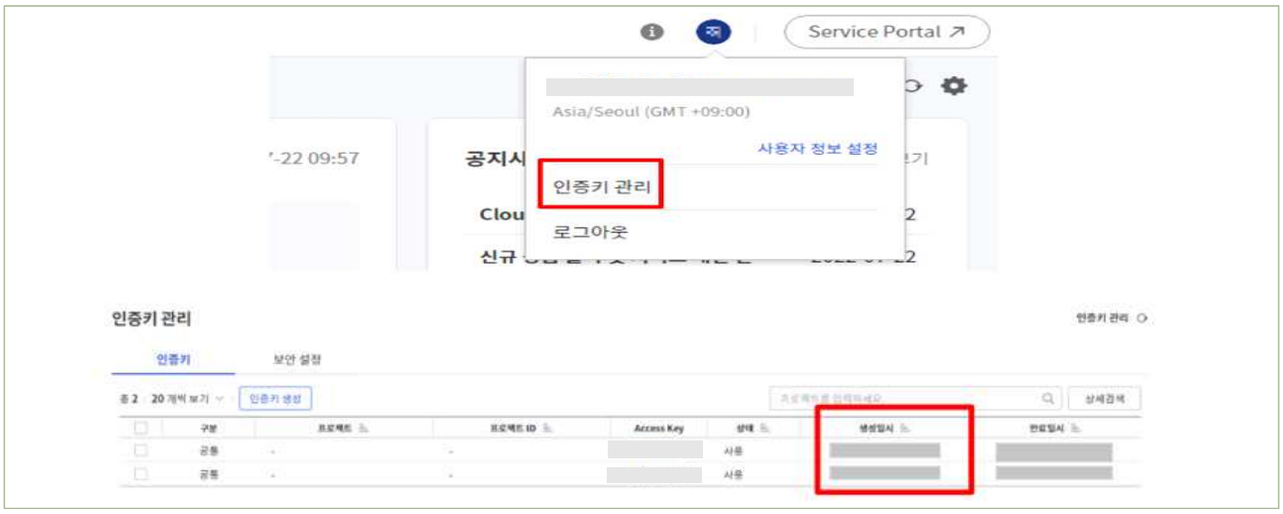
A. 사용자 계정 로그인 → 우측 상단 사용자 아이콘 → 인증키 관리

B. 보안 설정 탭 →수정

C. 보안 설정 수정 → 인증 방식에 임시키 인증 체크 → 완료

⑥ 안전한 인증키 관리

- 인증키를 안전하게 보관하여 프로그래밍 방식 액세스 권한 부여로 보안성을 강화하여 인증키를 안전하게 보관
- 신청 경로: (Management) '인증키 관리'→ '인증키 관리하기'



| 그림 4.2.11 | 안전한 인증키 보관

A. 인증키는 주기적으로 변경

B. 인증키는 평문으로 저장하거나 공유폴더에 저장하면 안 됨.

※ 공유폴더, Object Storage, Bastion Host 등

C. 소스코드 내 인증키, 임시키를 평문으로 포함하지 않음.

4 참고 사항

- 위 가이드는 정보제공의 목적으로만 제공되며, 키설정 변경 시 충분한 사전 영향도 검토가 필요
- 「Samsung Cloud Platform 사용자 가이드」에서는 KMS 키를 활용한 암호화 예제가 소개되어 있음. 더 자세한 내용을 알고 싶으시면 해당 가이드 참조 (https://cloud.samsungsds.com/manual/ko/scp_user_guide.html#encryption_example_utilizing_kms_key)

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 상시 모니터링 수행

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

3 우수 사례

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

- 정책 생성, 권한그룹 추가 등 권한 설정을 위해서는 해당 프로젝트 관리자 권한 필요(권한그룹 - AdministratorGroup)

  ① '권한그룹/역할연결'에서 정책에 연결한 권한그룹과 역할을 선택하여 연결 가능

  - 신청 경로: (Security) 'Key Management Service 신청' → 'Key Management Service 상세' → '키 권한 관리' → 정책 탭 → '정책 생성' → '정책요건 설정'

| 그림 4.3.1 | 정책요건 설정

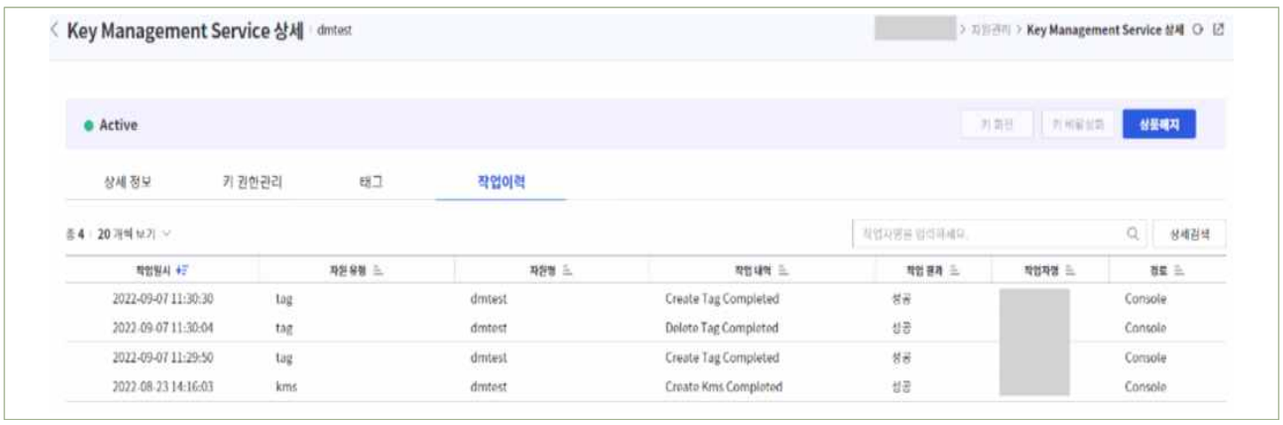
A. 하나 이상의 적용 대상이 추가되어야 정책 요건 설정이 완료

B. 정책요건 설정 항목 중 적용 대상, 액션 타입만 가이드에 따라 설정

- Key Manager : List, Read, Create, Update, Delete
- Key Encryptor/Decryptor : List, Read, Update
- Key Encryptor : List, Read
- Key Decryptor : List, Update

② 역할부여 현황에 대한 상시 모니터링

- 신청 경로: (KMS) 'KMS 작업이력 확인하기' → '상세검색' 클릭 → 상시 모니터링(작업일시, 작업 결과, 경로, 작업자명) 확인 가능



| 그림 4.3.2 | 역할 현황 관련 상시 모니터링

A. 검색 영역에 찾고자 하는 검색어를 입력하여 검색

※ 권한그룹명: 향후 관리를 위해 기존에 생성한 KMS 정책명과 동일하게 입력/권장

B. 상세검색을 클릭하여 작업일시, 작업 결과, 경로, 작업자명으로 상세검색

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

- 권한그룹을 추가하려면 권한관리 〉 권한그룹 탭 〉 권한그룹 추가 클릭
  (권한그룹 - AdministratorGroup)

| 그림 4.3.3 | 권한그룹과 역할연결

A. 권한그룹명은 향후 관리를 위해 기존에 생성한 KMS 정책명과 동일하게 입력하도록 권장

※ Key Manager,Key Encryptor, Key Decryptor, Key Encryptor/Decryptor

B. 권한그룹에 기존에 생성한 KMS 정책을 연결하고 해당 권한을 부여할 사용자를 추가

4 참고 사항

- 「Samsung Cloud Platform 사용자 가이드」에서는 키 사용 권한 관련 자세한 내용이 소개되어 있음. 더 자세한 내용을 알고 싶으시면, '프로젝트 권한 관리하기' 참고.
  (https://cloud.samsungsds.com/manual/ko/scp_user_guide.html#e397ba9859bbae01)

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) 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

1) 암호키 관리 서비스(KMS)를 통해 암호키 호출 시 목적에 따라 권한 부여

- '키 권한 변경/해지하기'에서 KMS에 연결된 권한그룹, 정책 및 사용자를 변경하거나 해지 등록된 키의 새로운 버전을 생성하거나 사용 상태를 변경할 수 있음.

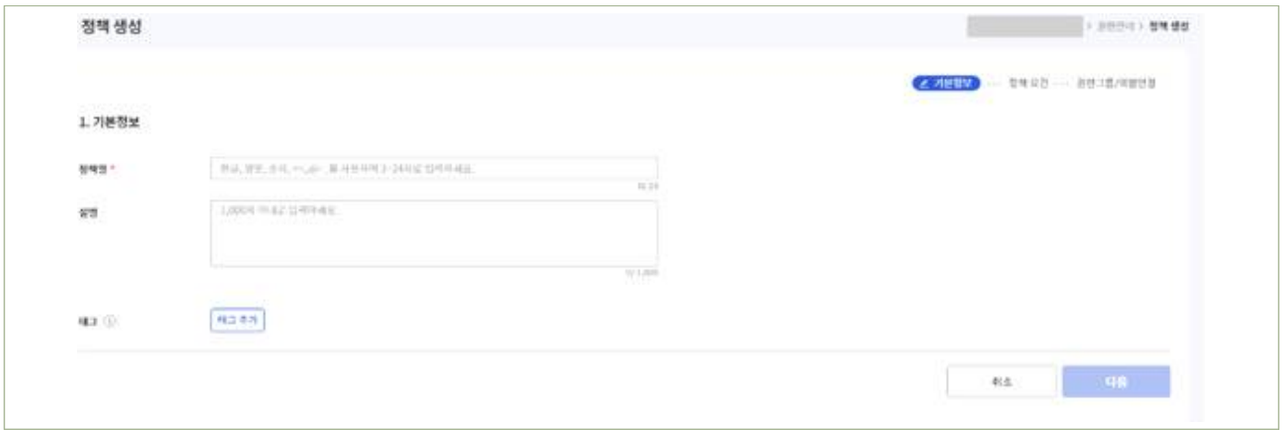
  ① 키 권한설정

  - 신청 경로: (Security시스템) 'Key Management Service 신청' → 'KMS 상세정보 확인하기' → 'KMS 키 권한 관리하기' → '키 권한 설정하기' → '키 권한 변경/해지'

| 그림 4.4.1 | KMS 키 권한 관리하기

A. 등록된 키 권한을 확인하고 관리할 수 있음.

B. 정책 생성, 권한그룹 추가 등 권한 설정을 위해서는 해당 프로젝트 관리자 권한 필요(권한그룹 – AdministratorGroup)



| 그림 4.4.2 | KMS 키 권한 설정

A. 정책명 : 권한에 맞는 정책명 입력

※ KeyManager : 키를 생성/조회/삭제, 암/복호화 및 서명/검증 전체 기능을 사용할 수 있는 관리자 정책

※ KeyEncryptor : 키 조회, 암호화 및 서명 기능만 사용할 수 있는 사용자 정책

※ KeyDecryptor : 키 조회, 복호화 및 검증 기능만 사용할 수 있는 사용자 정책

※ KeyEncryptor/Decryptor : 키 조회, 암/복호화 기능을 사용할 수 있는 사용자 정책

B. 설명: 정책에 대한 설명 입력.

C. 태그 : 정책에 추가할 태그를 선택(최대 50개까지 등록 가능)

② 키 권한 변경/해지하기

- 신청 경로: ‘프로젝트 권한 관리하기‘ → ‘정책 설정하기’ → ‘정책 수정하기’ → KMS에 연결된 권한그룹, 정책 및 사용자를 변경 또는 해지

| 그림 4.4.3 | KMS 키 권한 변경/해지

A. KMS에 연결된 권한그룹, 정책 및 사용자를 변경 또는 해지

③ 정책요건에 개별 자원 추가

- 자원 목록에서 원하는 자원을 선택
- 신청 경로: (권한관리 IAM) → 정책 탭 → '정책 상세' → 정책 요건 → 수정 → 적용자원 항목 → 개별 자원 → 적용 대상과 원하는 액션 타입 선택

| 그림 4.4.4 | KMS 정책요건에서 자원선택

| 그림 4.4.5 | KMS 정책요건에서 개별자원 추가하기

A. 액션 선택: 액션 유형이 표시되며, 각 액션 유형을 클릭하면 포함된 상세 액션 목록이 표시.
※ 직접 입력: 액션명을 직접 입력하여 추가 가능

B. 자원 항목에서 “자원 추가를 클릭하세요.” 자원 추가 팝업창 확인

C. 추가 방식을 선택한 후, 원하는 자원을 추가

D. 추가하려는 자원의 정보를 직접 입력.

④ 암/복호화 기능이 호출 현황 관련 모니터링

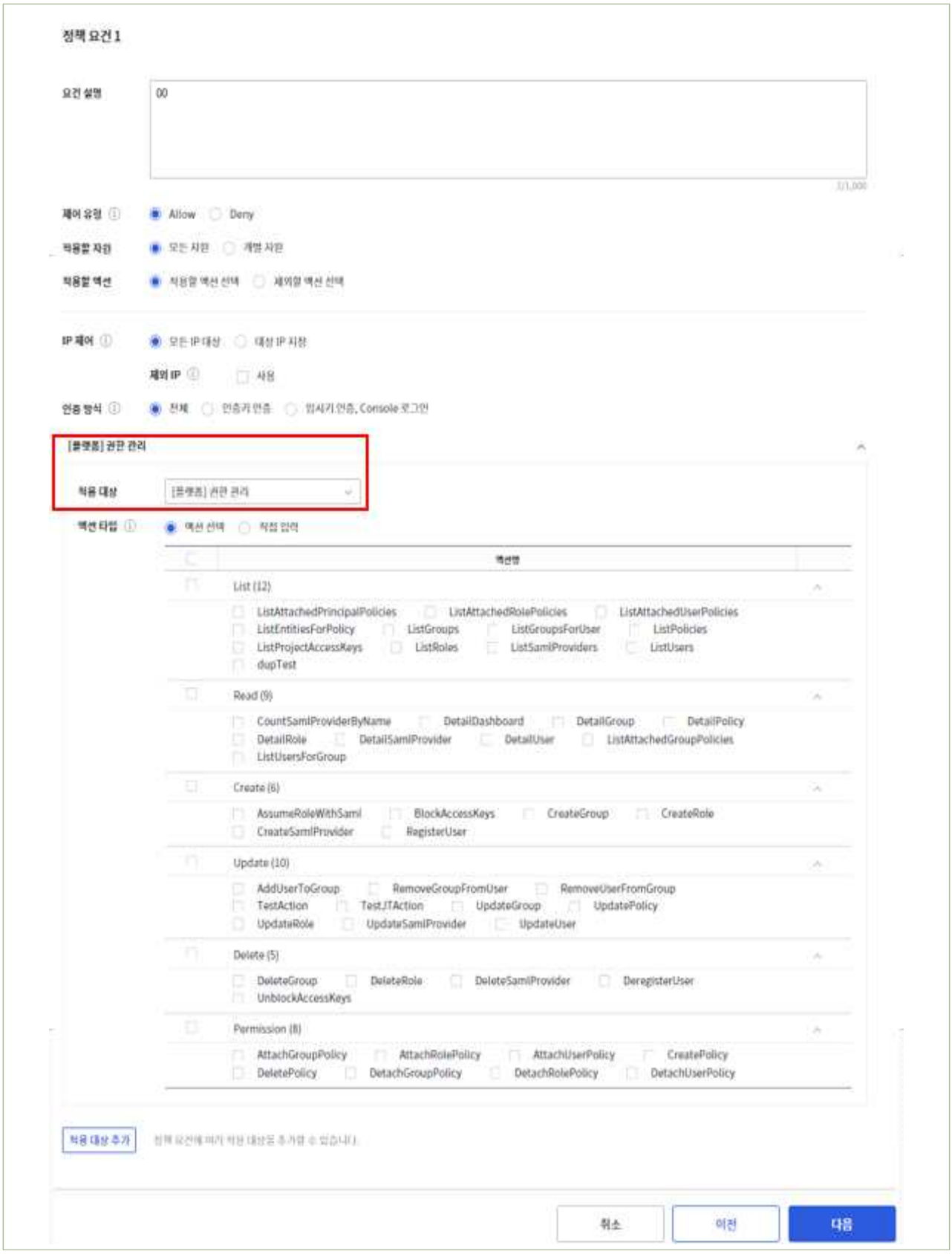
- 사용 중인 키의 상세 정보 및 상태 확인 및 필요한 경우 설정 변경
- 신청 경로: (Security) ‘Key Management Service 신청’ → ‘KMS 상세정보 확인하기’ → 키 정보의 사용 횟수(키를 사용해 암/복호화 기능이 호출된 현황 관련 모니터링

| 그림 4.4.6 | 암호키 호출 권한 현황에 대한 모니터링

A. 모니터링 콘솔을 이용하려면 각 상품에 대한 정책을 생성하고 모니터링 권한을 설정
B. 모니터링은 Samsung Cloud Platform Console에서 운영하는 프로젝트의 자원 운영 현황을 모니터링하고 분석할 수 있는 자원 관리 시스템으로 사용자는 대시보드 화면과 위젯, 차트 기능을 이용하여 프로젝트의 자원을 효율적으로 관리 가능
C. 사용자는 Samsung Cloud Platform 포털에서 사용 권한을 가지고 있는 프로젝트만 모니터링 가능
D. 모니터링 대상에 대한 권한이 없는 경우, 사용자 권한 확인 메시지가 팝업으로 표시.

⑤ 암호키 호출 권한 현황 모니터링

- 암호키 호출 권한 세팅으로 암호키 호출 현황에 대한 모니터링 설정
- 신청 경로: (Monitoring) → ‘권한관리(IAM)’ → 정책 탭 → '정책 생성' → 기본 정보 입력 → Key와 Value를 입력하여 태그 설정 또는 태그 추가 → 정책 요건 설정 → '적용 대상' → 적용 대상과 원하는 액션 타입 선택→액션 선택에서 모니터링을 위한 권한 선택



| 그림 4.4.7 | 암호키 호출 권한 현황에 대한 모니터링 설정

A. 각 정책 요건에 설정된 접근 제어 옵션과 액션 타입 확인

B. 정책 요건의 내용을 적용할 대상을 선택

C. 정책 요건의 내용을 적용할 대상 추가

D. 정책 요건의 내용을 적용할 액션 그룹을 목록에서 선택하면, 선택한 적용 대상과 관련이 있는 액션 그룹만 표시

※ List 〉 ListMonitor: 모니터링 목록 확인 권한

※ MonitorView: 모니터링 보기 권한

※ MonitorSet: 모니터링 보기 및 설정 권한

4 참고 사항

- 「Samsung Cloud Platform 사용자 가이드」에서는 암호키 호출 권한 현황에 대한 모니터링 방법이 소개되어 있음. 더 자세한 내용을 알고 싶으시면, 'Cloud Monitoring 사용자 가이드' 참고 (https://cloud.samsungsds.com/manual/ko/eb51f69cbb399c18.html)

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.

  - 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

1) 이용자가 관리하는 암호키로 암호화 기능 적용

- OpenAPI 보안 인증키를 통해, HMAC SHA256 알고리즘으로 암호화 후 Base64 인코딩

  ① 그룹 별 인증키

  - 삼성 클라우드 플랫폼은 2개의 인증키 값을 이용하고 그룹(프로젝트) 단위로도 인증키를 받아 사용 가능
  - OpenAPI 사용자를 고려하여 프로젝트 단위의 키를 별도로 발행하여 보안을 강화

  ② MFA

  - OpenAPI를 사용하려면 MFA(Multi-factor authentication) 적용으로 인해 임시키를 발급을 받아 인증키와 임시키를 쌍으로 사용하여 MFA 적용을 통해 보안 강화

  ③ HMAC 알고리즘

  - OpenAPI 인증키는 HMAC MAC SHA256 알고리즘으로 암호화 후 Base64로 인코딩

  ④ IP 접근제어

  - OpenAPI는 IP 접근제어 기능이 적용 되어, 높은 보안 수준이 요구되는 경우 외부망으로부터 지정되지 않는 IP의 API 호출 제한 가능
  - AES-256 방식의 암호화 알고리즘(볼륨별 암호화 기능)을 통해 고객의 중요한 데이터를 안전하게 저장 및 다운로드 되며, 저장된 데이터는 여러 단계의 보안장비로 안전하게 보호

2) OpenAPI 호출 절차

① 인증키 생성 및 관리

- 신청 경로: (Management) 콘솔 내 '사용자 아이콘' → '인증키 관리'→ 'API 불러오기'
- Open API 서비스는 인증키 또는 임시키를 통한 사용자 인증만 허용
- 사용자는 Secret Key를 이용하여 API 요청 정보를 HMAC(Hash-based Message Authentication Code) 형식의 Signature를 생성 후, OpenAPI 요청과 함께 서버에 전달하고, 서버에서 Access Key와 Signature를 이용하여 사용자 인증을 처리
- 요청으로부터 서명할 문자열을 생성하고 Access Secret Key로 HMAC SHA256 알고리즘으로 암호화 후 Base64 인코딩하고, 이 값을 x-Cmp-Signature로 사용

② 인증키는 주기적으로 교체

- 신청 경로: (Management) 콘솔 내 '사용자 아이콘' → '인증키 관리'→'신규 인증키 생성'
- 인증키를 안전하게 보관하여 프로그래밍 방식 액세스의 보안성을 강화하고, 인증키 생성일시 확인 후 주기적으로 인증키 교체

| 그림 4.5.1 | Access Key, Access Secret Key 확인

A. 인증키 목록에서 발급받은 Access Key, Access Secret Key 확인
※ 인증키 : 사용자 인증키(최대 2개) 또는 프로젝트별 인증키(최대 2개)

B. 인증키로 로그인 하려면 '인증키 관리' 페이지에서 인증키를 생성하고, 보안 설정 탭에서 인증 방식을 인증키 인증으로 설정 필요

C. 인증키는 평문으로 저장하거나 공유폴더에 저장하지 않도록 유의
※ 공유폴더, Object Storage, Bastion Host 등

D. 소스코드 내 인증키, 임시키를 평문으로 포함되지 않도록 유의

③ API 호출 및 알고리즘

- 신청 경로: (Management) 콘솔 내 '사용자 아이콘' → '인증키 관리'→'API 불러오기'
- Open API 서비스는 인증키 또는 임시키를 통한 사용자 인증만 허용
- Access Key와 Secret Key는 한 쌍으로 구성
- 사용자는 Secret Key를 이용하여 API 요청 정보를 HMAC(Hash-based Message Authentication Code) 형식의 Signature를 생성 후 OpenAPI 요청과 함께 서버에 전달하고, 서버에서 Access Key와 Signature를 이용하여 사용자 인증을 처리
- 호출 API 요청으로부터 서명할 문자열을 생성하고 Access Secret Key로 HMAC SHA256 알고리즘으로 암호화 후 Base64 인코딩하고, 이 값을 x-Cmp-Signature로 사용

```
curl -i -X GET
-H "X-Cmp-AccessKey:
-H "X-Cmp-Signature:

-H "X-Cmp-Timestamp:
-H "X-Cmp-ClientType:
-H "X-Cmp-ProjectId:
'{URL}/iam/v2/access-keys
```

| 그림 4.5.2 | 인증 파라미터를 사용한 API 호출 예시

A. X-Cmp-AccessKey : Samsung Cloud Platform 포털에서 발급받은 Access Key를 입력

B. X-Cmp Signature : 호출 API 요청을 Access Key와 매핑되는 Access Secret Key로 암호화한 서명, HMAC 암호화 알고리즘은 HMAC SHA256 사용

C. X-Cmp-Timestamp : 1970 년 1 월 1 일 00:00:00 협정 세계시부터 경과 시간을 1/1000초(Millisecond) 단위로 정의

D. X-Cmp-ClientType : Client Type을 입력(OpenApi)

E. X-Cmp-ProjectId : API를 실행하려는 프로젝트의 아이디를 입력

④ 데이터를 알고리즘으로 암호화

- VPN을 통한 보안 침해 방지를 위하여 송수신 되는 데이터를 안전한 암호화 알고리즘으로 암호화

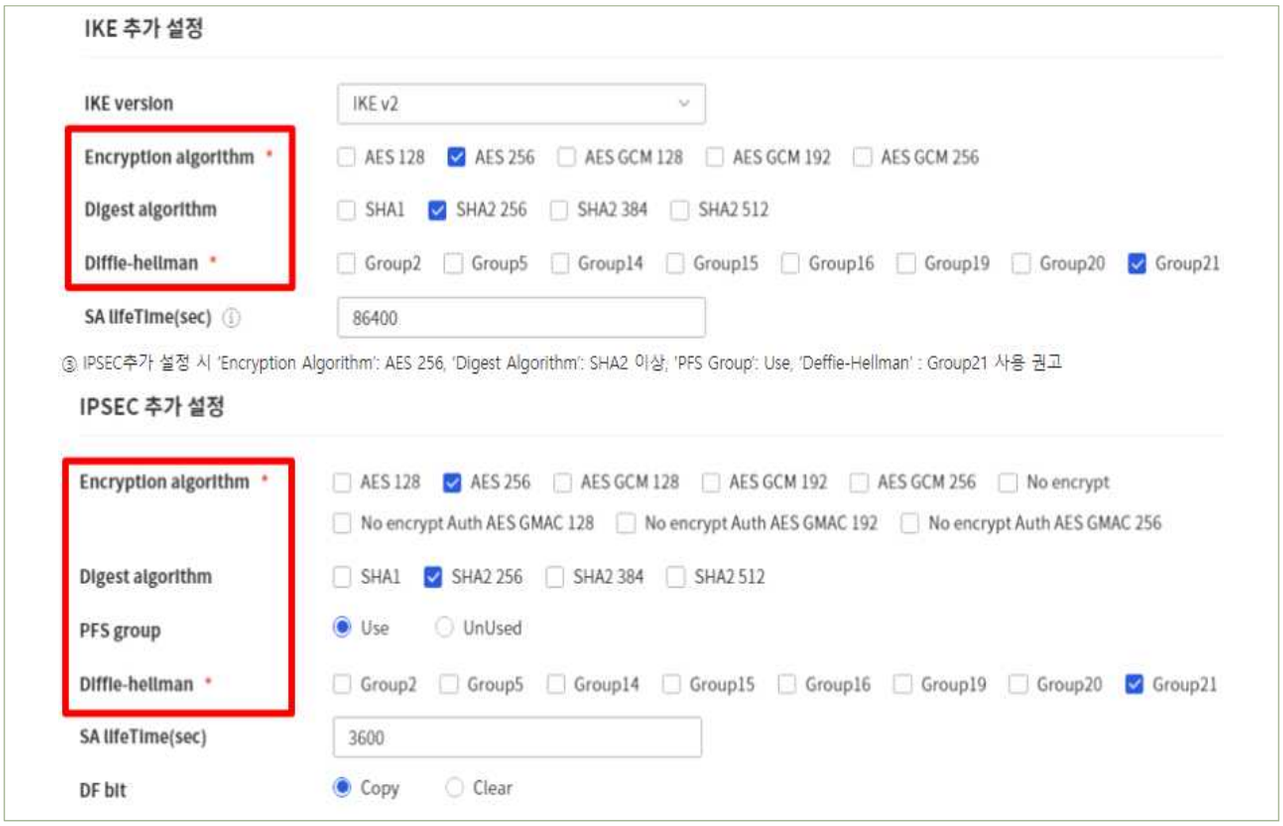
- 안전한 VPN 생성을 위해, VPN 인증 방법과 송수신되는 패킷의 암호화 알고리즘 등 세부사항 결정 필요
- 신청 경로: 'Project' → '자원관리' → 'Networking' → 'VPN' → 'VPN Tunnel' → VPN Tunnel 생성 → 'Pre-shared Key'
  : 32 character 이상 길이

| 그림 4.5.3 | VPN Pre-shared key, IKE, IPSEC설정/확인

A. 업무상 필요한 사용 대역 IP 혹은 호스트 IP만 등록하여 향후 원치 않는 호스트로 접속이 되지 않도록 보안 설정 필요

⑤ IKE추가 설정

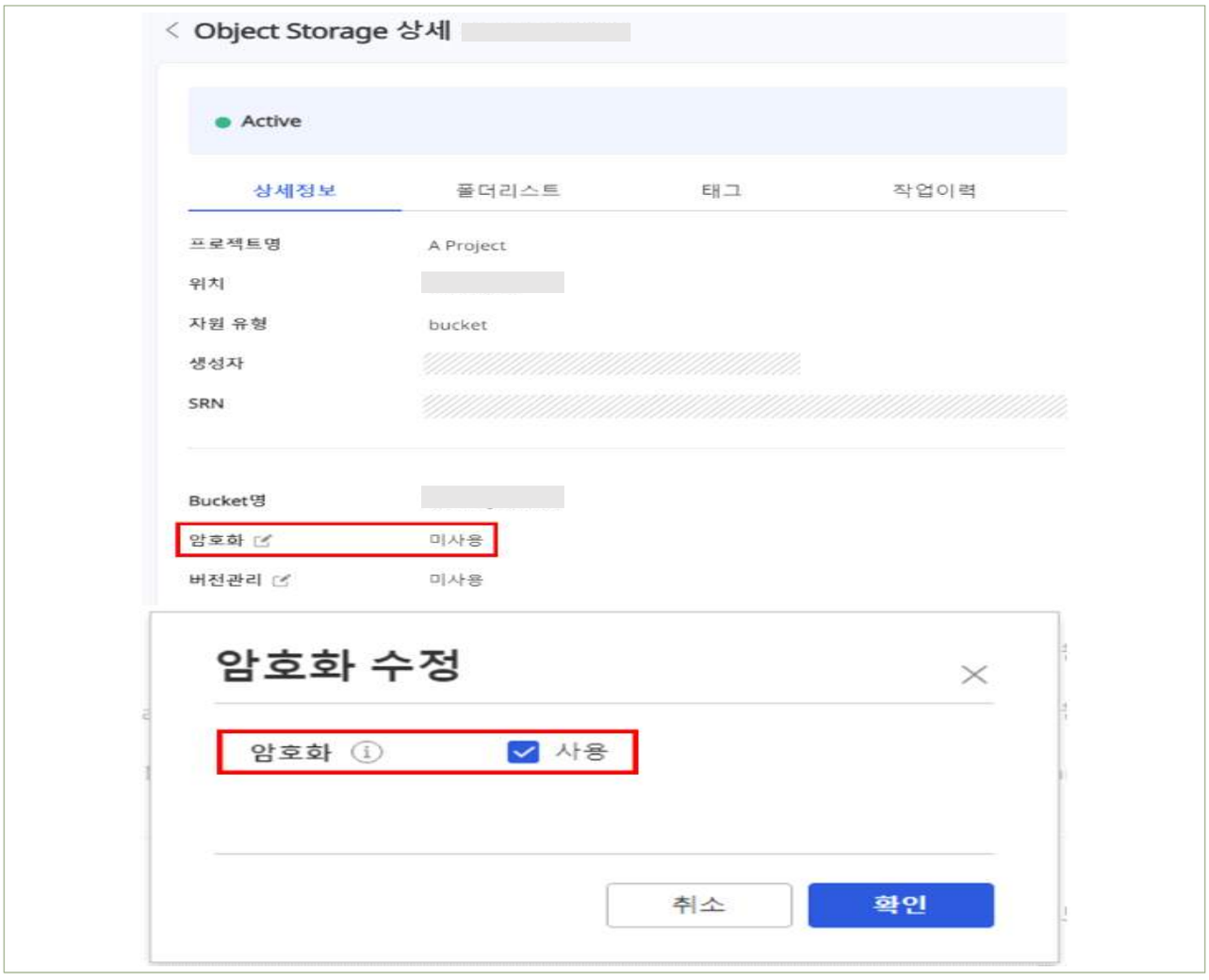
- IKE추가 설정 시 'Encryption Algorithm' : AES 256, 'Digest Algorithm': SHA2 이상, 'Deffie-Hellman' : Group21 사용 권고



| 그림 4.5.4 | IKE 추가설정, IPSEC 추가설정

⑥ Object Storage 암호화

- Object Storage Bucket 암호화 기능을 SSE-S3(Server Side Encryption-S3) 암호화 키 방식 및 AES256 암호화 알고리즘 적용하여, Bucket 단위로 암호화하여 데이터를 안전하게 보관
- 신청 경로: (Storage) 'Object Storage' → 'Object Storage 신청하기 → ' Object Storage 상세정보 확인하기' → 암호화 수정 → 체크



| 그림 4.5.5 | Object Storage를 사용하여 안전하게 보관

2) KMS 서비스를 통해 암호화 시 안전한 암호화 알고리즘을 제공

- KMS가 지원하는 암호화: AES-256, RSA-2048, ECDSA
- KMS는 애플리케이션의 중요한 데이터를 안전하게 보호하기 위해, 암호키를 간편하게 생성하고 안전하게 저장/관리하는 서비스

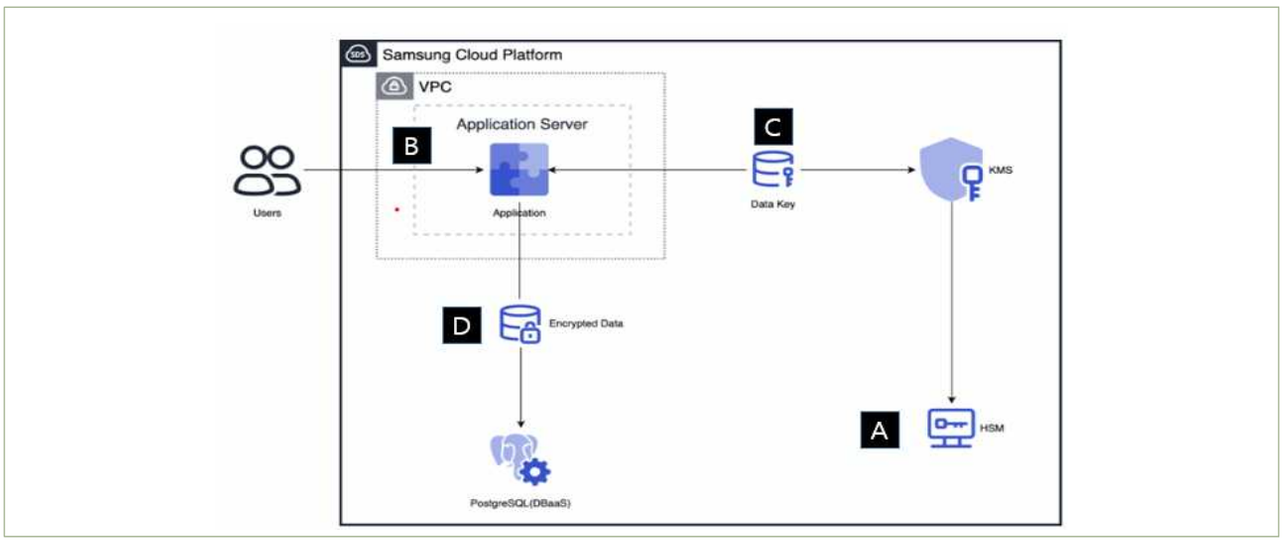
※ 사용자는 암호키를 이용하여 데이터를 암호화/복호화하며, 암호키는 계층적으로 암호화 된 중앙 집중 암호키 방식으로 안정적 관리

① 제공키 종류

- 암호화/복호화(AES-256): 대칭 키 방식의 AES256 키를 생성해 최대 32KB 데이터 암호화에 이용
- 암/복호화 및 서명/검증(RSA-2048): 비대칭 키 방식의 RSA(2048비트)키를 생성해 최대 190B 데이터 암호화 또는 8KB 서명에 이용
- 서명/검증 (ECDSA): 비대칭 키 방식의 ECDSA 키를 생성해 최대 8KB 데이터 서명에 이용

② KMS를 활용한 키 관리 및 암호화/복호화

- KMS는 고객이 암호키를 안전하게 생성, 보관, 관리할 수 있도록 제공하는 Managed Service 상품으로, 안정적인 중앙 집중 암호키 관리 방식의 서비스
- 데이터의 보안은 클라우드 환경에서 중요한 요소로 암호키를 사용하여 서비스 또는 애플리케이션 내의 데이터를 API를 통해 암호화 할 수 있음. 또한 KMS에서 생성되는 암호키는 FIPS 140-2에 따라 검증된 하드웨어 보안 모듈을 통해 보호



| 그림 4.5.6 | KMS를 활용한 키관리 및 암복호화

A. KMS 관리자에 의해 생성된 마스터키는 폐쇄된 별도 네트워크 망에 구성된 안전한 HSM에 저장하여 관리

B. 사용자는 애플리케이션에서 평문 데이터를 저장

C. 암호화 API가 KMS에 암호화를 위한 데이터 키를 요청하고, KMS에서 마스터키를 통해 데이터 키를 발급

D. 애플리케이션 암호화 로직에서 데이터 키를 통해 평문 데이터를 암호화하여 암호화된 데이터를 Database에 저장

③ KMS를 활용한 안전한 알고리즘 사용 사례

- 개인정보 저장을 위한 암호화 : 민감한 사용자 정보(이름, 주민번호, 핸드폰번호 등)는 평문이 아닌 암호화 한 형태로 저장이 필요하며, 데이터를 저장할 때 KMS를 통해 발급 받은 암호키로 암호화 후 저장하면 개인정보 유출의 위험성도 낮출 수 있으며, 보안적으로도 안전
- 디지털 서명 및 검증 : KMS는 비대칭 키를 지원하므로, 공개키 방식의 암호화를 이용하여 인증을 위한 서명/검증 값을 쉽게 획득 가능. 또한, 문서의 내용을 고객이 개인키로 암호화하여 서명하고, 전송 받은 서버 측에서는 미리 고객으로부터 제공받은 공개키로 복호화하여 검증하는 과정을 진행. 대칭키 사용 대비 기밀성이 높으며 탈취로 인한 문제도 해결 가능

④ KMS 키를 활용한 암호화 예제

- 「Samsung Cloud Platform 사용자 가이드」에 소개된 코드는 KMS에 대한 이해를 돕기 위한 단순 참고용 예시이므로, 실제 적용 시에는 사용자의 실제 시나리오에 맞게 수정하여 활용하도록 권고

[봉투 암호화(Envelope Encryption) 사용]

- 봉투 암호화 사용 시나리오를 제시하고, 시나리오에 따라 작성된 Java 예제 코드와 결과값 확인 가능
- 시나리오 : 암호화된 봉투 파일의 Datakey 복호화 및 복호화된 Datakey로 봉투 파일의 암호화 데이터를 복호화
- Java 예제 코드 : 상단에 제시된 시나리오에 따라 작성된 Java 예제 코드는 「Samsung Cloud Platform 사용자 가이드」를 참고 (https://cloud.samsungsds.com/manual/ko/scp_user_guide.html#f3b45be766a4ede7)

[데이터 서명 사용]

- 데이터의 무결성을 보증하기 위한 데이터 서명 사용 시나리오를 제시하고 시나리오에 따라 작성된 Java 예제 코드와 결과값 확인
- 시나리오 : 서명할 데이터를 OpenAPI로 호출하여 서명 및 서명된 데이터는 봉투화하여 json 파일로 저장
- Java 예제 코드 : 상단에 제시된 시나리오에 따라 작성된 Java 예제 코드는 「Samsung Cloud Platform 사용자 가이드」 참고 (https://cloud.samsungsds.com/manual/ko/scp_user_guide.html#f3b45be766a4ede7)

[데이터 검증 사용]

- 데이터의 무결성을 검증하기 위한 검증 사용 시나리오를 제시하고 시나리오에 따라 작성된 Java 예제 코드와 결과값 확인
- 시나리오 : 서명된 봉투 파일의 서명값을 가져오고, 서명된 데이터를 검증하여 결과값을 출력
- Java 예제 코드 : 상단에 제시된 시나리오에 따라 작성된 Java 예제 코드는 「Samsung Cloud Platform 사용자 가이드」를 참고 (https://cloud.samsungsds.com/manual/ko/scp_user_guide.html#f3b45be766a4ede7)

4 참고 사항

- 「Samsung Cloud Platform 사용자 가이드」에서는 KMS에서 생성한 키를 사용하여 봉투 암호화(Envelope Encryption) 및 데이터 서명/검증을 구현하기 위한 Java 코드 예제가 소개되어 있으며, 상세 내용은 'KMS 키를 활용한 암호화 예제' 참고. (https://cloud.samsungsds.com/manual/ko/scp_user_guide.html#encryption_example_utilizing_kms_key)

5. 로깅 및 모니터링 관리

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

5 로깅 및 모니터링 관리

1 기준

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

2 설명

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

  - 예시

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

    2) 가상자원에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근기록

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

    4) 가상자원 내 전산자료의 처리 내용을 확인할 수 있는 사용자 로그인, 액세스 로그 등 접근기록

3 우수 사례

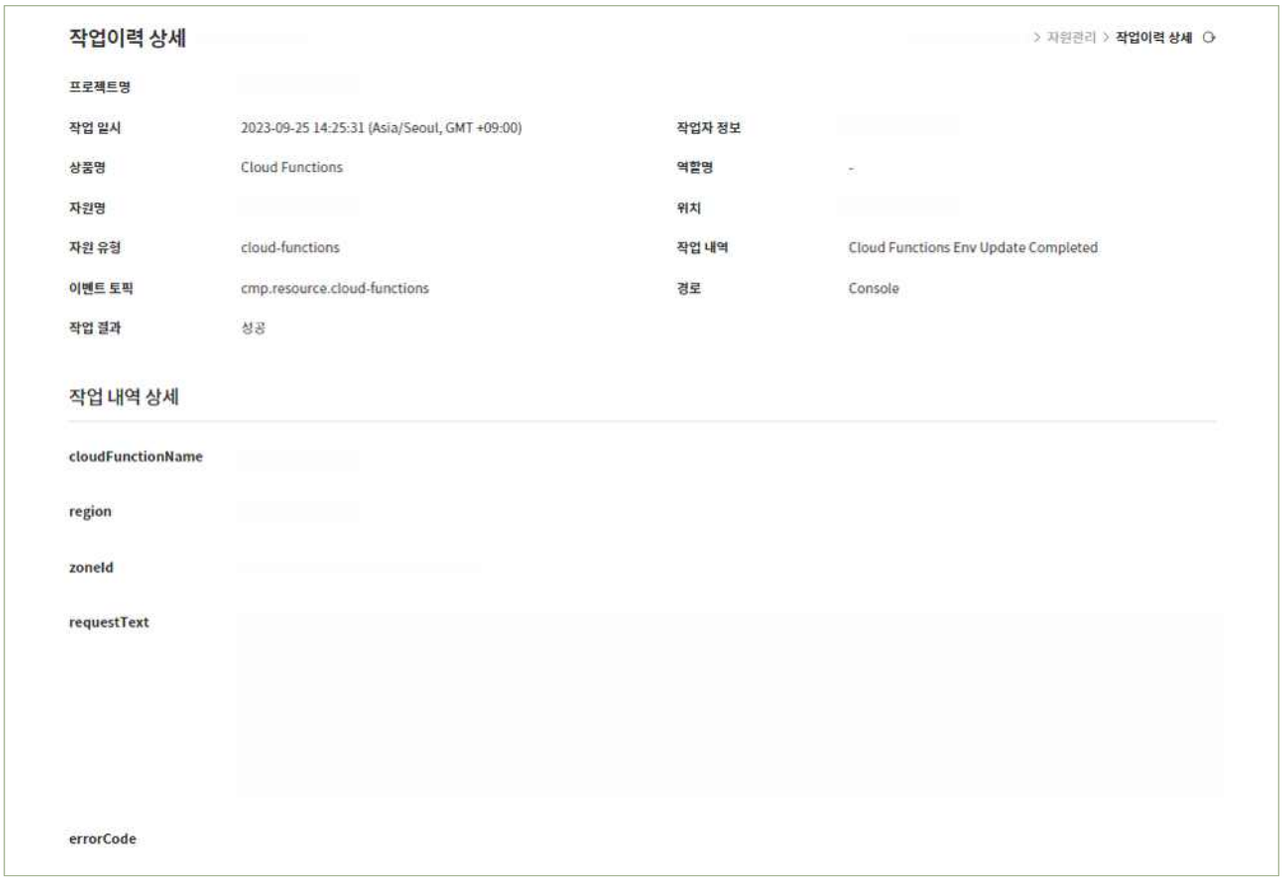
1) 가상자원 변경 사항에 관한 행위(생성, 변경, 삭제 등)

- 사용자 활동 내역 확인

  ① Logging&Audit → Logging&Audit 활동내역에서 별도 설정 없이 사용자가 수행하는 모든 활동 내역 확인 가능

| 그림 5.1.1 | Logging&Audit 활동내역 조회

② 활동내역 목록에서 상세정보를 확인하려는 활동 내역을 클릭하여 작업 일시, 작업자 정보, 자원명, 작업 내역 등 상세 내용 확인 가능



| 그림 5.1.2 | Logging&Audit 활동내역 상세 조회

2) 가상자원 내 전산자료의 처리 로그

- 금융회사에서는 가상자원으로 구성한 정보처리시스템 내 전산자료(소스코드, 고객정보, 회사정보 등)에 대한 처리 로그(전산자료의 수정 및 삭제, 접근 등)를 수집하여야 한다.

4 참고 사항

- Trail을 생성하여 선택한 상품, 계정의 로그를 사용자 Object Storage에 보관할 수 있습니다. (별도 저장기간 없음)
- 자세한 사항은 Samsung Cloud Platform 콘솔의 '사용자 가이드'를 참고
  https://cloud.samsungsds.com/manual/ko/scp_user_guide.html#6a6c4893a0862253

1 기준

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

2 설명

- 클라우드 가상자원 이용에 관한 행위추적성 증적에 대해 모니터링 및 주기적 검토를 수행하여야 한다.

  - 예시

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

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

3 우수 사례

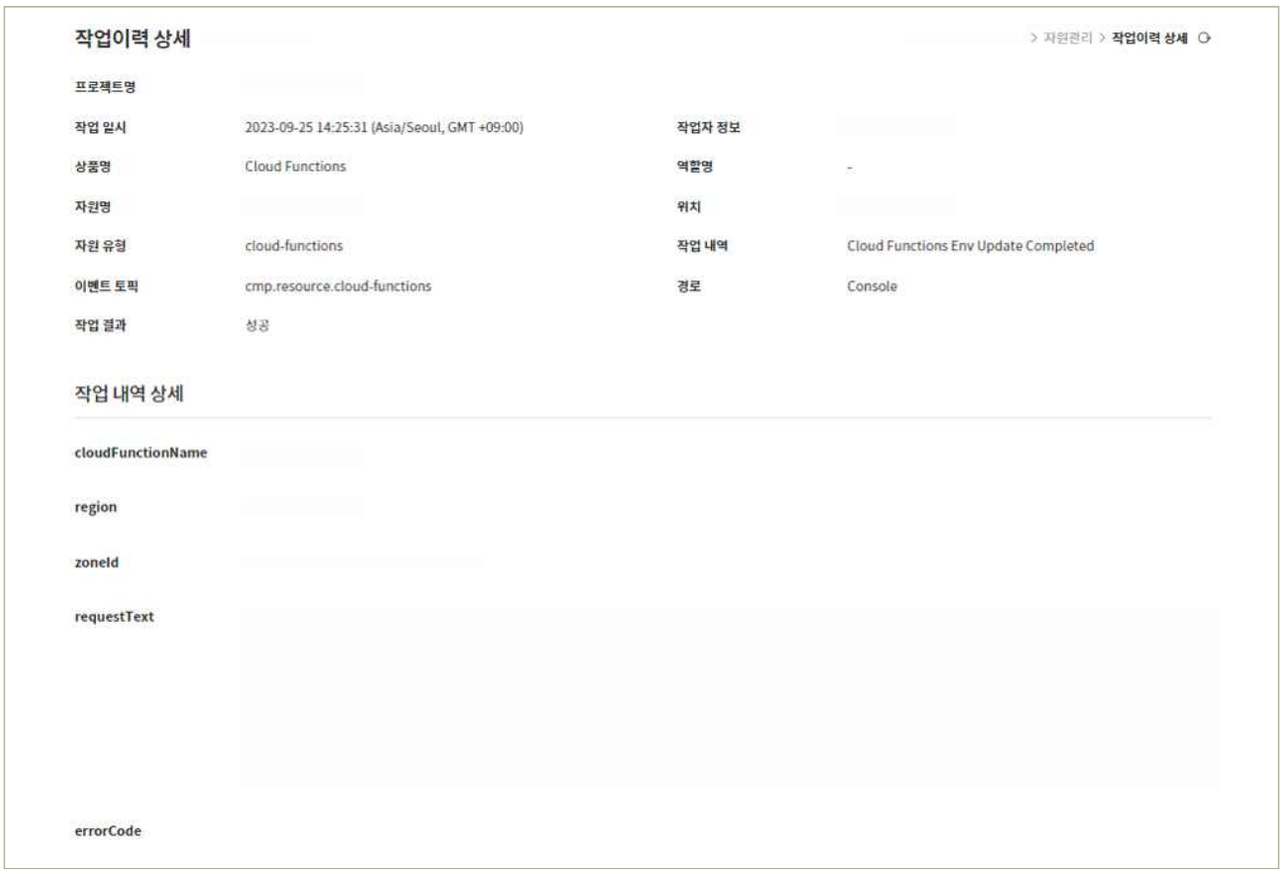
1) 클라우드 가상자원 이용에 관한 행위추적성 증적(ex. 감사로그 등)에 대한 상시 모니터링 수행

- 가상자원 이용에 대한 로그 확인

  ① Logging&Audit → Logging&Audit 활동내역에서 별도 설정 없이 사용자가 수행하는 모든 활동 내역을 확인할 수 있습니다.

| 그림 5.2.1 | Logging&Audit 활동내역 조회

② 활동내역 목록에서 상세정보를 확인하려는 활동 내역을 클릭하여 작업 일시, 작업자 정보, 자원명, 작업 내역 등 상세 내용을 확인할 수 있습니다.



| 그림 5.2.2 | Logging&Audit 활동내역 상세 조회

2) 클라우드 가상자원 이용에 관한 행위추적성 증적에 대한 주기적 검토

- '5.1 가상자원 이용에 관한 행위추적성 확보' 기준을 통해 확인된 로그에 대해 금융회사에서는 주기적 검토 필요
  - 인가받지 않은 가상자원 접속, 생성, 변경, 삭제 등

4 참고 사항

- Trail을 생성하여 선택한 상품, 계정의 로그를 사용자 Object Storage에 보관할 수 있습니다. (별도 저장기간 없음)
- Trail 생성 후 Object Storage에 저장된 로그 파일이 변경, 수정, 삭제가 되었는지 로그 파일 검증 기능을 통해 확인이 가능합니다.

1 기준

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

2 설명

- 이용자 가상자원 가용성 확보 및 장애대응을 위한 모니터링 기능을 확보하여야 한다.

  - 예시

    1) 가상자원 상태 모니터링(사용량, 트래픽 용량 등)
    2) 가상자원 장애 모니터링(장애 발생 시 담당자 공지 등)
    3) 가상자원 장애 발생 시 장애상황기록부 작성 등
    4) 가상자원 네트워크 정책 변경(삭제 등) 모니터링

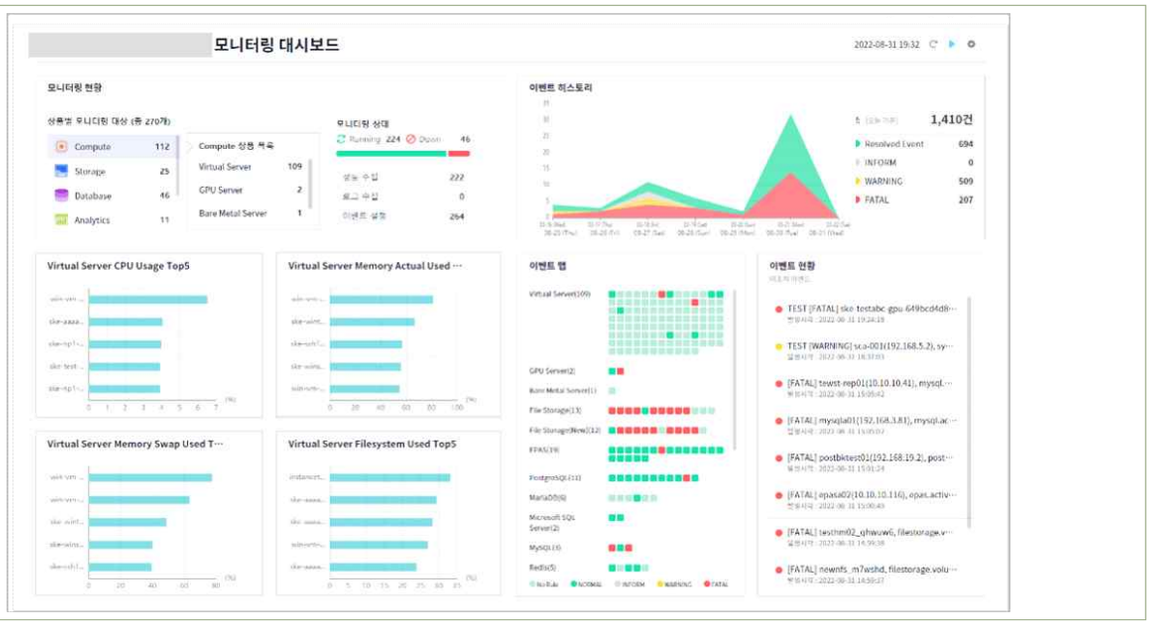
3 우수 사례

1) 가상자원 상태 모니터링(사용량, 트래픽 용량 등)

- Cloud Monitoring을 통한 SCP 인프라 리소스 운영 현황 모니터링

  ① 모니터링 대시보드

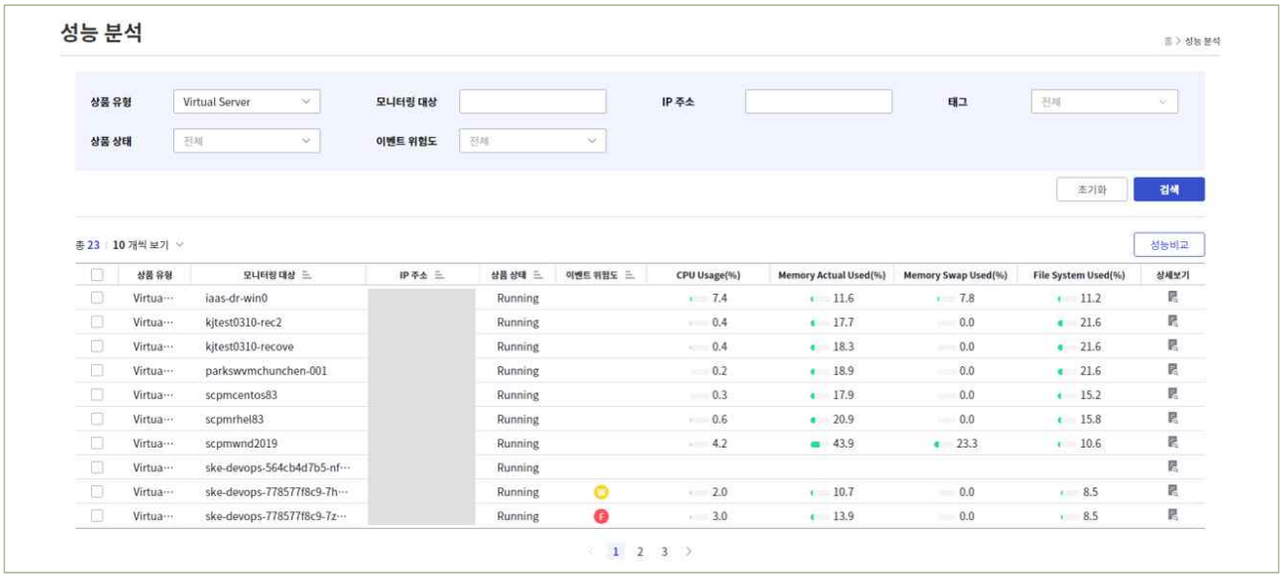
  - 선택한 프로젝트의 모니터링 대상 상품 및 자원에 대한 운영 현황, 이벤트 현황, 사용률 상위 항목 등을 확인할 수 있습니다.



| 그림 5.3.1 | 모니터링 대시보드

② 성능 분석

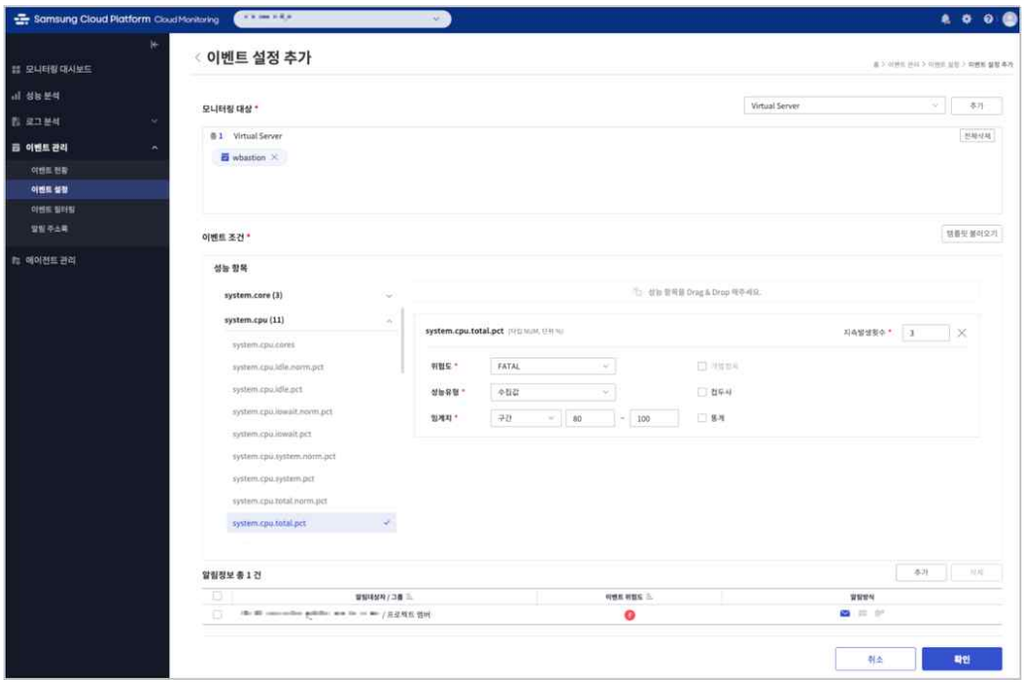
- CPU 사용률, 디스크 사용률, 메모리 사용률 등의 지표를 확인할 수 있습니다.



| 그림 5.3.2 | 성능 분석

③ 이벤트 관리

- 이벤트 관리 → 이벤트 설정에서 모니터링 대상의 이벤트가 발생할 경우 특정 사용자에게 알림전달 가능



| 그림 5.3.3 | 이벤트 관리

4 참고 사항

- 자세한 사항은 Samsung Cloud Platform 콘솔 → 'Cloud Monitoring 사용자 가이드'를 참고
  https://cloud.samsungsds.com/manual/ko/eb51f69cbb399c18.html

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.

  - 예시

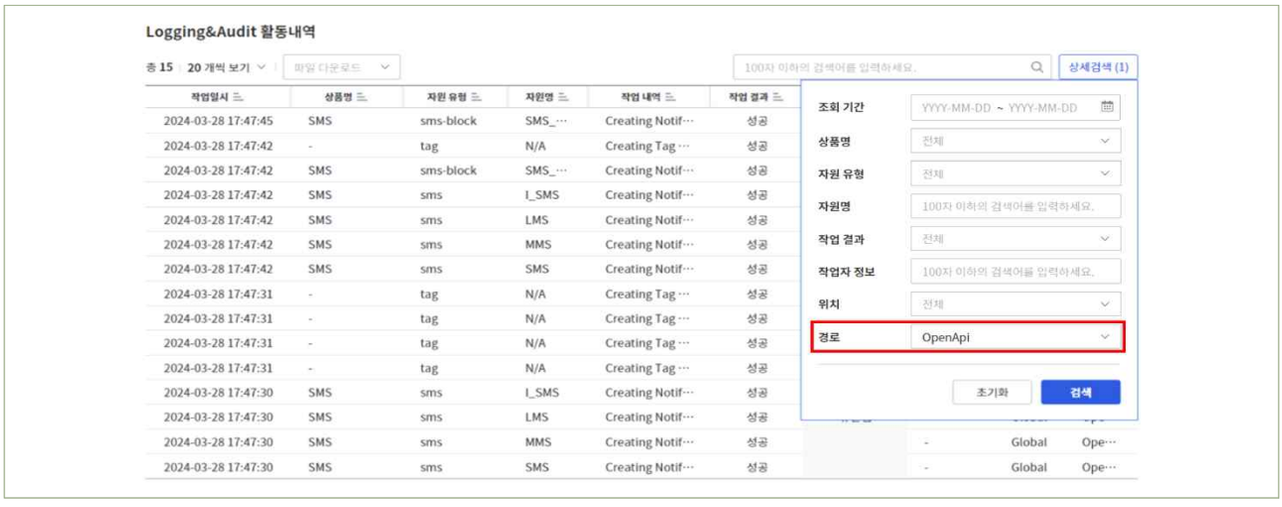
    1) API 호출에 관한 정보(호출대상, 호출자, 호출일시 등)

3 우수 사례

1) API 호출에 관한 정보(호출대상, 호출자, 호출일시 등)

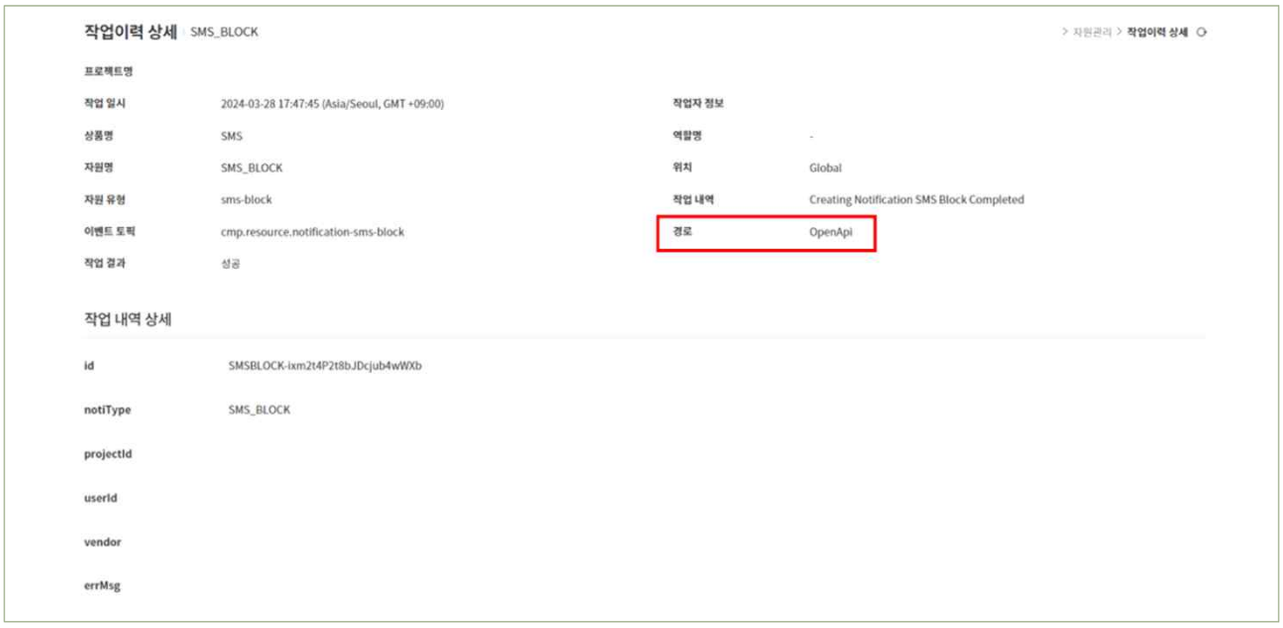
- API 호출에 대한 로그 확인

  ① Logging&Audit → Logging&Audit 활동내역에서 별도 설정 없이 사용자가 수행하는 모든 활동 내역 중 API 호출에 관한 정보만을 필터링하여 확인 가능



| 그림 5.4.1 | Logging&Audit 활동내역 조회 (경로: OpenApi)

② 활동내역 목록에서 상세정보를 확인하려는 활동 내역을 클릭하여 작업 일시, 작업자 정보, 자원명, 작업 내역 등 상세 내용 확인 가능



| 그림 5.4.2 | Logging&Audit 활동내역 상세 조회

4 참고 사항

- N/A

1 기준

식별번호	기준	내용
5.5.	**네트워크 관련 서비스(VPC, 보안그룹, ACL 등)에 관한 행위추적성 확보**	**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

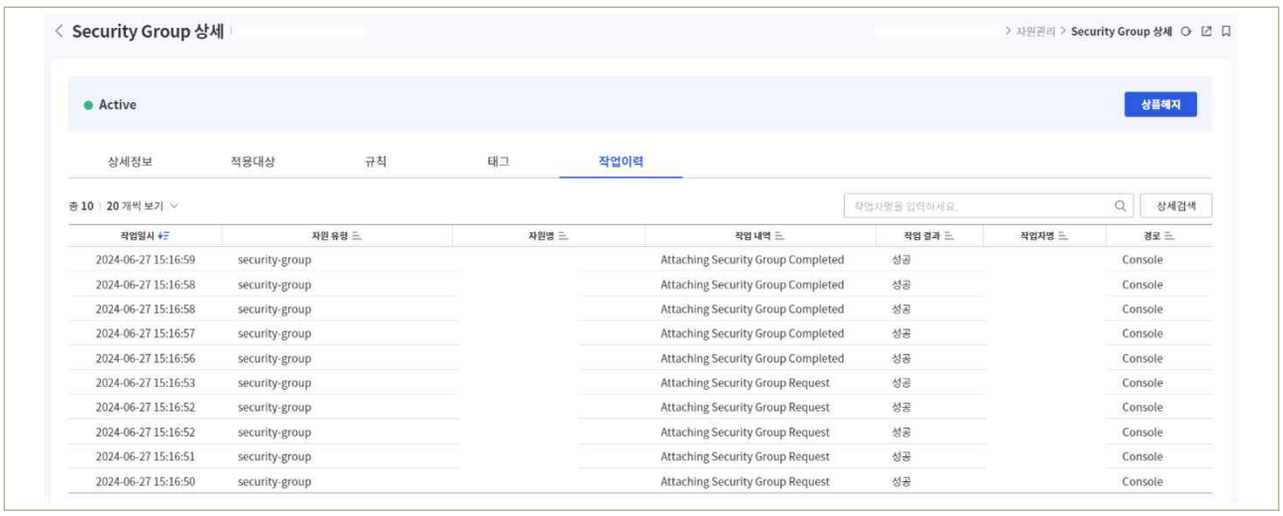
3 우수 사례

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

- 네트워크 서비스 이용에 대한 로그 확인

  ① 네트워크 자원의 생성, 규칙 생성, 변경이력 조회

  - 네트워크 자원(예: Security Group, Firewall 등) 상세 → 작업이력 탭에서 자원 생성, 규칙 생성 및 변경이력 등 로그 조회 가능



| 그림 5.5.1 | Security Group 작업이력

- 작업이력 목록에서 상세정보를 확인하려는 내역을 클릭하여 작업 일시, 작업자 정보, 자원명, 작업 내역 등 상세 내용 확인 가능

| 그림 5.5.2 | 작업이력 상세정보 조회

4 참고 사항

- VPC 로그 관리와 관련하여 자세한 사항은 Samsung Cloud Platform 콘솔의 '사용자 가이드' 참고
  https://cloud.samsungsds.com/manual/ko/scp_user_guide.html#vpc_log_management

1 기준

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

2 설명

- 클라우드 계정 변동사항에 대한 행위추적성(로그 등)을 확보하여야 한다.

  - 행위 감사로그

    1) 클라우드 가상자원 관리시스템 접속 계정 생성, 변경, 삭제에 관한 사항

    2) 클라우드 가상자원(서버, 데이터베이스 등) 접속 계정 생성, 변경, 삭제에 관한 사항

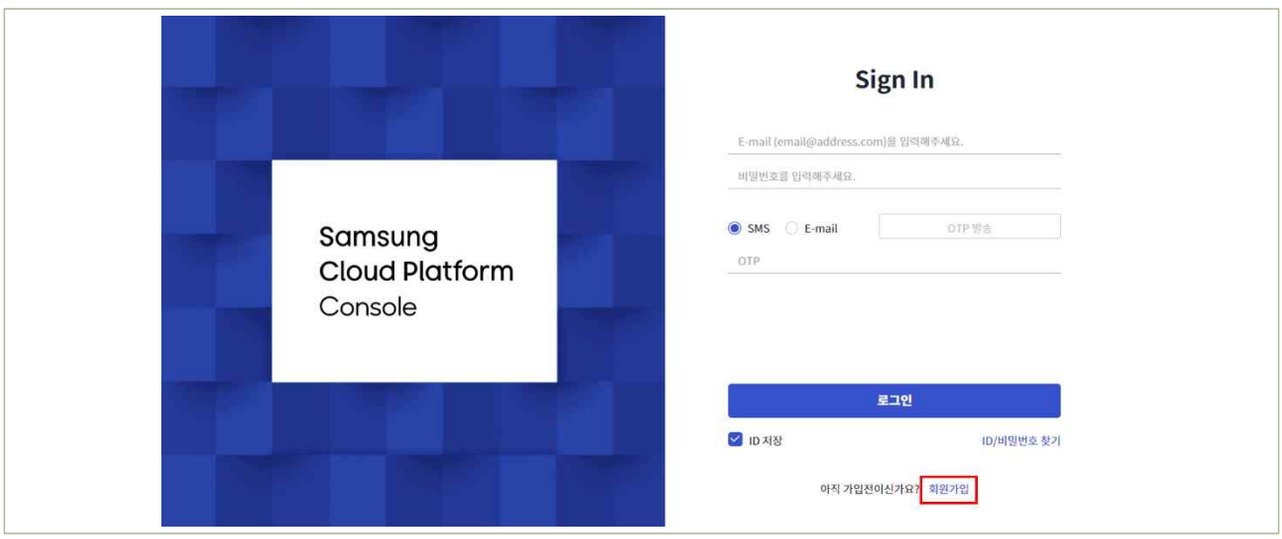
3 우수 사례

1) 클라우드 가상자원 관리시스템 접속 계정 생성, 변경, 삭제에 관한 사항

- SCP는 콘솔계정 생성, 변경, 탈퇴 등 접속계정 관리를 고객이 직접 수행

  ① 회원가입

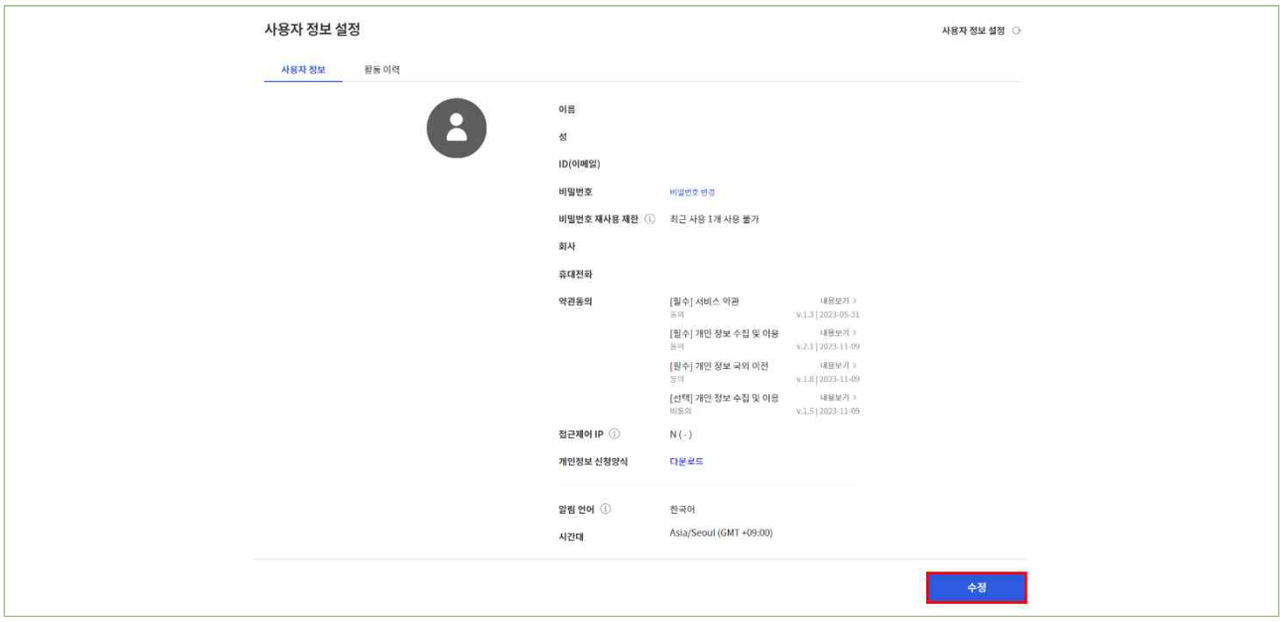
  - 콘솔 랜딩 페이지에서 회원가입 버튼을 클릭하여 콘솔 계정을 생성



| 그림 5.6.1 | 회원가입

② 사용자 정보 설정

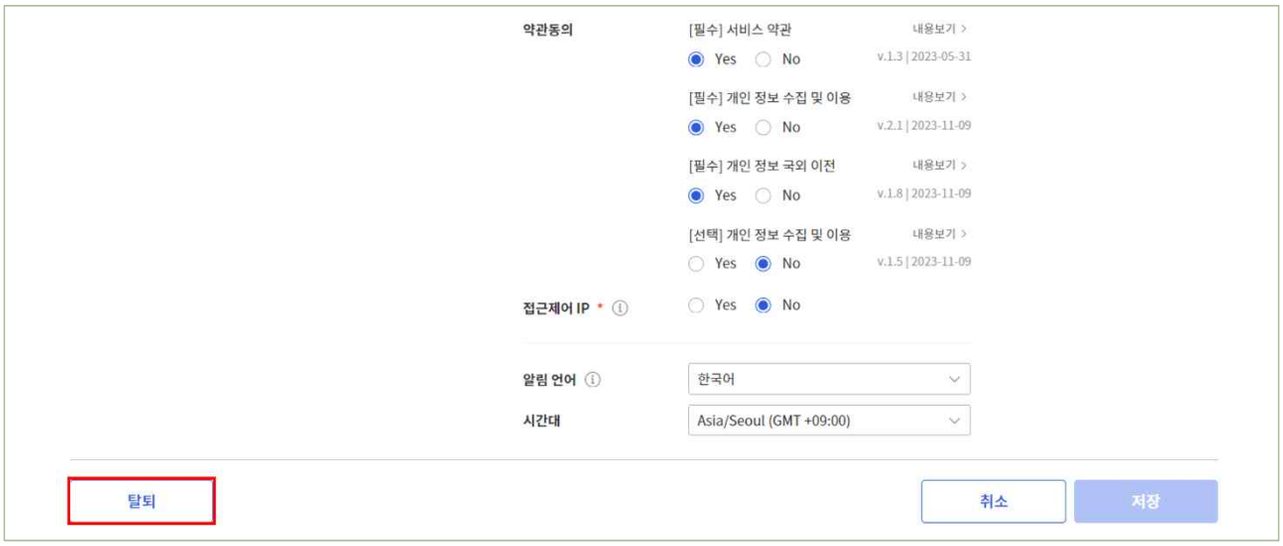
- My 메뉴 → 사용자 정보 설정에서 사용자의 계정 정보 및 활동 이력 조회 가능



| 그림 5.6.2 | 사용자 정보 설정

③ 회원 탈퇴

- My 메뉴 → 사용자 정보 설정 → 수정 → 탈퇴 버튼을 클릭하여 콘솔에서 탈퇴 가능



| 그림 5.6.3 | 회원 탈퇴

4 참고 사항

- 회원 탈퇴 시 수집된 회원 정보는 모두 파기되며, 프로젝트 내 권한이 모두 삭제되어 재가입하더라도 서비스 이용 관련 정보 및 권한은 복구 불가
- 어카운트 유저(또는 어카운트의 유일한 유저)는 '서포트센터' → '1:1 문의'를 클릭한 후, 프로젝트 생성/관리를 위한 어카운트 유저 역할을 양도 또는 어카운트 삭제 필요

1 기준

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

2 설명

- 클라우드 서비스 이용 계정 변경사항에 관한 모니터링을 수행하여야 한다.

  - 예시

    1) 계정 변경사항에 관한 상시 모니터링 수행
    2) 전자금융감독규정 및 금융회사 내부 규정 등에 수립된 주기에 맞추어 주기적 검토 수행
    3) 관리자 계정에 대해서는 이중 확인 수행 등

3 우수 사례

1) 클라우드 가상자원 관리시스템 접속 계정 생성, 변경, 삭제에 관한 사항

- 고객사 또는 MSP가 수행해야 할 영역이나, SCP의 특정 상품(SCP Logging&Audit)을 활용하여 해당 요건 수행 시 활용 가능.
- (상품별 활동내역 모니터링) ‘자원관리’ → ‘상품별 자원관리’ → ‘Management’ → ‘Logging&Audit’ → ‘활동내역’에서 변경사항(생성, 삭제 등) 확인

| 그림 5.7.1 | Logging&Audit를 통한 모니터링 예시

항목		설명
❶	표시 개수	한 페이지에 표시할 로그 개수를 설정할 수 있습니다.
❷	**파일 다운로드**	조회된 활동 목록을 JSON 또는 CSV 파일 형식으로 내려받을 수 있습니다.
❸	검색 영역	검색어를 입력하거나 **상세검색**를 클릭하여 카테고리나 기간을 선택하여 검색할 수 있습니다. • **조회 기간**: 클릭하여 검색 시작일과 종료일을 선택할 수 있습니다. • **상품명**, **자원 유형**, **자원명**, **작업 결과**, **작업자 정보**, **역할명**, **위치**, **경로** 중 검색 카테고리를 선택한 후 키워드를 입력하여 검색할 수 있습니다.
❹	활동 목록	활동 목록을 표시합니다. • 활동 내역(로그)을 클릭하여 "작업이력 상세" 팝업창에서 상세정보를 확인할 수 있습니다.

| 그림 5.7.2 | ‘Logging&Audit’ 활동내역 상세정보 확인 예시

2) 클라우드 가상자원 관리시스템 계정 변경사항에 관한 주기적 검토

- 금융회사 및 전자금융업자는 전자금융감독규정 및 내부 규정 등에 수립된 주기에 맞추어 계정 변경사항(인가받지 않은 계정의 생성, 삭제 및 권한 오부여 등)에 대한 주기적 검토 수행 필요

| 그림 5.7.3 | 작업이력 상세

4 참고 사항

- N/A

6. API 관리

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

6 API 관리

1 기준

식별번호	기준	내용
6.1.	API 호출 시 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 호출 시 사용되는 인증값을 단기 인증 값으로 사용 등

3 우수 사례

1) API 호출이 가능한 IP 지정

- ▶ 접근 허용 IP 사용여부 선택

  ① '접근 허용 IP 사용'을 선택하면 특정 IP 대역의 접근만 허용되며, IP 미등록 시 모든 IP의 접근이 거부됩니다.

| 그림 6.1.1 | 접근 허용 IP 사용여부 선택

A. 접근 허용 IP: 접근 허용 IP 사용 여부를 선택하고, OpenAPI 사용을 허가할 IP 정보를 등록합니다.

- 사용: 접근 허용할 IP를 등록합니다. 추가 버튼을 클릭하여 IP 정보를 입력합니다.
- 사용 안함: 모든 IP의 접근을 허용합니다.

2) API 호출 시 사용되는 인증값을 단기 인증 값으로 사용 등

- ▶ 인증 방식(임시키 인증/인증키 인증) 선택

① 인증키

Ⅰ. 암호화된 키를 제공하여 고객의 중요한 데이터를 보호하는 공통 키 관리 서비스로, Access Key와 Secret Key 한 쌍으로 구성됩니다.

Ⅱ. 사용자는 Secret Key를 이용하여 API 요청 정보를 HMAC 형식의 Signature를 생성 후 OpenAPI 요청과 함께 서버에 전달하고, 서버에서 Access Key와 Signature를 이용하여 사용자 인증을 처리합니다.

② 임시키

Ⅰ. 인증키를 사용하여 발급하는 사용 기한에 제약이 있는 인증키로, 최소 15분에서 최대 36시간까지 사용 기한을 부여할 수 있습니다.

| 그림 6.1.2 | 인증 방식 선택

A. 인증 방식: OpenAPI 인증 방식을 선택합니다.

- 임시키 인증: OpenAPI 인증에 임시키만 허용합니다.
- 인증키 인증: OpenAPI 인증에 인증키만 허용합니다.

4 참고 사항

- 인증키의 만료 기한은 1~365일까지 설정이 가능하며, 영구 옵션을 통해 만료 기한이 없도록 설정할 수 있습니다. 보안 강화를 위해 인증키를 주기적으로 변경하는 것을 권고합니다.
- 인증키를 이용하여 한시적인 사용 기한을 가지는 임시키를 발급할 경우, 임시키의 사용 기한은 최소 15분에서 최대 2160분(36시간)의 사용기한을 가집니다.

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 보안키와 서명을 통한 변조방지 대책 마련 등

3 우수 사례

1) API 보안키와 서명을 통한 변조방지 대책 마련 등

- ▶ API 호출 시 필요한 인증키 생성

① 인증키 생성 : 인증키를 생성하여 API 호출 시 필요한 Access Key와 Secret Key를 발급받아야 합니다.

Ⅰ. 인증키 생성

Ⅱ. 인증키 상세 정보 확인

[I. 인증키 생성]

- 신청 경로: My 메뉴 → '인증키 관리' → '인증키 생성'

| 그림 6.2.1 | 인증키 생성

A. 구분: 인증키의 적용 범위를 선택합니다.

- 공통: 모든 프로젝트의 접근을 허용합니다.
- 프로젝트: 선택한 프로젝트만 접근을 허용합니다.

B. 만료기한: 인증키의 만료 기한을 선택합니다.

- 직접 입력: 인증키의 만료 기한을 최대 365일까지 직접 입력합니다.
- 영구: 인증키를 영구적으로 사용합니다.

[II. 인증키 상세 정보 확인]

- 확인 경로: My 메뉴 → '인증키 관리' → 인증키' 상세

| 그림 6.2.2 | 인증키 상세 정보 확인

A. 인증키 정보: 인증키, 임시키 상세정보를 확인할 수 있습니다.

B. 상태: 상태 변경을 클릭하여 인증키의 상태를 변경할 수 있습니다.
C. 인증키: '보기'를 클릭하여 인증키의 Access Key 및 Secret Key를 조회 및 복사할 수 있습니다.
D. 생성일시: 인증키의 생성일시를 표시합니다.
E. 만료일시: 인증키의 만료일시를 표시합니다.

- ▶ API 호출하기

① 호출 API 요청을 Access Key와 매핑되는 Secret Key로 암호화하여 서명으로 사용합니다.
Ⅰ. AUTHPARAMS 요청
Ⅱ. Signature 생성

[I. AUTHPARAMS 요청]

```
curl -i -X GET
-H "X-Cmp-AccessKey:(Access Key)"
-H "X-Cmp-Signature:(Signature)"
-H "X-Cmp-Timestamp:1605290625682"
-H "X-Cmp-ClientType:OpenApi"
-H "X-Cmp-ProjectId:(Project ID)"
'{URL}/iam/v2/access-keys
```

| 그림 6.2.3 | AUTHPARAMS 요청 예시

A. X-Cmp-AccessKey: Samsung Cloud Platform 포털에서 발급받은 Access Key를 입력합니다.
B. X-Cmp-Signature: 호출 API 요청을 Access Key와 매핑 되는 Secret Key로 암호화한 서명으로, HMAC 암호화 알고리즘은 HmacSHA256을 사용합니다.
C. X-Cmp-Timestamp: 1970년 1월 1일 00:00:00 협정 세계시(UTC)부터의 경과 시간을 밀리초(Millisecond)로 정의합니다.
D. X-Cmp-ClientType: Client Type을 입력합니다. (OpenApi)
E. X-Cmp-ProjectId: API를 실행하려는 프로젝트의 프로젝트 아이디를 입력합니다.

[II. Signature 생성]

```
public static String makeHmacSignature(String method,
                                       String url,
                                       String timestamp,
                                       String accessKey,
                                       String accessSecretKey,
                                       String headerProjectId,
                                       String headerClientType) {
        String body = method + url + timestamp + accessKey + headerProjectId +
headerClientType;

        String encodeBase64Str = null;

        try {
            byte[] message = body.getBytes("UTF-8");
            byte[] secretKey = (Secret Key);

            Mac mac = Mac.getInstance("HmacSHA256");
            SecretKeySpec secretKeySpec = (Secret Key Spec);
            mac.init(secretKeySpec);
            byte[] hmacSha256 = mac.doFinal(message);
            encodeBase64Str = Base64.getEncoder().encodeToString(hmacSha256);
        } catch (Exception e) {
            throw new RuntimeException("Failed to calculate hmac-sha256", e);
        }

        return encodeBase64Str;
    }
```

| 그림 6.2.4 | Signature 생성 Sample Code (Java)

```
<script
src="https://cdnjs.cloudflare.com/ajax/libs/crypto-js/3.1.2/rollups/hmac-sha256.js"></scr
ipt>
<script
src="https://cdnjs.cloudflare.com/ajax/libs/crypto-js/3.1.2/components/enc-base64-min
.js"></script>

<script type="text/javascript">
function makeSignature() {
    var method = "GET"; // Method
    var url = "{url}"; // url
    var timestamp = Date.now(); // timestamp
    var accessKey = "{accessKey}";
    var secretKey = "{secretKey}";
    var projectId = "{projectId}";
    var clientType = "openApi"; // client type

    url = encodeURI(url); // 한글, 특수 문자 처리

    var message = method + url + timestamp + accessKey + projectId + clientType;

    var hash = CryptoJS.HmacSHA256(message, secretKey);
    return CryptoJS.enc.Base64.stringify(hash);
}
</script>
```

| 그림 6.2.5 | Signature 생성 Sample Code (JavaScript)

4 참고 사항

- API 호출 시 요청으로부터 서명할 문자열을 생성하고 Secret Key로 HmacSHA256 알고리즘으로 암호화 후 Base64로 인코딩합니다.
  (이 값을 x-Cmp-Signature로 사용합니다.)
- Samsung Cloud Platform 사용자 가이드에서는 OpenAPI 가이드가 소개되어 있음. 더 자세한 내용을 알고 싶으시면 해당 가이드 참조
  (https://cloud.samsungsds.com/openapiguide/#/docs/v3-ko-overview-overview)

1 기준

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

2 설명

- API 호출 시 인용되는 유니크 값(ex. 보안키 등)은 안전하게 보관 및 관리하여야 한다.

  - 예시

    1) API 보안키 생성 시 이용자에게 1회만 노출 등

3 우수 사례

1) API 보안키 생성 시 이용자에게 1회만 노출 등

- ▶ Samsung Cloud Platform의 인증키는 최초 생성 후, 이용자의 비밀번호를 입력해야만 조회 및 복사 가능.

  ① 인증키 생성: 인증키를 생성하여 API 호출 시 필요한 Access Key와 Secret Key를 발급받아야 합니다.

  Ⅰ. 인증키 생성

  Ⅱ. 인증키 상세 정보 확인

[I. 인증키 생성]

- 신청 경로: My 메뉴 → '인증키 관리' → '인증키 생성'

| 그림 6.3.1 | 인증키 생성

A. 구분: 인증키의 적용 범위를 선택합니다.
  · 공통: 모든 프로젝트의 접근을 허용합니다.
  · 프로젝트: 선택한 프로젝트만 접근을 허용합니다.

B. 만료기한: 인증키의 만료 기한을 선택합니다.
  · 직접 입력: 인증키의 만료 기한을 최대 365일까지 직접 입력합니다.
  · 영구: 인증키를 영구적으로 사용합니다.

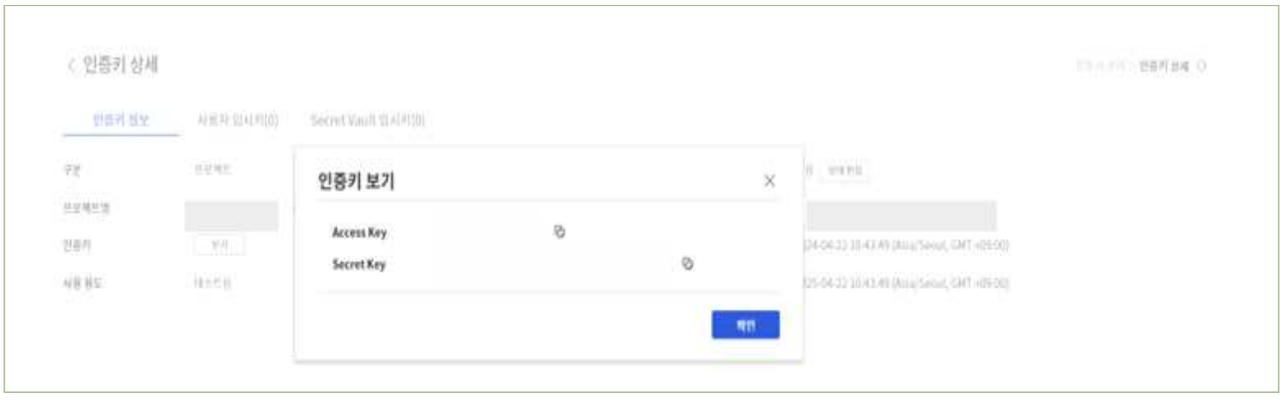
[II. 인증키 상세 정보 확인]

- 확인 경로: My 메뉴 → 인증키 관리 → 인증키 상세

| 그림 6.3.2 | 인증키 상세 정보 확인

A. 인증키 정보: 인증키, 임시키 상세정보를 확인할 수 있습니다.
B. 상태: 상태 변경을 클릭하여 인증키의 상태를 변경할 수 있습니다.
C. 인증키: '보기'를 클릭하여 인증키의 Access Key 및 Secret Key를 조회 및 복사할 수 있습니다.
D. 생성일시: 인증키의 생성일시를 표시합니다.
E. 만료일시: 인증키의 만료일시를 표시합니다.

| 그림 6.3.3 | 인증키 보기 버튼 클릭 시 비밀번호 확인



| 그림 6.3.4 | 인증키 보기

4 참고 사항

- Samsung Cloud Platform 사용자 가이드에서는 인증키(Access Key) 활용 가이드가 소개되어 있음. 더 자세한 내용을 알고 싶으시면 해당 가이드 참조 (https://cloud.samsungsds.com/manual/ko/scp_user_guide.html#introduction_to_access_key)

1 기준

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

2 설명

- API 세션 및 서명값에 대한 유효기간 설정하고, 유니크값(보안키 등) 유출 방지대책으로 만료기간을 적용하여야 한다. 기능 이용 시 보안성 향상을 위해 API 세션 및 서명값에 대한 유효기간을 설정하여야 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

1) 서명 유효기간 확인

- ▶ 서명의 생성에 사용하는 timestamp의 유효시간 적용
  - 서명의 생성에 사용하는 timestamp의 유효시간은 생성 후 15분으로 제한됩니다. (유효기간 만료 시 401 코드 반환)

HTTP 상태 코드	오류 코드	오류 메시지	설명
400	PLATFORM-COMMON-00003	Invalid input data	입력값 검증 실패
401	PLATFORM-COMMON-00004	Unauthorized	인증 실패
401	PLATFORM-IAM-000105	Authentication method or IP address is not allowed	인증키 보안 설정 오류 (인증키 보안 설정에서 인증 방식, 접근 허용 IP 설정 확인)
401	PLATFORM-IAM-000103	Unauthorized	인증실패 (공통 인증키가 필요한 요청에 프로젝트 인증키를 사용)
401	PLATFORM-IAM-000104	Project id not found	인증실패 (프로젝트 아이디가 필요한 요청에 프로젝트 아이디가 없음)
401	PLATFORM-GW-00006	Request time out	인증실패 (Signature 생성에 사용하는 timestamp의 유효 시간은 생성 후 15분으로 제한됨)
401	PLATFORM-GW-00012	Session expired	인증실패 (OpenAPI 요청을 Console 주소로 보냄, 요청 주소 확인)
403	PLATFORM-COMMON-00008	Access denied	권한 없음
404	PLATFORM-GW-00002	Access key not found	Access Key가 존재하지 않음
404	PLATFORM-COMMON-00010	Api not found	지정된 API가 존재하지 않음
404	PLATFORM-RESOURCE-GROUP-000001	Resource is already deleted or does not exist	자원이 존재하지 않음
412	PLATFORM-GW-00003	Signature does not match	Signature 불일치로 인증 실패
500	PLATFORM-COMMON-00018	Internal server error	예외 처리가 안된 오류

| 그림 6.4.1 | 공통 오류 코드

2) API 보안키 만료기간 설정

- ▶ 인증키 생성 시 만료기한 설정

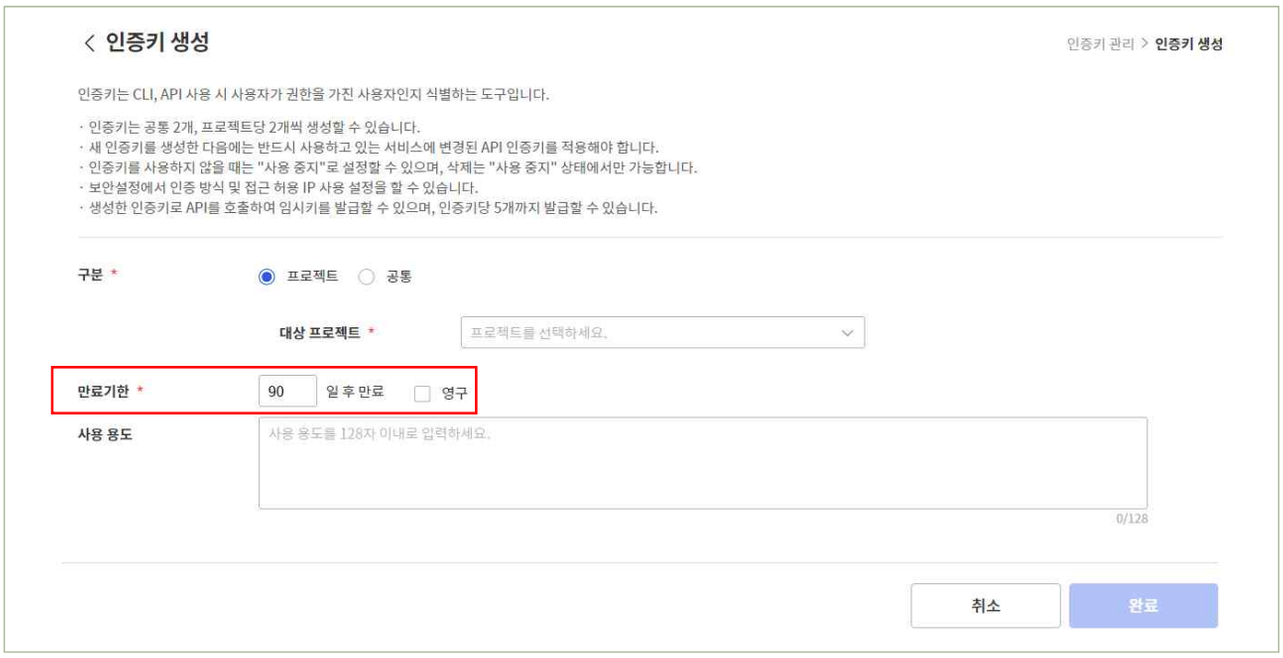
① 인증키 생성: 인증키를 생성하여 API 호출 시 필요한 Access Key와 Secret Key를 발급받아야 합니다.

Ⅰ. 인증키 생성

Ⅱ. 인증키 상세 정보 확인

[Ⅰ. 인증키 생성]

- 신청 경로: My 메뉴 → 인증키 관리 → 인증키 생성



| 그림 6.4.2 | 인증키 생성

A. 구분: 인증키의 적용 범위를 선택합니다.

- 공통: 모든 프로젝트의 접근을 허용합니다.
- 프로젝트: 선택한 프로젝트만 접근을 허용합니다.

B. 만료기한: 인증키의 만료 기한을 선택합니다.

- 직접 입력: 인증키의 만료 기한을 최대 365일까지 직접 입력합니다.
- 영구: 인증키를 영구적으로 사용합니다.

[II. 인증키 상세 정보 확인]

- 확인 경로: My 메뉴 → 인증키 관리 → 인증키 상세

| 그림 6.4.3 | 인증키 상세 정보 확인

A. 인증키 정보: 인증키, 임시키 상세정보를 확인할 수 있습니다.

B. 상태: 상태 변경을 클릭하여 인증키의 상태를 변경할 수 있습니다.

C. 인증키: '보기'를 클릭하여 인증키의 Access Key 및 Secret Key를 조회 및 복사할 수 있습니다.

D. 생성일시: 인증키의 생성일시를 표시합니다.

E. 만료일시: 인증키의 만료일시를 표시합니다.

- ▶ 임시키를 발급하여 사용기한 부여

① 임시키 발급: 인증키를 생성하여 API 호출 시 필요한 Access Key와 Secret Key를 발급받아야 합니다.

Ⅰ. 보안 설정 수정

Ⅱ. 임시키 발급을 위한 OTP 요청

Ⅲ. 임시키 생성

[I. 보안 설정 수정]

- 수정 경로: My 메뉴 → 인증키 관리 → 보안 설정 수정

| 그림 6.4.4 | 보안 설정 수정 - 인증 방식 선택

A. 인증 방식: OpenAPI 인증 방식을 선택합니다.

- 임시키 인증: OpenAPI 인증에 임시키만 허용합니다.
- 인증키 인증: OpenAPI 인증에 인증키만 허용합니다.

[II. 임시키 발급을 위한 OTP 요청]

```
Method : POST
URL : /iam/v2/access-keys/temporarys/otp/{transmissionMethod}
```

| 표 6.4.1 | OTP 요청 OpenAPI

A. transmissionMethod: OTP 발급 매체를 입력합니다. 입력값은 E-Mail, SMS 둘 중 하나를 선택합니다.

[III. 임시키 생성]

```
Method : POST
URL : /iam/v2/access-keys/temporarys/
Body :
{
    "durationMinutes": "2160",
    "otp":"123456"
}
```

| 표 6.4.2 | 임시키 생성 OpenAPI

A. durationMinutes: 임시키의 사용 기한을 입력합니다.

B. otp: 전송받은 OTP 값을 입력합니다.

4 참고 사항

- 인증키의 만료 기한은 1~365일까지 설정이 가능하며, 영구 옵션을 통해 만료 기한이 없도록 설정할 수 있습니다. 보안 강화를 위해 인증키를 주기적으로 변경하는 것을 권고합니다.
- 인증키를 이용하여 한시적인 사용 기한을 가지는 임시키를 발급할 경우, 임시키의 사용 기한은 최소 15분에서 최대 2160분(36시간)의 사용기한을 가집니다.
- 임시키는 API 호출 또는 CLI로만 생성할 수 있습니다.
- Samsung Cloud Platform 사용자 가이드에서는 OpenAPI 가이드가 소개되어 있음. 더 자세한 내용을 알고 싶으시면 해당 가이드 참조 (https://cloud.samsungsds.com/openapiguide/#/docs/v3-ko-overview-overview)

1 기준

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

2 설명

- API를 통한 클라우드 가상자원 관리 수행 시 네트워크 트래픽 보호를 위한 암호화된 통신구간을 적용하여야 한다.

  - 예시

    1) SSL 적용 등

3 우수 사례

1) SSL 적용 (ex. TLS 1.3)

- ▶ 암호화된 통신구간 적용

  ① 사용자가 'API URL'에 'SSL'로 접속

  I. OpenAPI(https://openapi.samsungsdscloud.com/)로 접근 가능

  A. API의 endpoint가 SSL로 적용

| 그림 6.5.1 | AUTHPARAMS 요청 예시

4 참고 사항

- Samsung Cloud Platform 사용자 가이드에서는 OpenAPI 가이드가 소개되어 있음. 더 자세한 내용을 알고 싶으시면 해당 가이드 참조
  (https://cloud.samsungsds.com/openapiguide/#/docs/v3-ko-overview-overview)

7. 스토리지 관리

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

7 스토리지 관리

1 기준

식별번호	기준	내용
7.1.	**스토리지 접근 관리**	**스토리지 접근 시 적절한 통제방안을 적용하여야 한다.**

2 설명

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

  - 예시

    1) 외부 공개가 불필요한 경우, 스토리지 퍼블릭 엑세스 차단

    2) 스토리지에 접근 가능한 계정(IAM) 적용

    3) URL로 접근 시 접근 가능한 시간, 별도 IP 지정 등

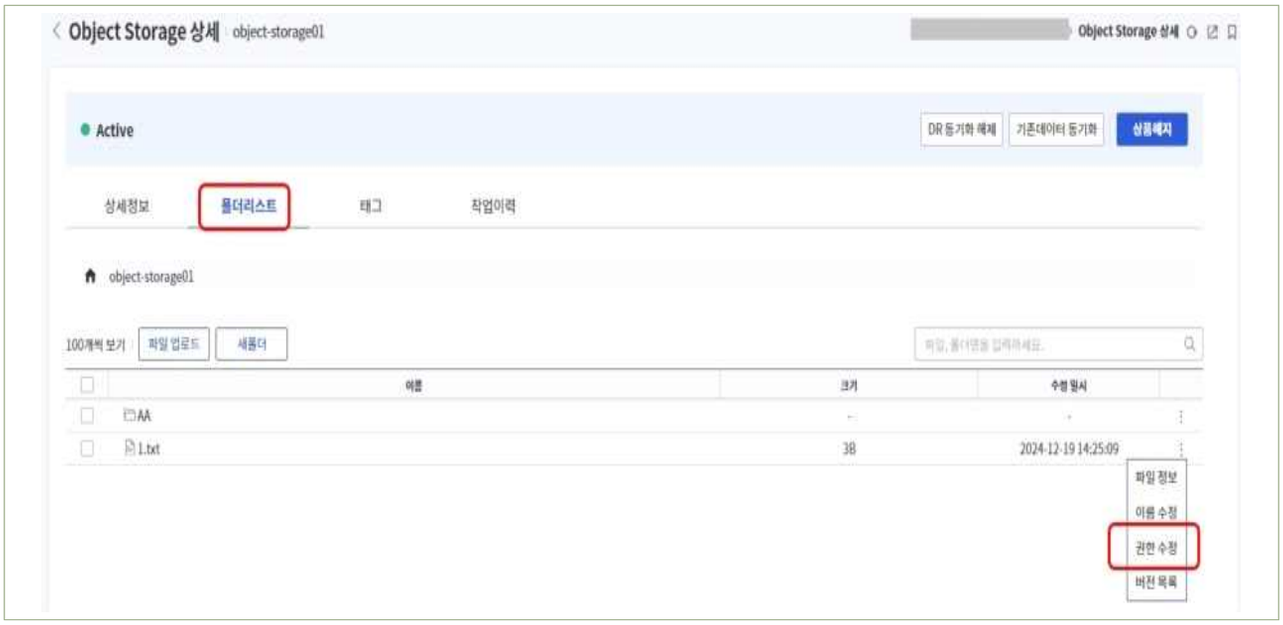
3 우수 사례

1) 외부 공개가 불필요한 경우, Object Storage의 퍼블릭 엑세스 차단

- Object Storage의 권한수정을 통해 퍼블릭 엑세스를 차단할 수 있고, 권한 현황을 조회할 수 있음

  ① 권한수정 : Object Storage 상세현황에서 파일에 대한 권한을 수정할 수 있습니다.

  - 신청 경로 : '모든상품' → 'Storage' → 'Object Storage' → '자원관리' → 'Object Storage상세' → '폴더리스트' → '권한수정'



| 그림 7.1.1 | Object Storage상세 (폴더리스트)

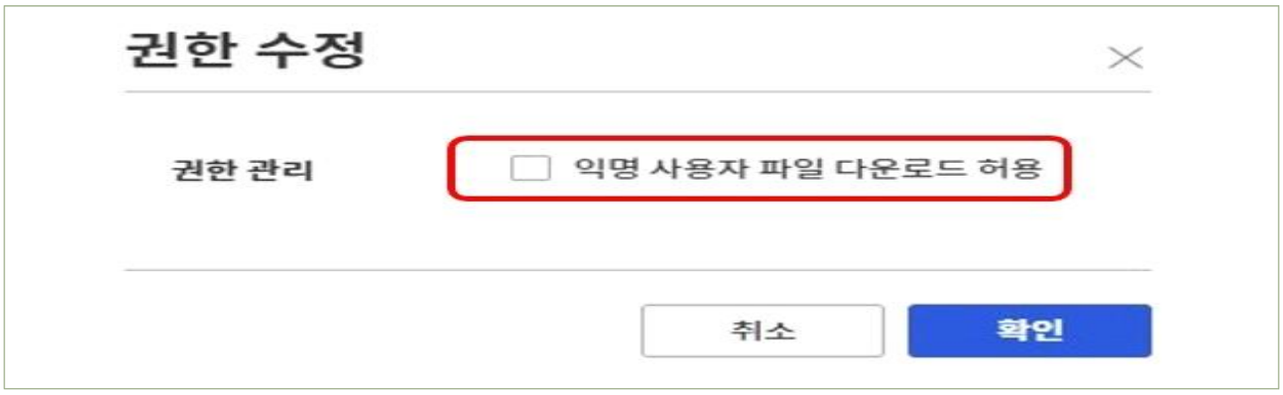
A. 폴더리스트 : 버킷내 전체 폴더와 파일을 조회합니다.

B. 폴더 목록에서 폴더 이름을 클릭하여 파일 목록을 확인할 수 있습니다.

C. 폴더 또는 파일의 첫 글자를 검색 영역에 입력하여 원하는 폴더나 파일을 찾을 수 있습니다.

D. 폴더 목록에서 폴더 항목의 오른쪽 끝에 있는 세로 줄임표(⋮)를 클릭하여 폴더의 정보를 확인하고 정보를 수정할 수 있습니다.

E. 권한수정을 클릭하여 권한수정 팝업화면을 조회합니다

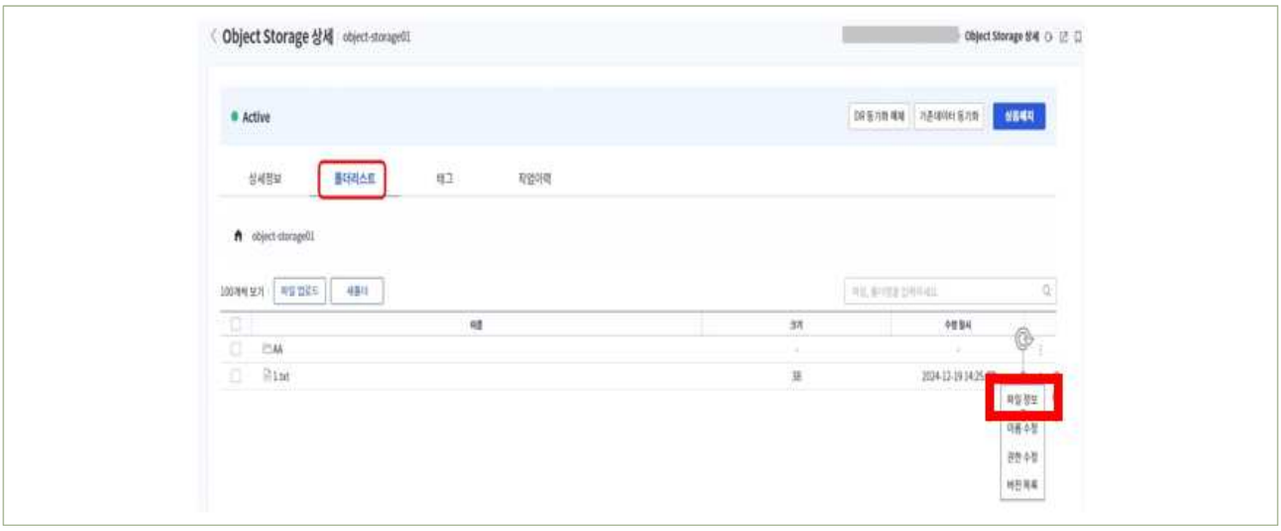


| 그림 7.1.2 | Object Storage상세 (권한수정)

- 익명사용자 파일 다운로드 허용을 체크하지 않고 확인을 클릭 시, 해당 파일에 대한 퍼블릭 엑세스를 차단합니다.
  (익명 사용자 파일 다운로드 허용을 체크할 경우, 외부에 공개 즉 퍼블릭 엑세스가 가능하게 됩니다)

② 권한조회 : 해당 파일의 파일정보를 조회하여 '익명 사용자 파일 다운로드 허용하지 않음'으로 권한이 부여되어, 퍼블릭 엑세스 권한을 허용하지 않는지 확인한다

- 신청 경로 : '모든상품' → 'Storage' → 'Object Storage' → '자원관리' → 'Object Storage상세' → '폴더리스트' → '파일정보'



| 그림 7.1.3 | Object Storage상세 (폴더리스트)

A. '파일 정보'를 클릭하여 권한수정 팝업화면을 조회합니다. 권한이 '익명 사용자 파일 다운로드 허용하지 않음'으로 셋팅된 것을 확인할 수 있습니다.

| 그림 7.1.4 | Object Storage상세 (파일정보)

2) 스토리지에 접근 가능한 계정(IAM) 적용

- 스토리지에 접근 가능한 계정 적용 가능

① 정책 및 권한그룹 생성: 사용자 정의 정책을 생성하고 권한그룹을 추가하여 어느 사용자에게 무슨 동작을 허용 또는 금지할지 설정할 수 있습니다.

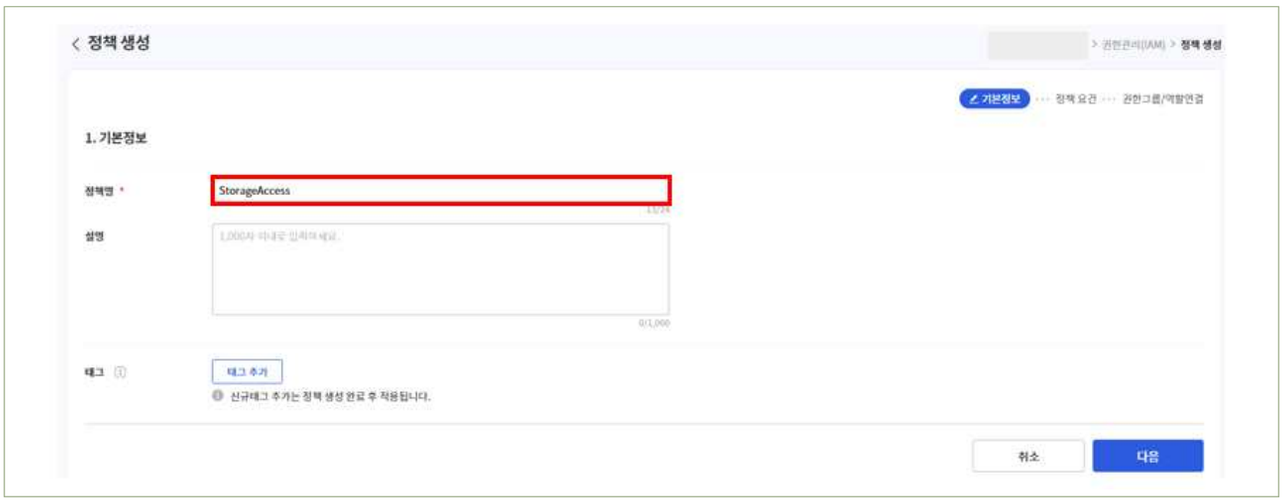
Ⅰ. 정책 생성

Ⅱ. 권한그룹 추가

Ⅲ. 정책-권한그룹 연결

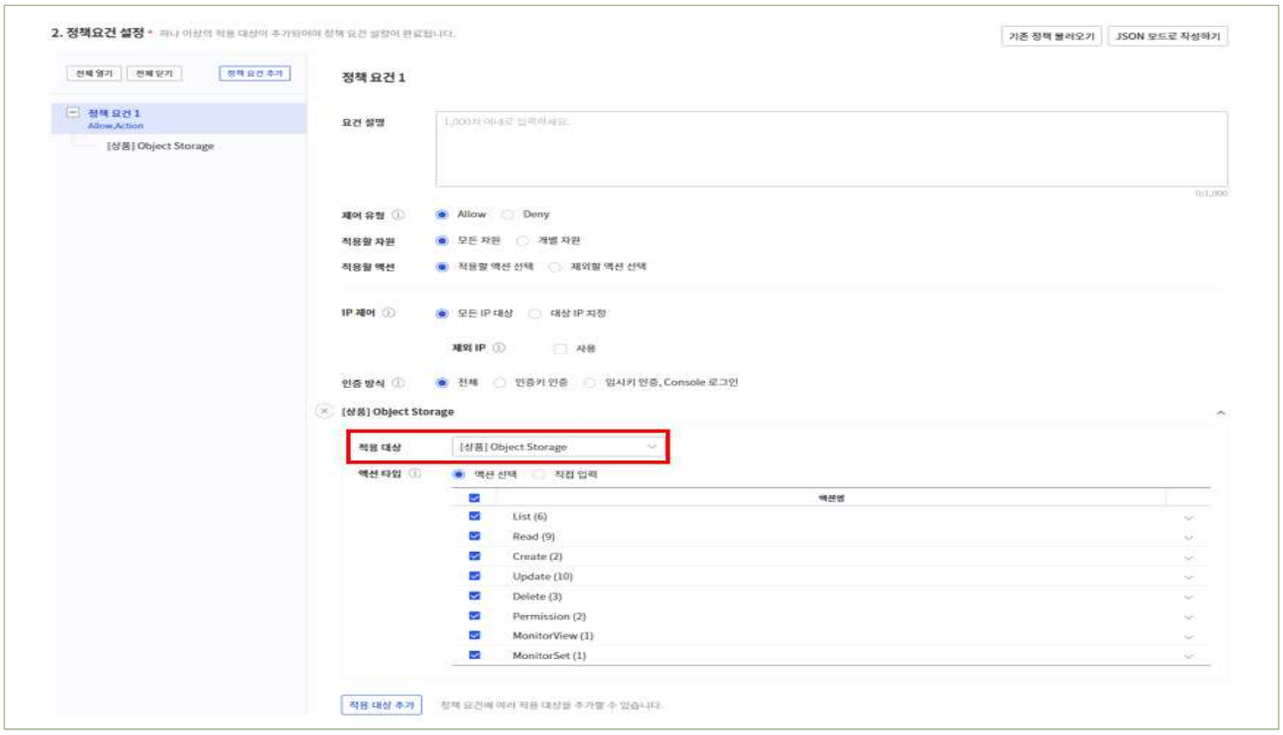
[Ⅰ. 정책 생성]

- 신청 경로: '프로젝트' → '권한관리(IAM)' → '정책'



| 그림 7.1.5 | 정책 생성 (기본정보 입력)

A. 정책명: 사용자 정의 정책의 이름을 입력합니다.



| 그림 7.1.6 | 정책 생성 (정책요건 설정)

A. 제어 유형: 정책 적용 대상의 접근 제어 방식을 설정합니다.
- Allow: 접근을 허용합니다.
- Deny: 접근을 거부합니다.

B. 적용할 자원: 정책이 적용될 대상 자원을 지정합니다.
- 모든 자원: 모든 자원을 대상으로 정책을 적용합니다.
- 개별 자원: 자원 목록을 지정하고 해당 자원에 대해 정책을 적용합니다. '적용할 액션'을 '제외할 액션 선택'으로 설정한 경우에는 선택할 수 없습니다.

C. 적용할 액션: 정책에 적용할 액션을 선택하는 방식을 설정합니다.
- '적용할 자원'이 '개별 자원'인 경우에는 '제외할 액션 선택'을 설정할 수 없습니다.

D. IP 제어: 정책 요건이 적용될 IP 주소 또는 범위를 설정합니다.
- 모든 IP 대상: 모든 IP를 정책 요건 대상으로 설정합니다.
- 대상 IP 지정: '/'를 이용하여 IP 대역을 지정하는 CIDR 방식으로 표기할 수도 있습니다. ex) 192.168.10.1 or 192.168.10.0/24
- 제외 IP: 정책 요건의 대상에서 제외할 IP를 등록합니다.

E. 인증 방식: 정책을 적용할 사용 대상의 인증 방식을 선택합니다.
- 전체: 인증 방식과 상관없이 적용
- 인증키 인증: 인증키로 인증한 사용자에게 적용

- 임시키 인증, Console 로그인: 임시키로 인증한 사용자나 Console 로그인한 사용자에게 적용

F. 적용 대상: 정책 요건을 적용할 대상을 선택합니다.

G. 액션 타입: 정책 요건의 내용을 적용할 액션을 목록에서 선택하거나 직접 입력할 수 있습니다.

H. 적용 대상 추가: 정책 요건을 적용할 대상을 추가합니다.

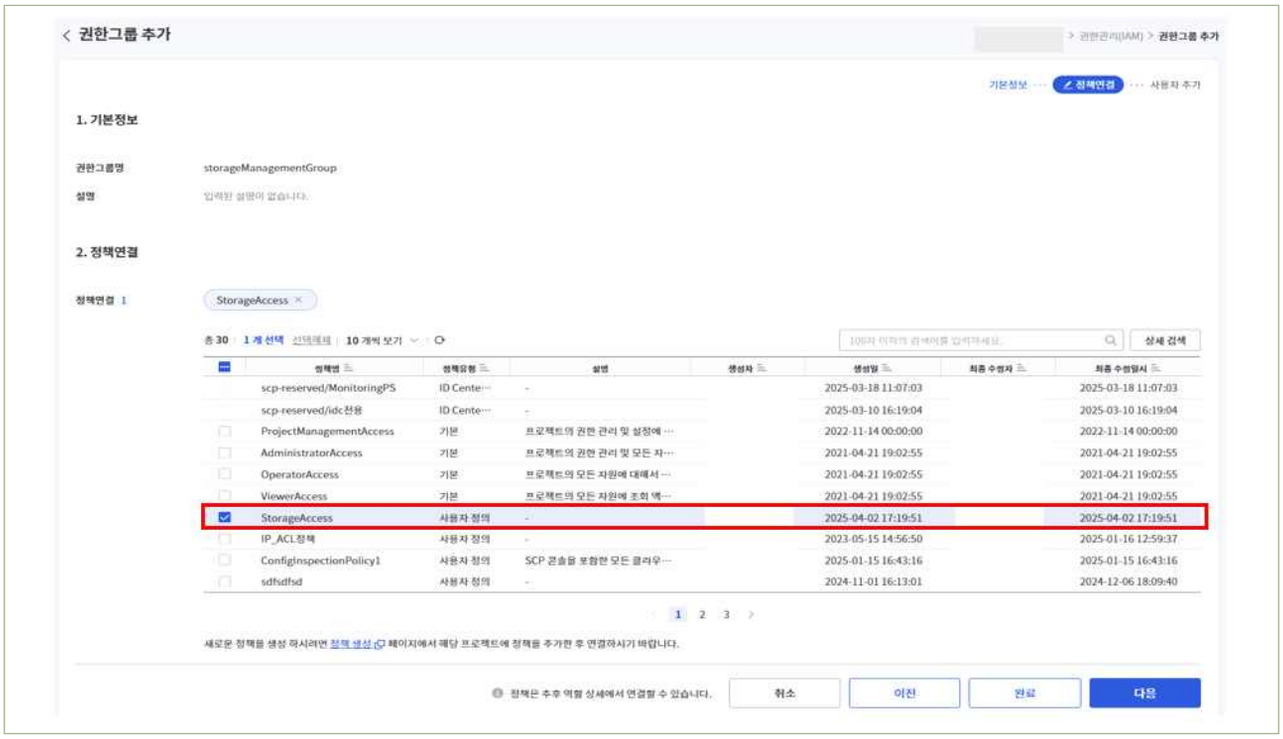
- 정책 요건에 여러 적용 대상을 추가할 수 있습니다.

[II. 권한그룹 추가]

- 신청 경로: '프로젝트' → '권한관리(IAM)' → '권한그룹'

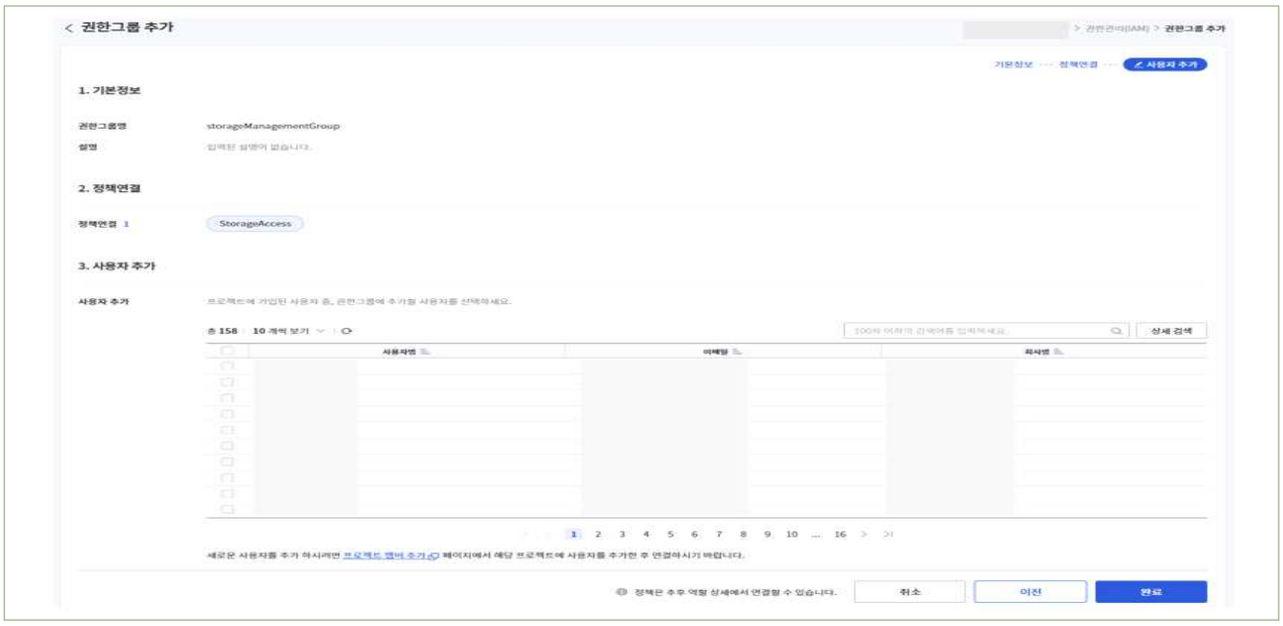
| 그림 7.1.7 | 권한그룹 추가 (기본정보 입력)

A. 권한그룹명: 사용자 정의 권한그룹의 이름을 입력합니다.



| 그림 7.1.8 | 권한그룹 추가 (정책 연결)

A. 정책 목록에서 권한그룹에 연결할 정책을 선택합니다.



| 그림 7.1.9 | 권한그룹 추가 (사용자 추가)

A. 사용자 목록에서 권한그룹에 추가할 사용자를 선택합니다.

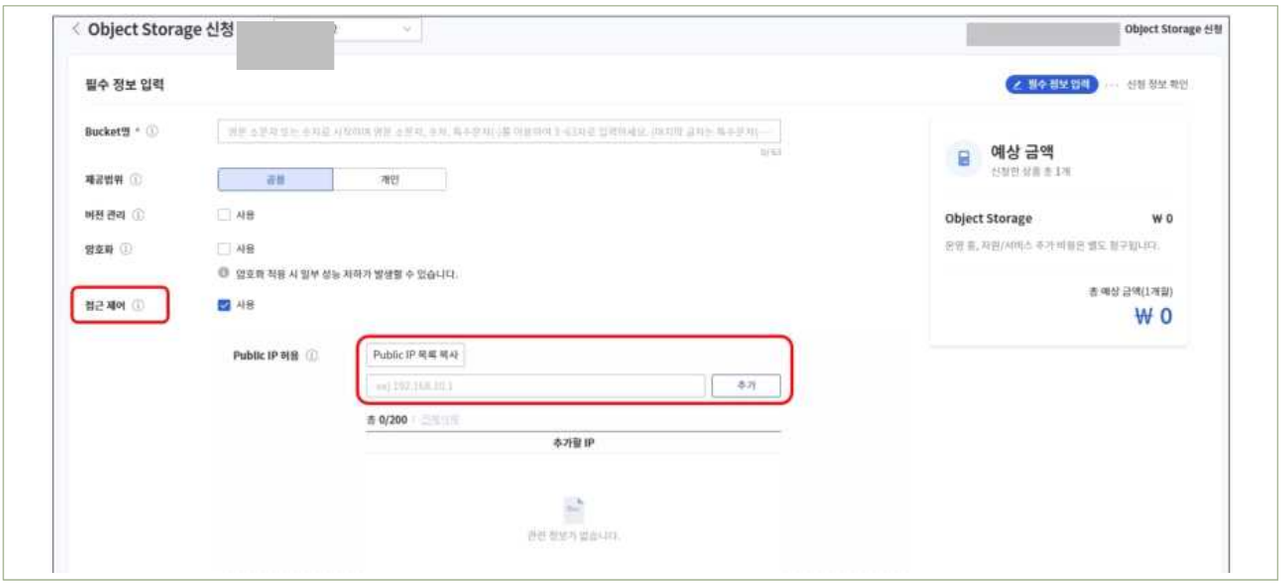
- 여러 사용자를 동시에 선택할 수 있습니다.

3) URL로 접근 시 접근 가능한 별도 IP 지정

- 스토리지에 대한 접근 가능한 IP 등록 및 수정 가능.

① 접근가능 IP 등록: Object Storage 신청시, 등록한 IP만 접근 가능합니다.

- 신청 경로 : '모든상품' → 'Storage' → 'Object Storage' → '상품신청' → (Public IP 허용) '추가



| 그림 7.1.10 | Object Storage 신청 (Public IP 허용)

A. Bucket명: Bucket 이름을 입력한 후, 중복체크를 클릭해 중복 여부를 확인합니다.

B. 제공범위: Bucket과 스토리지 인증키의 제공 범위를 설정합니다.

- 개인: 사용자 고유의 인증키로 사용하며 신청자의 목록에서만 Bucket 및 인증키를 확인할 수 있습니다. Samsung Cloud Platform Console의 계정 정보가 없는 경우에는, 버튼이 표시되지 않습니다.
- 공용: 프로젝트 단위의 인증키를 통하여 Bucket을 사용할 수 있습니다.

C. 버전 관리: 사용으로 설정하면 Object 이력을 저장하고 관리할 수 있습니다

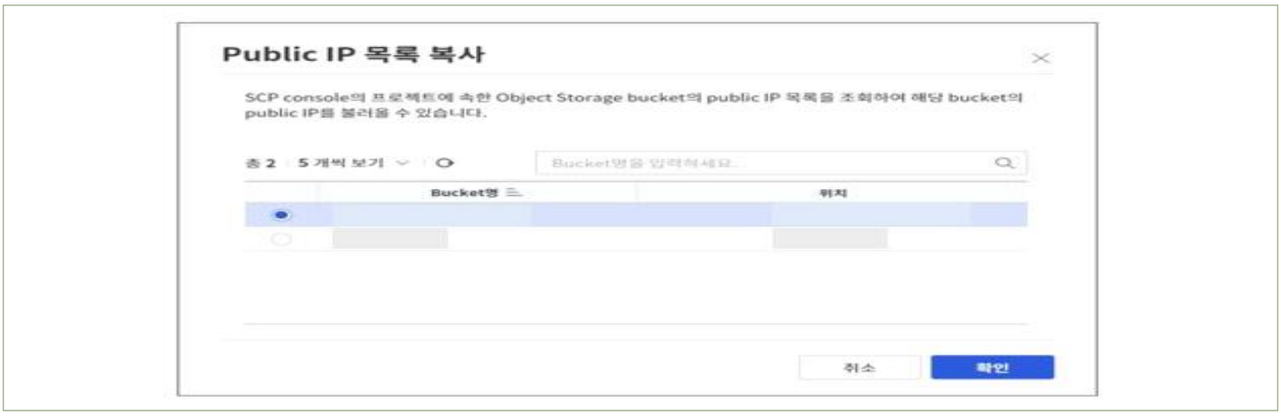
- DR을 사용하려면 버전 관리를 사용으로 설정해야 합니다.

D. 암호화: 사용을 선택하면 SSE-S3 암호키 방식 및 AES256 암호화 알고리즘을 적용할 수 있습니다.

E. 접근제어: 사용을 선택하면 생성할 버킷에 대한 접근이 허용되는 IP나 자원을 지정할 수 있습니다.

F. Public IP 허용: 사용자 PC에서 버킷에 파일을 업로드 하거나 버킷의 파일을 다운로드 하려면 사용자 IP를 추가해야 합니다.

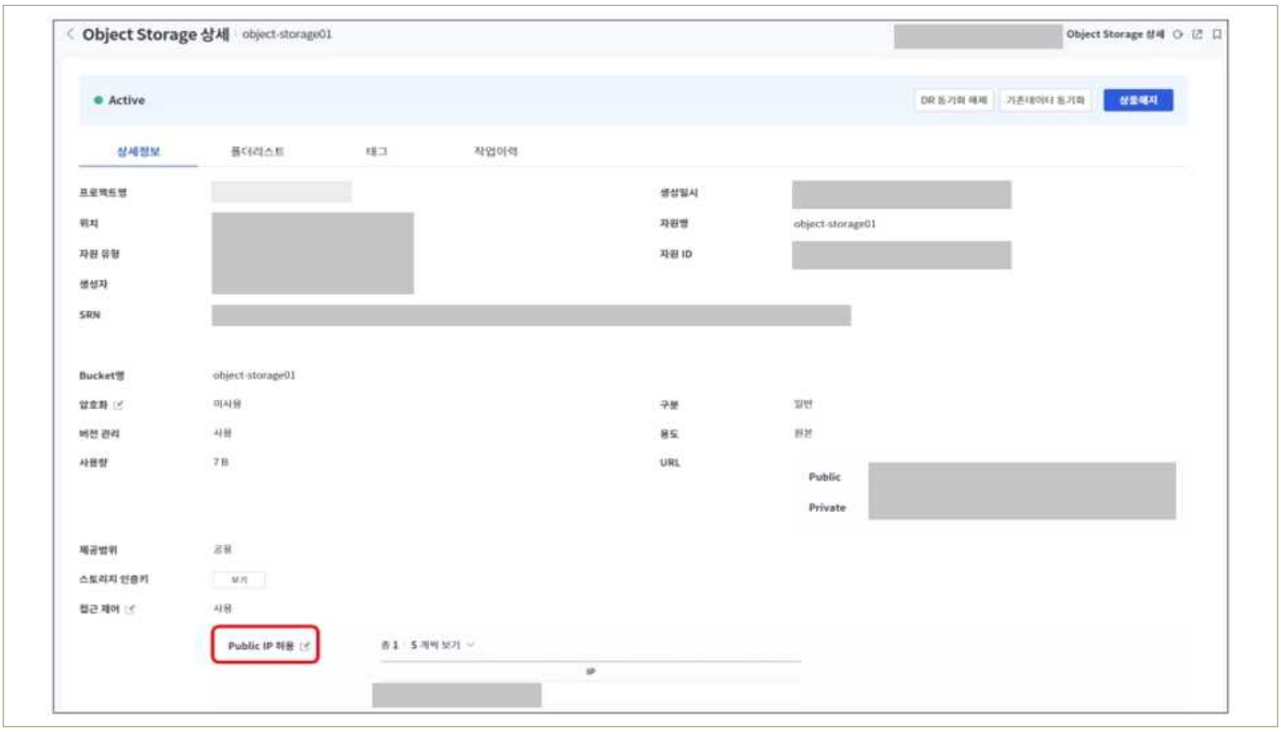
- 사용자 PC에서 업로드/다운로드 시 사용자 PC에 연계된 NAT IP로 버킷에 접근하므로 해당 NAT IP를 등록해야 합니다.
- 여러 NAT IP를 등록하려는 경우, CIDR 형식을 이용해 "100.100.100.100/24"와 같이 간편하게 등록할 수 있습니다.
- 'Public IP 목록 복사'를 클릭하면 사용자의 프로젝트 내, 다른 버킷에 지정된 IP를 불러올 수도 있습니다. 아래 예시에서는 'object-Storage01' 버킷에 이미 등록되어 있는 IP목록을 복사할 수 있습니다.



| 그림 7.1.11 | Public IP 목록 복사

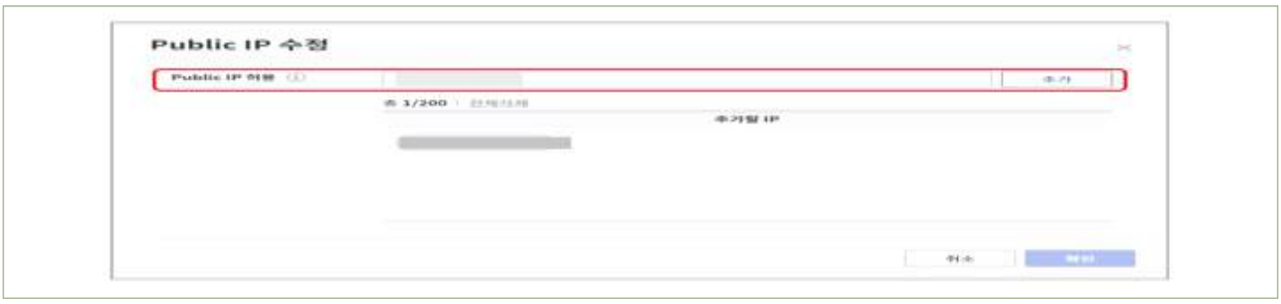
② 접근가능 IP 수정: "Object Storage 상세" 페이지의 상세정보 탭에서 접근 가능한 Public IP를 수정할 수 있습니다

- 신청 경로 : '모든상품' → 'Storage' → 'Object Storage' → '자원관리' → 'Object Storage 상세' → '상세정보' → 'Public IP 허용'



| 그림 7.1.12 | Object Storage 상세 (Public IP 허용)

A. ‘Public IP 허용‘을 클릭하면, 기존 등록된 Public IP 목록이 조회되며, 기존 등록된 Public IP를 삭제 및 신규 Public IP를 추가할 수도 있습니다.



| 그림 7.1.13 | Public IP 수정

- 허용할 IP를 입력하고 ‘추가’ 클릭하면 아래에 ‘추가할 IP’ 목록에 반영됩니다
- ‘추가할 IP’ 목록’ 에서 삭제하려면, 대상 IP 끝에 있는 ‘X’를 클릭하면 목록에서 삭제됩니다.
- 최종적으로 ‘확인’ 클릭 시 ‘추가할 IP’ 목록’에 있는 IP 값들이 접근 가능 하게 됩니다.

4 참고 사항

- Samsung Cloud Platform 사용자 가이드」에서는 Object Storage의 Public 엑세스 차단 및 URL로 접근 시 접근 가능한 별도 IP 지정 관련 활용 가이드가 소개되어 있음. 더 자세한 내용을 알고 싶으시면 해당 가이드 참조
  (https://cloud.samsungsds.com/manual/ko/scp_user_guide.html#d01f41140c011ef2)

1 기준

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

2 설명

- 스토리지 목적에 따라 읽기, 쓰기 등 권한을 세분화하여 적용하고 관리하여야 한다.

  - 예시

    1) 스토리지 객체 권한(읽기, 쓰기 등)을 목적에 따라 적용

    2) 스토리지 권한 부여 현황에 대해 주기적인 검토 수행 등

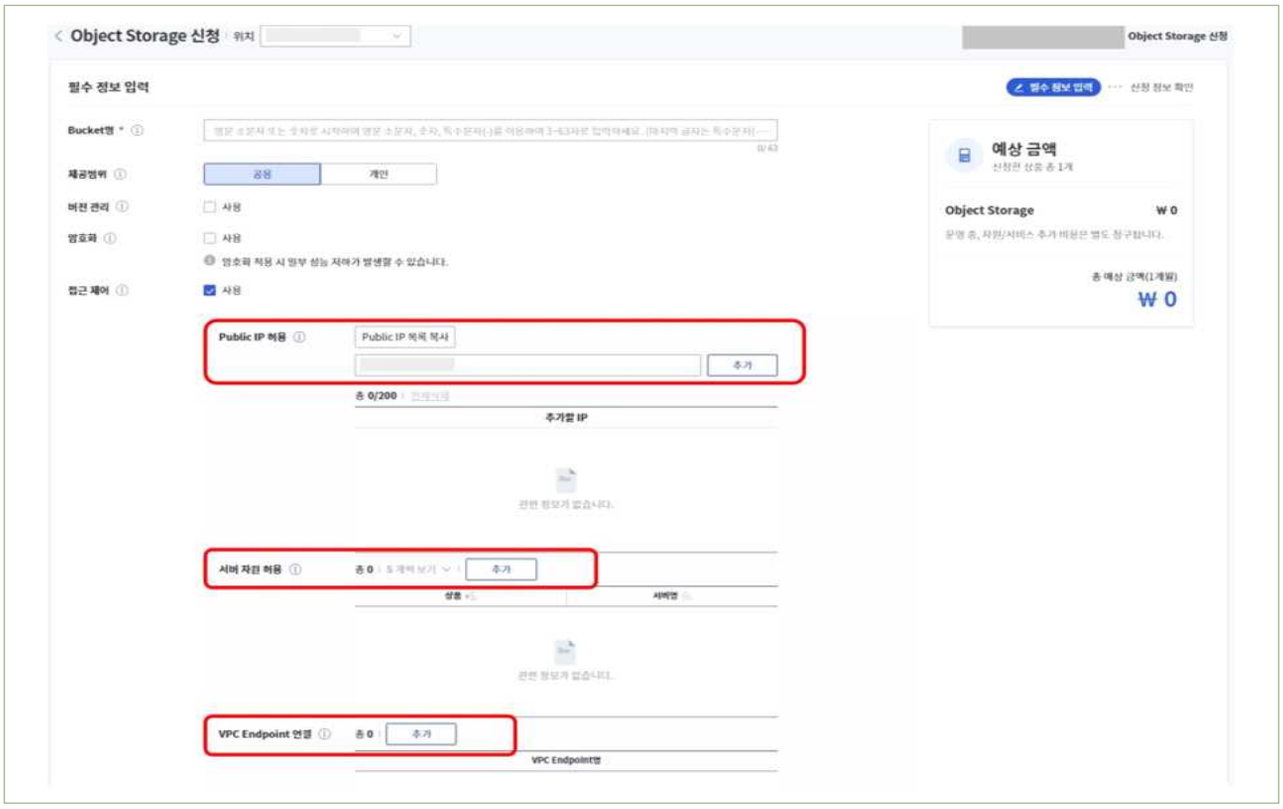
3 우수 사례

1) 목적에 따라 다양한 접근 제어 방법으로 객체 권한(읽기, 쓰기) 제공

- 다양한 접근 제어 방법(Public IP 허용, 서버 자원 허용, VPC Endpoint 연결)으로 객체에 권한(읽기, 쓰기)을 제공하며, 또한 모든 사용자에게 읽기 권한만 제공할 수도 있습니다.

  ① 객체 권한 등록: Object Storage 신청 시, 다양한 접근 제어 등록을 통한 권한(읽기, 쓰기)을 등록합니다.

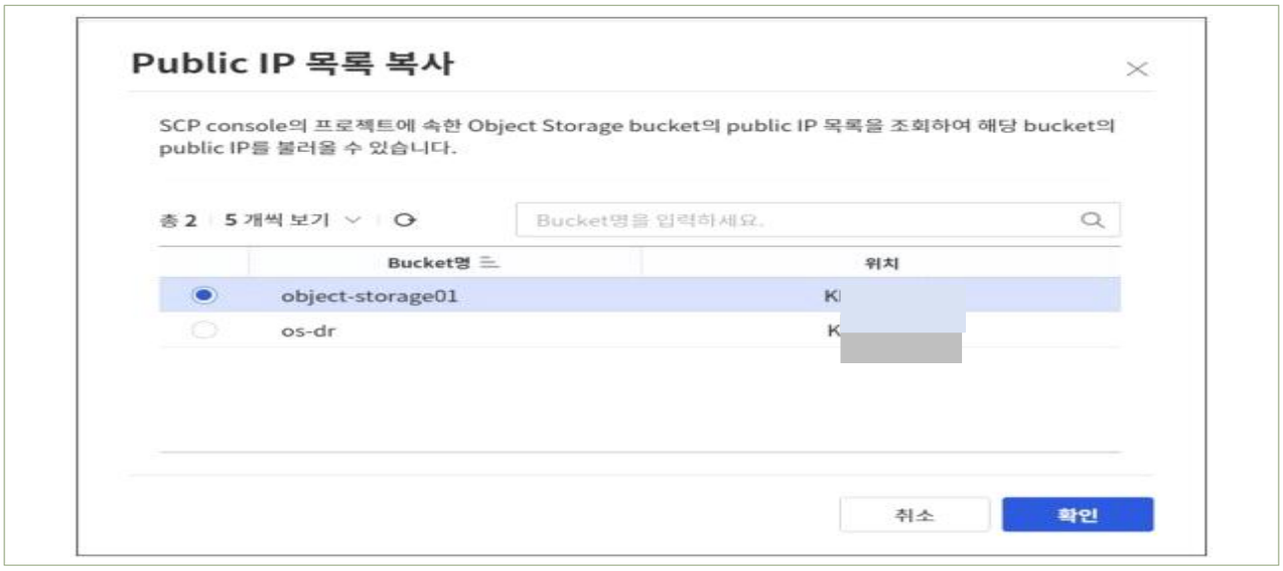
  - 신청 경로 : '모든상품' → 'Storage' → 'Object Storage' → '자원관리' → '상품신청' → '접근제어'



| 그림 7.2.1 | Object Storage 신청 (접근 제어)

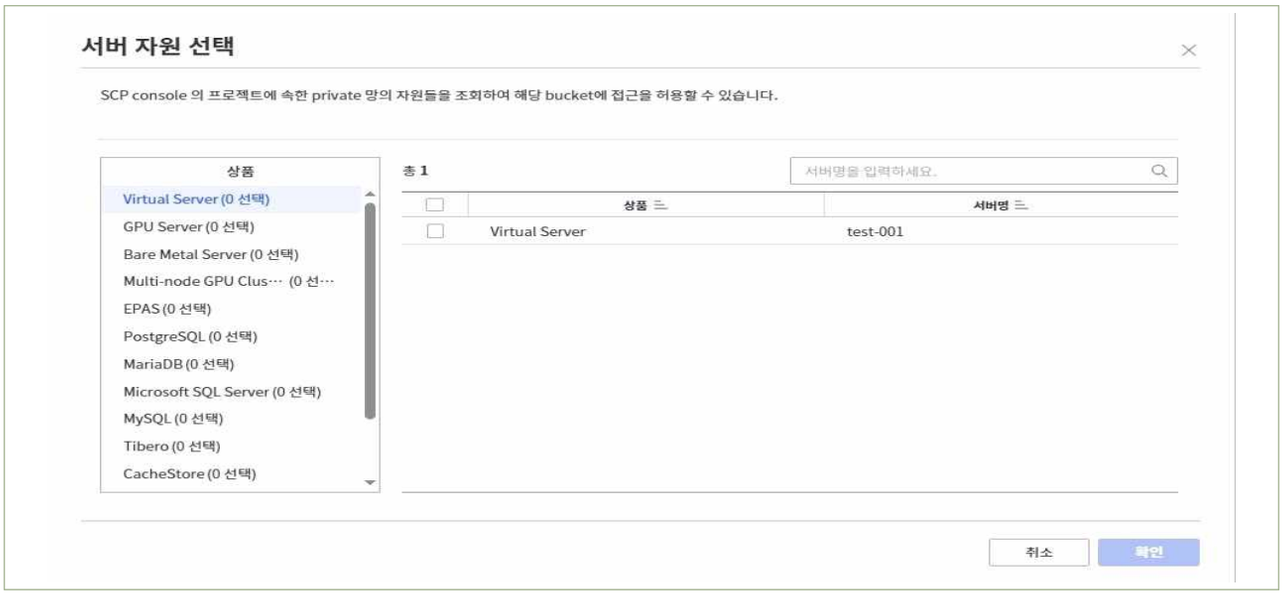
A. Public IP 허용: 사용자 PC에서 버킷에 파일을 업로드 하거나, 버킷의 파일을 다운로드 하려면 사용자 IP를 추가해야 합니다.

- 사용자 PC에서 업로드/다운로드 시 사용자 PC에 연계된 NAT IP로 버킷에 접근하므로 해당 NAT IP를 등록해야 합니다.
- 여러 NAT IP를 등록하려는 경우, CIDR 형식을 이용해 "100.100.100.100/24"와 같이 간편하게 등록할 수 있습니다.
- ‘Public IP 목록 복사’를 클릭하면 사용자의 프로젝트 내 다른 버킷에 지정된 IP를 불러올 수도 있습니다. 아래 예시에서는 ‘Object-Storage01’ 버킷에 이미 등록되어 있는 IP 목록을 복사할 수 있습니다.



| 그림 7.2.2 | Public IP 목록 복사

B. 서버 자원 허용: 동일 프로젝트에 속한 Private 망의 자원들이 해당 버킷에 접근하도록 허용할 수 있습니다. '추가'를 클릭하면 사용자의 프로젝트에 속한 Private망의 자원들을 조회하고 접근 허용하도록 선택할 수 있습니다.



| 그림 7.2.3 | 서버 자원 선택

C. VPC Endpoint 연결: Object Storage Bucket과 연결할 VPC Endpoint를 설정합니다. 추가를 클릭하여 동일 프로젝트, 동일 위치에 생성된 VPC Endpoint의 자원을 추가할 수 있습니다.

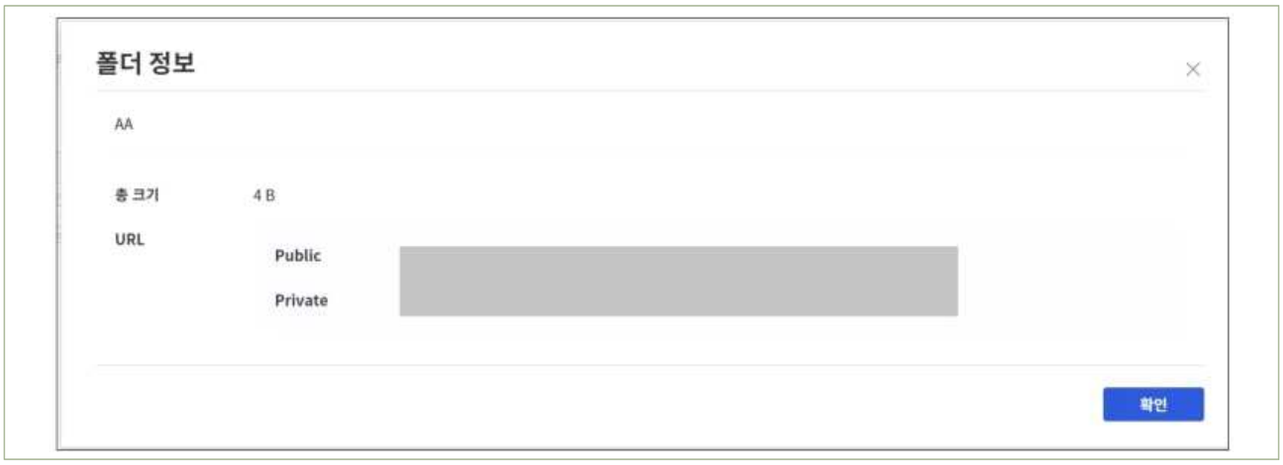
| 그림 7.2.4 | VPC Endpoint 선택

② 모든 사용자에게 읽기 권한만 제공할 수도 있습니다.

- 신청 경로 : '모든상품' → 'Storage' → 'Object Storage' → '자원관리' → 'Object Storage 상세' → '폴더리스트'

| 그림 7.2.5 | Object Storage 상세 (폴더리스트)

A. 각 항목의 우측 끝에 있는 세로 줄임표(⋮)를 클릭해서 '폴더 정보'를 클릭하여 폴더 정보를 확인할 수 있습니다. URL 복사를 클릭하면 해당 URL을 복사할 수 있습니다.



| 그림 7.2.6 | Object Storage 상세 (폴더정보)

B. 각 항목의 오른쪽 끝에 있는 세로 줄임표(⋮)를 클릭해서 'Public Access 권한부여'를 선택 후, 'Public Access 권한부여' 팝업화면에서 확인을 클릭 시, 해당폴더에 대한 읽기권한을 전체 사용자에게 부여됩니다.

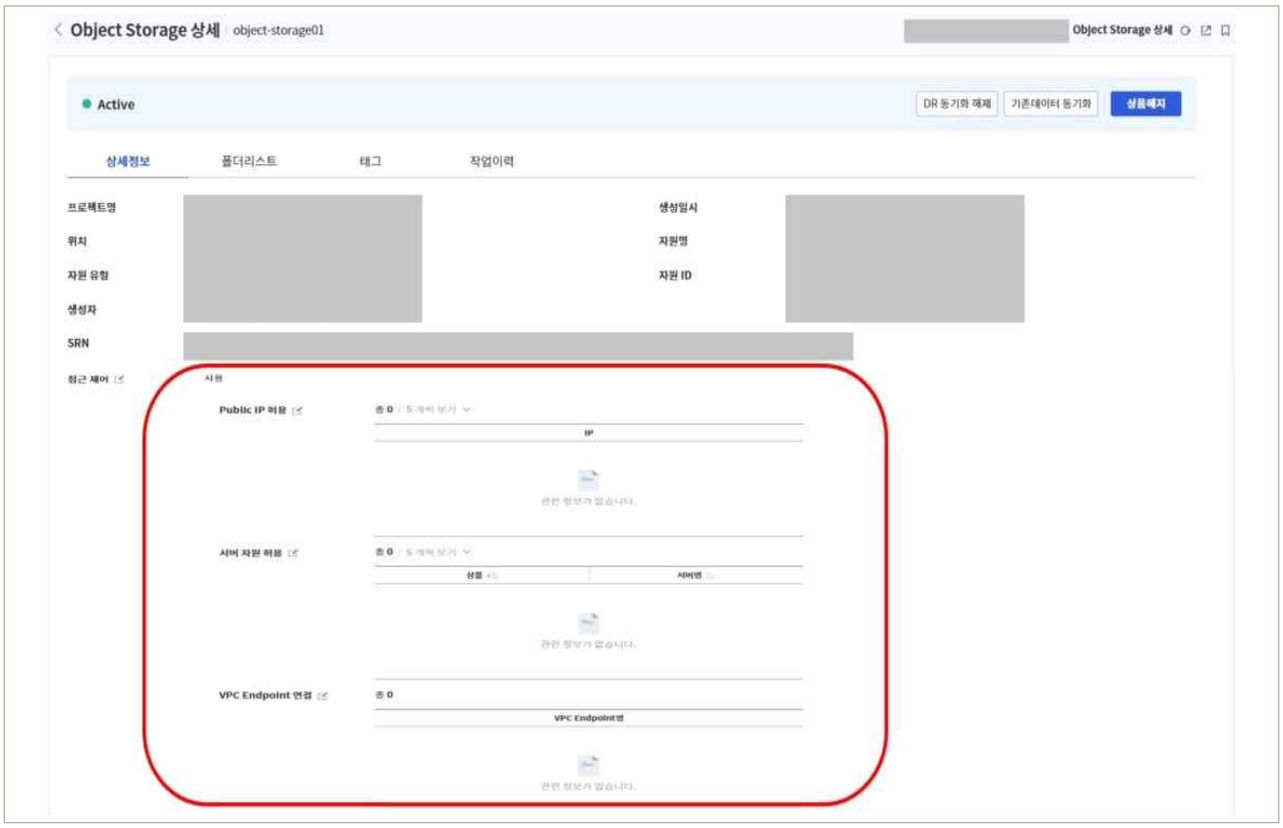
| 그림 7.2.7 | Object Storage 상세 (Public Access권한 부여)

2) 스토리지 권한 부여 현황에 대해 주기적인 검토 수행 등

- 스토리지 접근제어 현황을 통해 권한조회를 하고 주기적으로 권한 적정성에 대한 검토 수행

① 스토리지의 다양한 접근 제어 현황을 조회 및 검토

- 신청 경로 : '모든상품' → 'Storage' → 'Object Storage' → '자원관리' → 'Object Storage 상세' → '상세정보' → '접근제어'

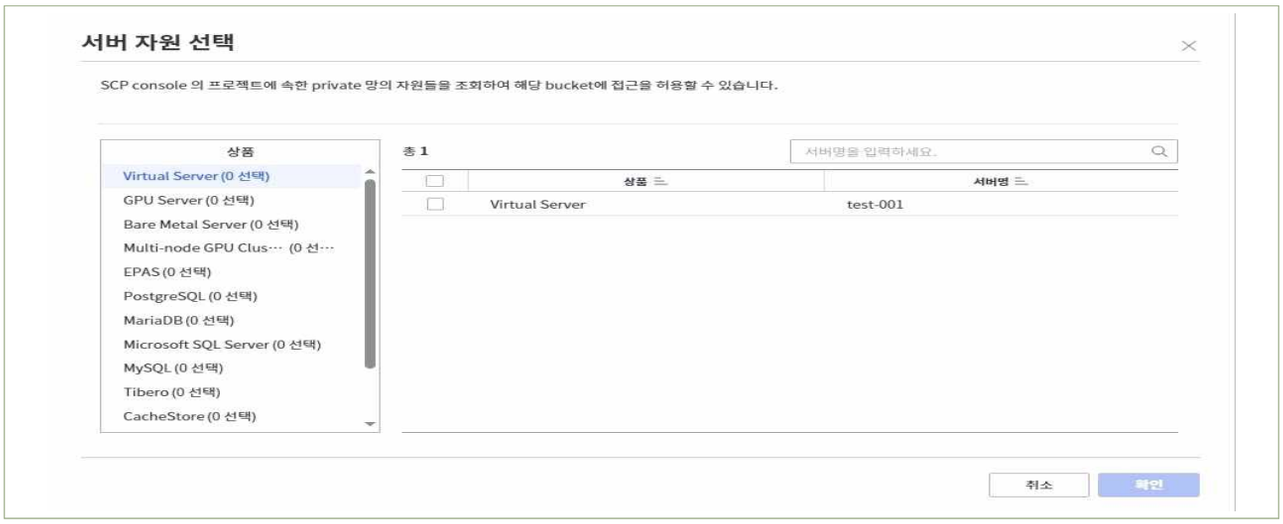


| 그림 7.2.8 | Object Storage 상세 (접근제어 현황) MS 변경(키 회전)

A. 'Public IP 허용'을 클릭하면, 기존 등록된 Public IP 목록이 조회되며, 기존 등록된 Public IP를 삭제할 수도 있고, 신규 Public IP를 추가할 수도 있습니다.

| 그림 7.2.9 | Public IP 수정

B. 서버 자원 허용: 동일 프로젝트에 속한 Private 망의 자원들이 해당 버킷에 접근하도록 허용할 수 있습니다. '추가'를 클릭하면 사용자의 프로젝트에 속한 Private 망의 자원들을 조회하고 접근 허용하도록 선택할 수 있습니다.



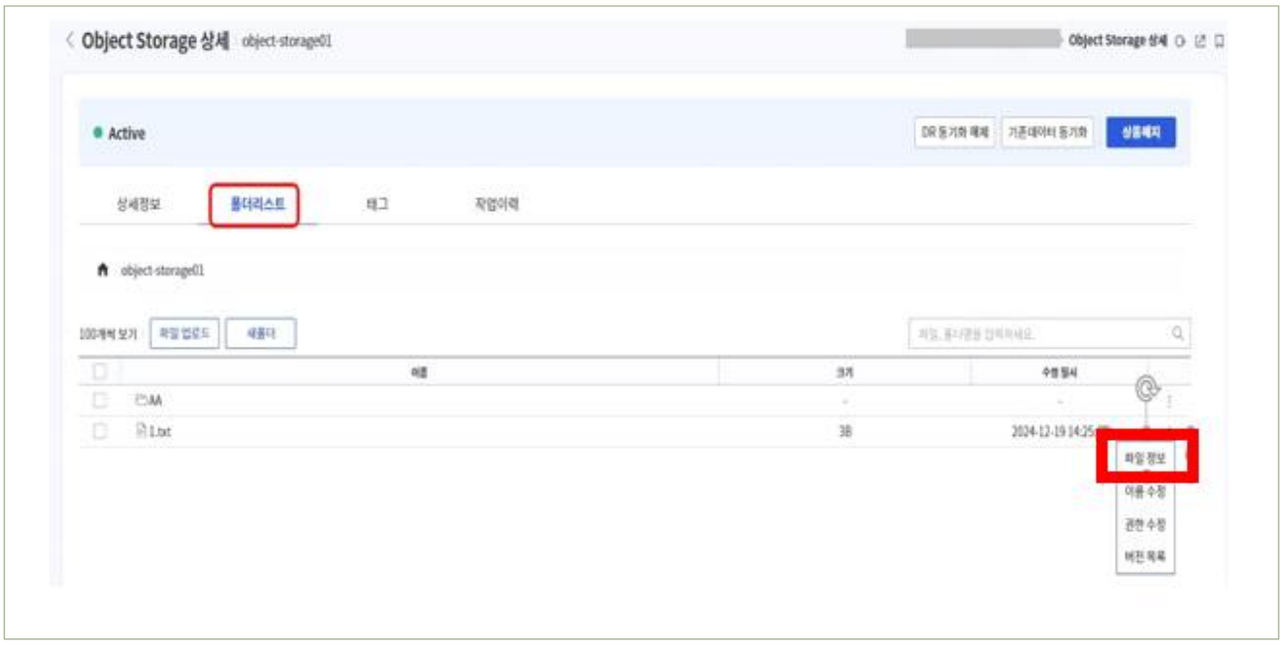
| 그림 7.2.10 | 서버 자원 선택

C. VPC Endpoint 연결: Object Storage Bucket과 연결할 VPC Endpoint를 설정합니다. 추가를 클릭하여 동일 프로젝트, 동일 위치에 생성된 VPC Endpoint의 자원을 추가할 수 있습니다.

| 그림 7.2.11 | VPC Endpoint 선택

② 모든 사용자에게 읽기 권한이 적절히 부여되었는지 조회하고 검토

- 해당 파일의 '파일정보'를 조회하여 '익명 사용자 파일 다운로드 허용하지 않음'의 체크 유무를 확인하여 퍼블릭 엑세스 권한을 허용하지 않는지 확인합니다
- 신청 경로 : '모든상품' → 'Storage' → 'Object Storage' → '자원관리' → 'Object Storage상세' → '폴더리스트' → '파일 정보'



| 그림 7.2.12 | Object Storage 상세현황 (폴더리스트)

A. '파일 정보'를 클릭하여 권한수정 팝업화면을 조회합니다. 권한이 '익명사용자 파일 다운로드 허용하지 않음'으로 세팅된 것을 확인할 수 있습니다

| 그림 7.2.13 | Object Storage 상세현황 (파일정보)

- ‘익명사용자 파일 다운로드 허용’으로 수정하려면, 권한수정 Popup화면에서 ‘익명사용자 파일 다운로드 허용’을 체크하면 됩니다
- 신청 경로 : ‘모든상품’ → ‘Storage‘ → ‘Object Storage‘ → ‘자원관리’ → ‘Object Storage 상세‘ → ‘폴더리스트‘ → ‘권한 수정‘

| 그림 7.2.14 | Object Storage 상세(권한수정)

4 참고 사항

- Samsung Cloud Platform 사용자 가이드」에서는 스토리지 목적에 따라 권한을 적용/관리 활용 가이드가 소개되어 있음. 더 자세한 내용을 알고 싶으시면 해당 가이드 참조 (https://cloud.samsungsds.com/manual/ko/scp_user_guide.html#d01f41140c011ef2)
- Samsung Cloud Platform 사용자를 위한 ISMS-P 인증기준 준수 가이드(52p)

SCP 활용 방안

③ Logging&Audit 상품을 활용한 로그 보관 및 접근권한 관리

SCP는 기본적으로 사용자가 수행하는 모든 활동 내역을 90일간 저장하고 있어, SCP Console 내 각 상품의 '작업 이력' 메뉴에서 수행한 작업 내역, 작업 결과, 작업자 등의 정보를 확인할 수 있습니다. 다만 클라우드 자원에 대한 변경 추적, 문제 해결, 보안 감사를 위해 90일을 초과하는 기간의 활동 내역을 보관하고자 하는 경우, Logging&Audit의 Trail 서비스를 활성화하여 지정한 Object Storage에 장기간 보관할 수 있습니다. Trail 서비스를 활성화할 때에는 적용 범위를 '전체 위치/전체 자원/전체 사용자'로 설정하는 것을 권장합니다. 또한 '로그파일 검증' 기능을 활성화하면 Trail 로그파일의 변경 및 삭제를 검증하기 위해 동일한 버킷에 Digest 파일을 저장하여 보관할 수 있고, '권한관리 (IAM)' 에서 해당 상품에 접근할 수 있는 사용자를 제한하는 정책을 만들어 로그 기록에 대한 접근 권한을 최소화할 수 있습니다.

- https://cloud.samsungsds.com/serviceportal/intro/techreport/repo3.html

1 기준

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

2 설명

- 스토리지 목적에 맞는 파일만 업로드 될 수 있도록 업로드 가능한 파일을 제한하여야 한다.

  - 예시

    1) 스토리지 버킷 정책 설정을 통한 업로드 파일 확장자 제한 등

    2) 금융회사에서 스토리지 내 파일 업로드 시 확장자 등을 검증할 수 있는 절차 마련

3 우수 사례

1) 스토리지 버킷 정책 설정을 통한 업로드 파일 확장자 제한 등

- N/A

2) 금융회사에서 스토리지 내 파일 업로드 시 확장자 등을 검증할 수 있는 절차 마련

- N/A

4 참고 사항

- N/A

8. 백업 및 이중화 관리

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

8 백업 및 이중화 관리

1 기준

식별번호	기준	내용
8.1.	**클라우드 이용에 관한 행위추적성 증적 (로그 등) 백업**	**클라우드 이용 내역을 추적할 수 있도록 관련 자료를 백업(1년 이상 보관)하여야 한다.**

2 설명

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

  - 예시

    1) 스토리지 행위 감사로그 백업

    2) 클라우드 웹 콘솔 감사로그 별도의 파일로 보관 등

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

3 우수 사례

1) 클라우드 웹 콘솔 감사로그 별도의 파일로 보관 등

- 자원별(혹은 전체), 계정별 활동내역을 Trail을 통해서 영구 보존하고 감사나 보안 사고에 근거 자료로 사용 가능

  ① Trail: Console과 API 호출을 통해 발생하는 사용자 활동 기록을 Object Storage와 연동하여 장기간 보관할 수 있습니다.

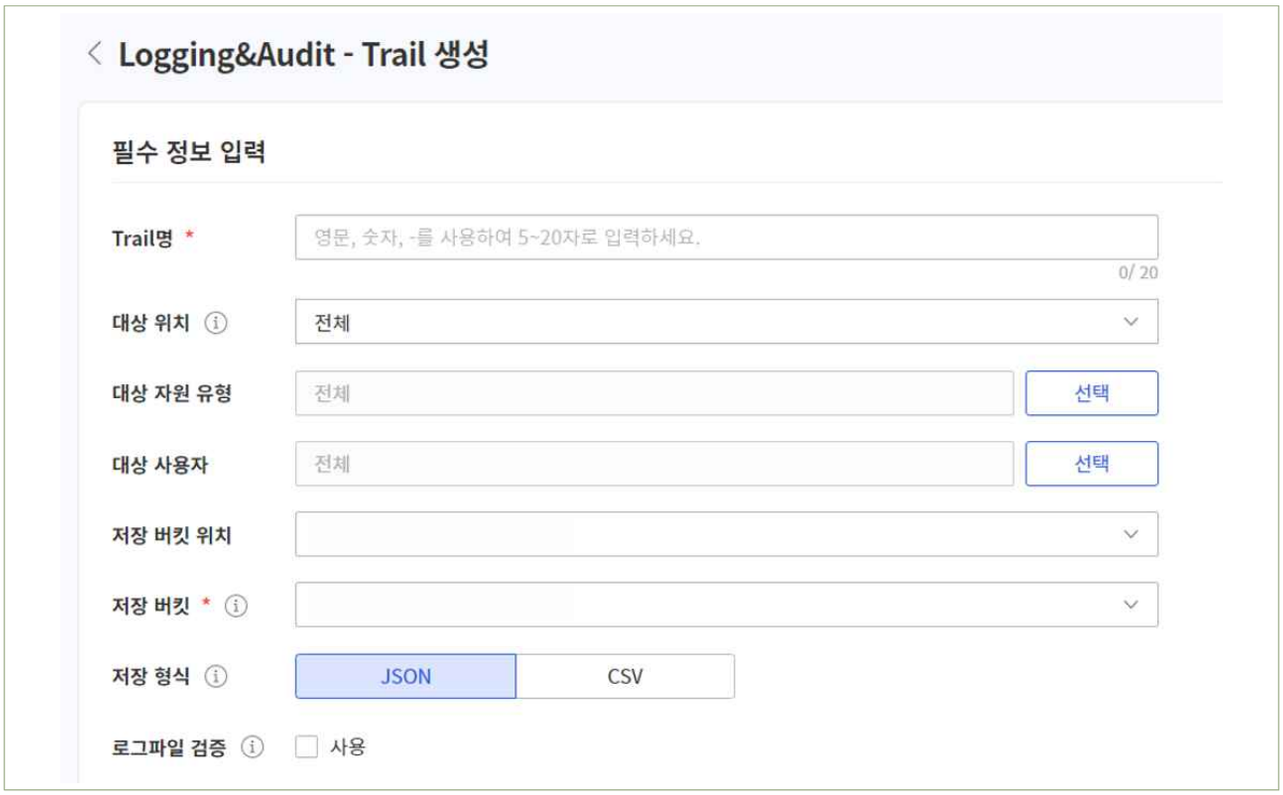
  Ⅰ. Trail 생성

  Ⅱ. Trail 상세 정보 확인

  Ⅲ. Trail 로그 확인

[I. Trail 생성]

- 신청 경로: '프로젝트' → '모든 상품' → 'Management' → 'Logging&Audit' → 'Trail' → Trail 생성



| 그림 8.1.1 | Trail 생성

A. 대상 위치: 활동 이력을 기록할 대상 위치를 선택할 수 있습니다.

B. 대상 자원 유형: 활동 이력을 기록할 대상 상품을 선택할 수 있습니다.

C. 대상 사용자: 활동 이력을 기록할 사용자(계정)를 선택할 수 있습니다.

D. 저장 버킷 위치: Trail의 위치에 해당하는 Object Storage를 선택합니다.

E. 저장 버킷: Trail을 생성할 Object Storage 버킷을 선택합니다.

- 버킷이 없을 경우 Trail을 생성할 수 없으므로 미리 생성하세요.

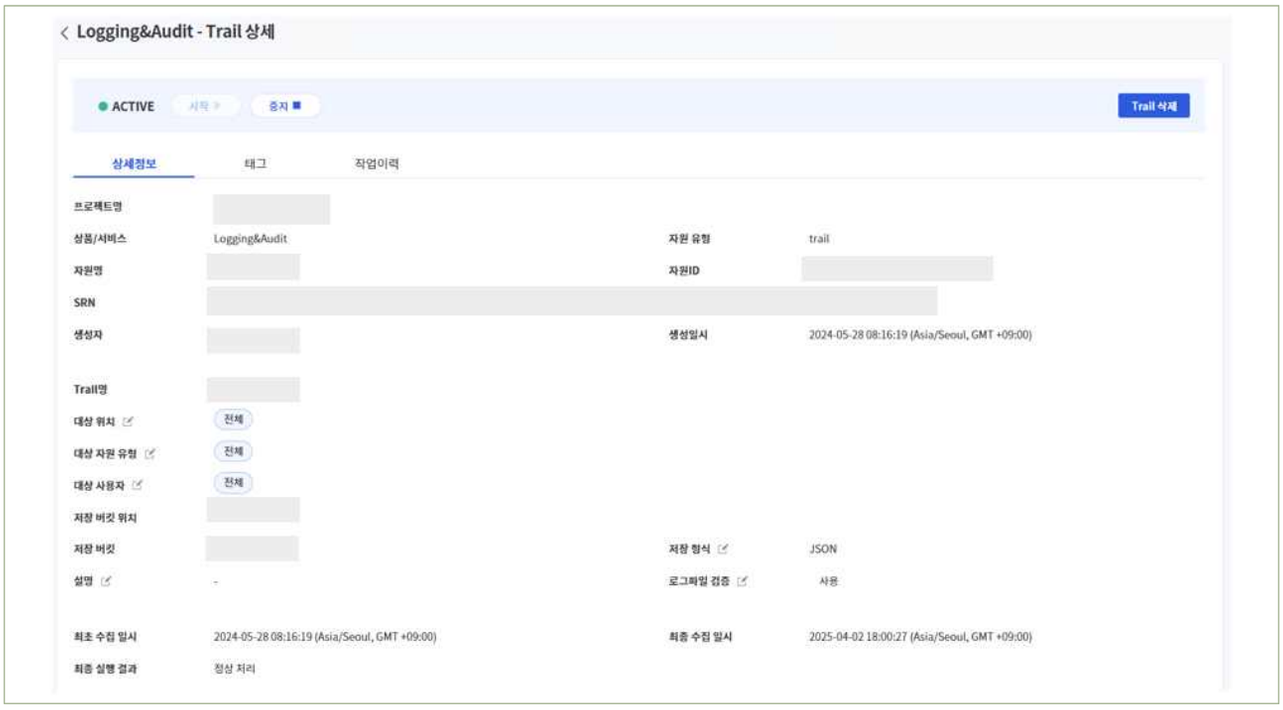
F. 저장 형식: 로그 데이터를 저장하는 파일 포맷을 JSON 또는 CSV 중 선택할 수 있습니다.

G. 로그파일 검증: Trail 로그파일의 변경 및 삭제를 검증하기 위해 동일한 버킷에 Digest 파일을 저장합니다.

- 로그 파일과 Digest 파일의 검증은 OpenAPI 또는 CLI를 사용하여 가능합니다.

[II. Trail 상세 정보 확인]

- 확인 경로: '프로젝트' → '자원 관리' → 'Management' → 'Logging&Audit' → 'Trail'



| 그림 8.1.2 | Trail 상세 정보 확인

A. 상태 표시: Trail의 상태를 표시합니다.
  - Active: Trail 작동 중
  - Stopped: Trail 작동 중지

B. 시작: 중지된 Trail을 다시 시작합니다.
  - Trail을 재시작을 설정한 날의 활동 내역부터 다시 저장됩니다.

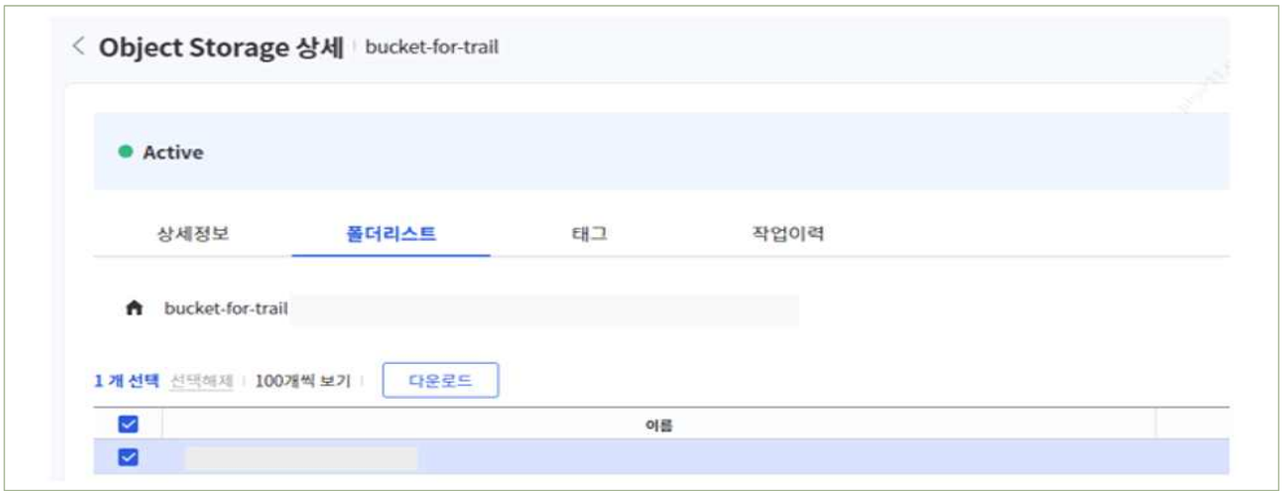
C. 중지: 작동 중인 Trail을 중지합니다. 기존 저장된 활동내역은 유지됩니다.

D. 상세정보: Trail에 대한 기본 정보와 상태, 대상 자원 및 사용자 정보를 확인하고 변경할 수 있습니다.
  - 수정한 내용은 수정한 시점부터 적용되며, 1시간 단위로 저장됩니다.

E. 작업이력: Trail의 작업이력을 확인할 수 있습니다.
  - 검색 영역에 찾고자 하는 검색어를 입력하여 검색할 수 있습니다.
  - '상세검색'을 클릭하여 작업일시, 작업 결과, 경로, 작업자명으로 상세검색할 수 있습니다.

[III. Trail 로그 확인]

- 확인 경로: 프로젝트 → 자원 관리 → Storage → Object Storage



| 그림 8.1.3 | Trail 로그 확인 (Object Storage 폴더리스트 탭)

A. 폴더리스트: Object Storage에서 Trail 로그를 확인할 수 있습니다.

- 월별, 일자별로 디렉토리가 생성되어 Trail 로그를 확인할 수 있습니다.
- 로그 파일은 JSON 또는 CSV 형태로 저장됩니다.
- 이벤트 로그는 1시간 단위로 저장됩니다.

| 그림 8.1.4 | Trail 로그 확인 및 다운로드

B. 다운로드: 다운로드 버튼을 클릭하면 선택한 파일을 다운로드 합니다.

- 다운로드 받은 활동내역 파일은 별도의 파일 편집기를 통해 상세 내역을 확인할 수 있습니다.

4 참고 사항

- 상품별 활동 수집 목록과 위치 적용 범위는 Samsung Cloud Platform 사용자 가이드를 참고하세요.
  (https://cloud.samsungsds.com/manual/ko/scp_user_guide.html#logging_and_audit_list_activities_by_product)
- 로그 파일과 Digest 파일의 검증 방법은 OpenAPI 가이드 또는 CLI 가이드를 참고하세요.
  (https://cloud.samsungsds.com/openapiguide/#/docs/v3-ko-logging_audit-definitions-TrailValidationRequest
  https://cloud.samsungsds.com/openapiguide/#/cli/docs/v3-ko-logging_audit-definitions-TrailValidationRequest)

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

1) 별도 스토리지 백업 기능(객체 잠금 등)을 통해 로그 무결성 보장 등

- Trail을 통해 자원별 활동내역 저장 시 로그파일 검증 기능을 통해 Trail 로그파일의 변경 및 삭제 여부를 검증 가능

  ① Trail: Console과 API 호출을 통해 발생하는 사용자 활동 기록을 Object Storage와 연동하여 장기간 보관할 수 있습니다.

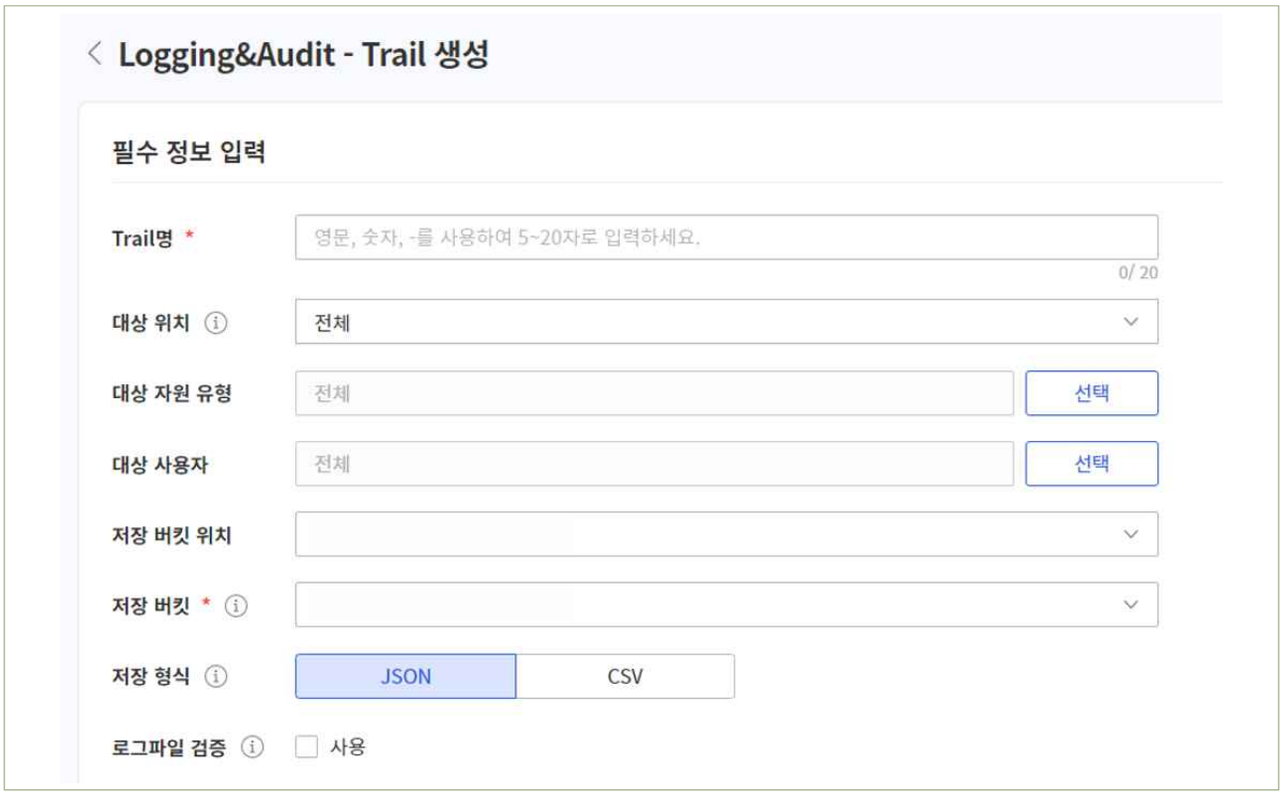
  Ⅰ. Trail 생성

  Ⅱ. Trail 상세 정보 확인

  Ⅲ. Trail 로그 확인

[I. Trail 생성]

- 신청 경로: '프로젝트' → '모든 상품' → 'Management' → 'Logging&Audit' → 'Trail' → Trail 생성



| 그림 8.2.1 | Trail 생성

A. 대상 위치: 활동 이력을 기록할 대상 위치를 선택할 수 있습니다.

B. 대상 자원 유형: 활동 이력을 기록할 대상 상품을 선택할 수 있습니다.

C. 대상 사용자: 활동 이력을 기록할 사용자(계정)를 선택할 수 있습니다.

D. 저장 버킷 위치: Trail의 위치에 해당하는 Object Storage를 선택합니다.

E. 저장 버킷: Trail을 생성할 Object Storage 버킷을 선택합니다.

  · 버킷이 없을 경우 Trail을 생성할 수 없으므로 미리 생성하세요.

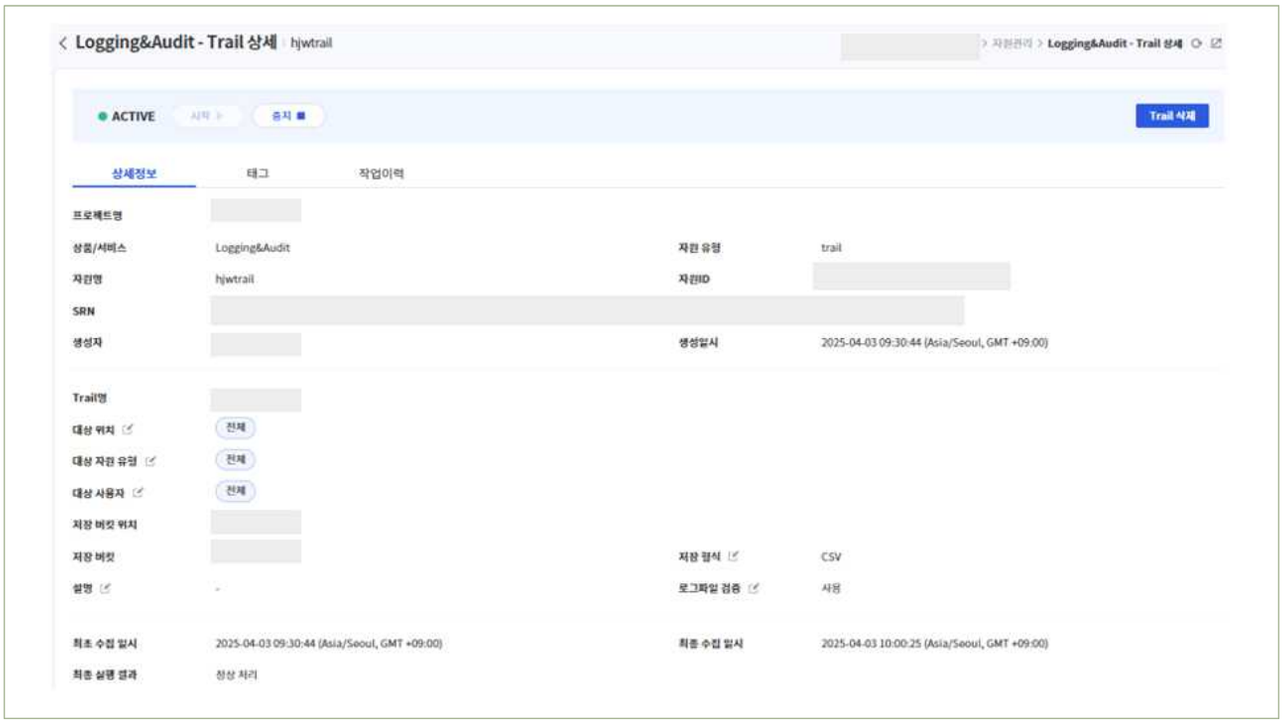
F. 저장 형식: 로그 데이터를 저장하는 파일 포맷을 JSON 또는 CSV 중 선택할 수 있습니다.

G. 로그파일 검증: Trail 로그파일의 변경 및 삭제를 검증하기 위해 동일한 버킷에 Digest 파일을 저장합니다.

  · 로그 파일과 Digest 파일의 검증은 OpenAPI 또는 CLI를 사용하여 가능합니다.

[II. Trail 상세 정보 확인]

- 확인 경로: '프로젝트' → '자원 관리' → 'Management' → 'Logging&Audit' → 'Trail'



| 그림 8.2.2 | Trail 상세 정보 확인

A. 상태 표시: Trail의 상태를 표시합니다.
  - Active: Trail 작동 중
  - Stopped: Trail 작동 중지

B. 시작: 중지된 Trail을 다시 시작합니다.
  - Trail을 재시작 설정일자의 활동 내역부터 다시 저장됩니다.

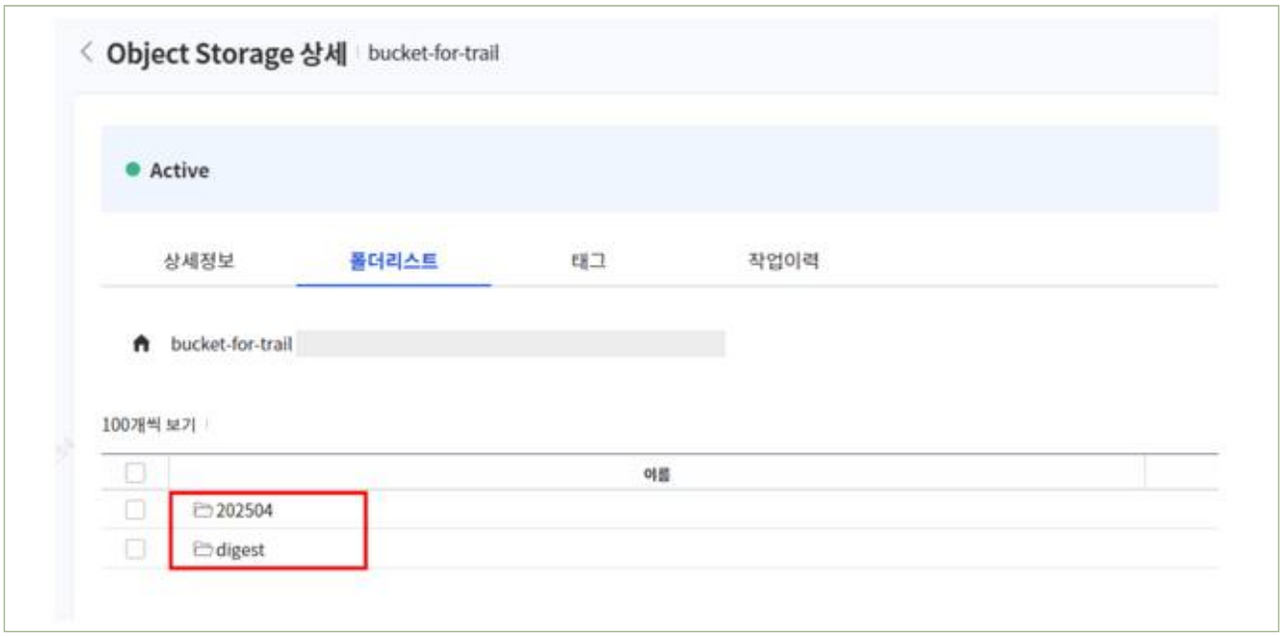
C. 중지: 작동 중인 Trail을 중지합니다. 기존 저장된 활동 내역은 유지됩니다.

D. 상세정보: Trail에 대한 기본 정보와 상태, 대상 자원 및 사용자 정보를 확인하고 변경할 수 있습니다.
  - 수정한 내용은 수정한 시점부터 적용되며, 1시간 단위로 저장됩니다.

E. 작업이력: Trail의 작업이력을 확인할 수 있습니다.
  - 검색 영역에 찾고자 하는 검색어를 입력하여 검색할 수 있습니다.
  - '상세 검색'을 클릭하여 작업 일시, 작업 결과, 경로, 작업자명으로 상세 검색을 할 수 있습니다.

[III. Trail 로그 확인]

- 확인 경로: 프로젝트 → '자원 관리' → 'Storage' → 'Object Storage'



| 그림 8.2.3 | Trail 로그 확인 (Object Storage 폴더리스트 탭)

A. 폴더리스트: Object Storage에서 Trail 로그를 확인할 수 있습니다.
  · 월별, 일자별로 디렉토리가 생성되어 Trail 로그를 확인할 수 있습니다.
  · 로그 파일은 JSON 또는 CSV 형태로 저장됩니다.
  · 이벤트 로그는 1시간 단위로 저장됩니다.

B. 동일한 버킷 내 digest 파일이 저장됩니다.

| 그림 8.2.4 | Trail 로그파일 및 Digest 파일 검증 OpenAPI 가이드

4 참고 사항

- 로그 파일과 Digest 파일의 검증 방법은 OpenAPI 가이드 또는 CLI 가이드를 참고하세요.
  (https://cloud.samsungsds.com/openapiguide/#/docs/v3-ko-logging_audit-definitions-TrailValidationRequest
  https://cloud.samsungsds.com/openapiguide/#/cli/docs/v3-ko-logging_audit-definitions-TrailValidationRequest)

1 기준

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

2 설명

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

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

  - 예시

    1) 클라우드 서비스 제공자(CSP)의 백업 서비스 이용

    2) 전산자료를 별도로 다운받아 금융회사가 관리하는 백업 서버 내 보관 등

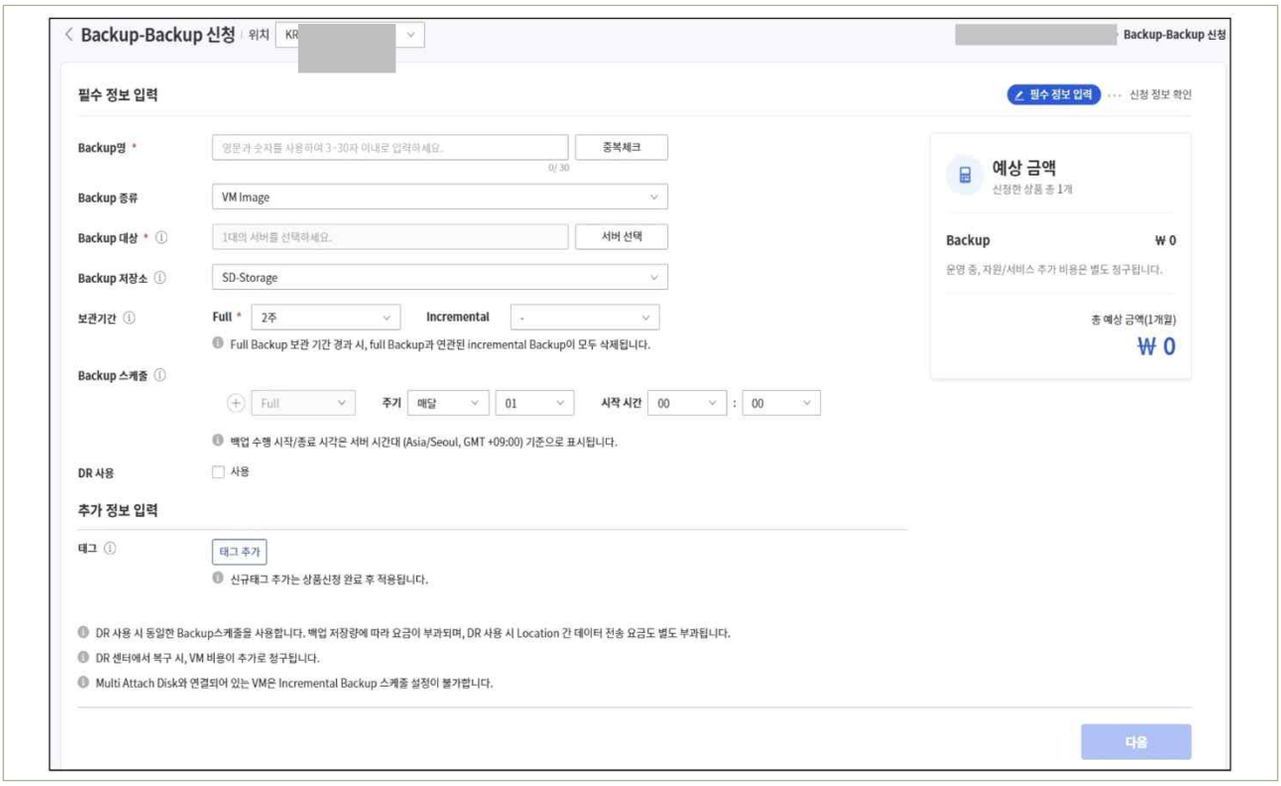
3 우수 사례

1) 데이터를 백업하고 복구하는 백업 서비스 이용

- 기업의 중요한 데이터를 안전한 방식으로 백업하는 Backup 서비스 이용해서, Backup 계획을 수립 및 실행할 수 있으며, 필요 시 Backup파일을 이용해 시스템을 백업할 수 있음.

  ① Backup 신청: Backup 계획을 수립할 수 있습니다.

  - 신청 경로 : ‘모든상품’ → ‘Storage‘ → ‘Backup‘ → ‘Backup’ → ‘상품 신청‘



| 그림 8.3.1 | Backup 신청

A. Backup명: 백업을 식별하기 위한 백업 이름을 입력합니다

B. Backup 종류: 백업 타입을 선택합니다(VM image)

C. Backup 대상: 서버 선택을 클릭한 후 정상 운영 중(Running 상태)인 Virtual Server를 선택합니다.

D. Backup 저장소: 백업을 저장할 장치 유형을 선택합니다

- SD-Storage: Object Storage를 이용한 대용량 시스템 백업

E. 보관기간: Full Backup과 Incremental Backup의 보관기간을 각각 설정합니다.

- Full Backup 보관 기간 경과 시, Full Backup과 연관된 Incremental Backup이 모두 삭제됩니다.
- Incremental 보관 기간은 Full 보관 기간과 같거나 보다 짧게 설정해야 합니다.
- Incremental Backup 사용 시, Full Backup 보관 기간의 권장 설정 기간은 다음과 같습니다.

  (Full 주기가 매 주인 경우: Incremental 보관 기간+1주)

  (Full 주기가 매 달인 경우: Incremental 보관 기간+4주)
- 월 단위는 31일을 기준으로 합니다

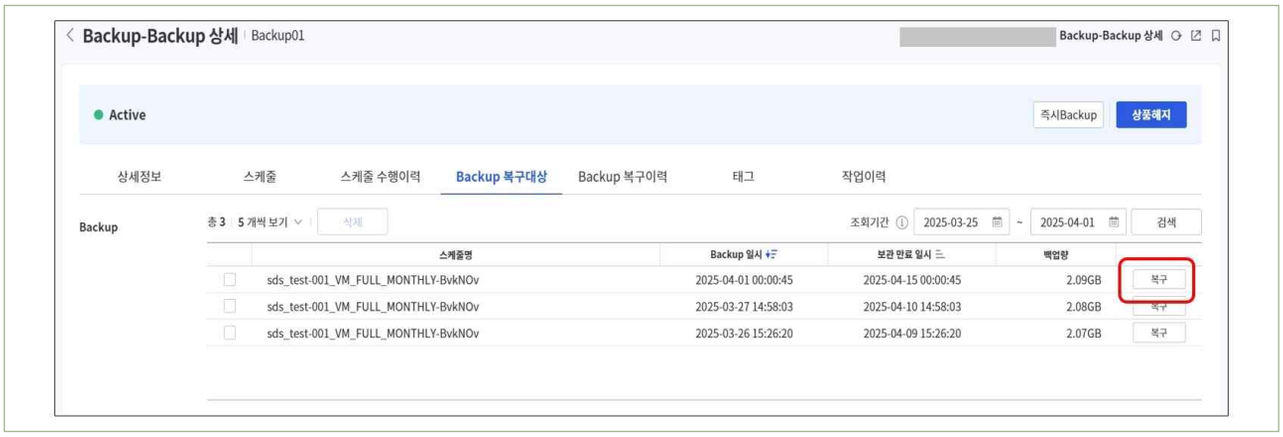
  (2개월-62일, 3개월-93일, 6개월-186일).

F. Backup 스케줄: 백업 유형을 선택한 후, 백업주기와 횟수, 시간을 설정합니다.

- Full: 전체 데이터 백업으로, 시스템 당 1개만 설정할 수 있습니다.
- Incremental: 변동 내용만 백업합니다.
  Full 백업 설정 후 추가할 수 있습니다(최대 6개).
  Multi Attach를 사용 중인 VM의 경우에는 설정할 수 없습니다.
- 백업 주기는 중복해서 설정할 수 없습니다.
- 기준 시간은 한국 표준시(KST)입니다.

② Backup 파일 목록을 확인하고 Backup 파일을 이용하여 시스템을 복구할 수 있습니다.

- 신청 경로 : '모든상품' → 'Storage' → 'Backup' → 'Backup' → '자원관리' → '상세정보' → 'Backup 복구대상'



| 그림 8.3.2 | Backup 상세 (Backup 복구대상)

A. 목록 우측 상단의 기간 영역에 검색할 기간을 설정할 수 있습니다.

B. 조회기간은 일주일로 기본 설정되어 있으며, 최대 조회기간은 한 달입니다.

C. Backup 파일 목록의 '복구'를 클릭하면 해당 Backup 파일을 사용하여 복구 작업을 진행할 수 있는 Popup화면이 조회됩니다.

| 그림 8.3.3 | Backup 복구

- Backup명: 복구하고자 하는 Backup파일명을 조회합니다.
- Backup 대상: Backup대상인 서버명을 조회합니다.
- Backup 일시: Backup을 수행했었던 일시를 조회합니다.
- 복원VM명 : Backup 파일을 이용해 복구 후 사용할 VM (Virtual Server) 이름을 입력 후, '확인' 클릭 시, 복원작업을 수행합니다.

③ 특정기간 동안의 복구 이력을 확인할 수 있습니다.

- 신청 경로 : '모든상품' → 'Storage' → 'Backup' → 'Backup' → '자원관리' → '상세정보' → 'Backup 복구이력'

| 그림 8.3.4 | Backup 상세 (Backup 복구이력)

A. 목록 우측 상단의 기간 영역에 검색할 기간을 설정할 수 있습니다.

B. 조회기간은 일주일로 기본 설정되어 있으며, 최대 조회기간은 한 달입니다.

C. 복구 일시: 복구작업 완료 일정과 시간을 조회합니다

D. Backup 일시: 복구시에 사용했었던 Backup 파일이 작성되었던 일시를 조회합니다

E. 상태: Completed(완료)

F. 복구대상: 복구 완료된(복구 후 사용할) VM (Virtual Server) 이름이 조회됩니다.

2) Database-as-a-Service(DBaaS)의 백업서비스 이용

- 데이터베이스의 전산자료를 정기적으로 오브젝트 스토리지에 백업하고, 복구가능

① DBaaS 백업관리: DB기능 활용백업과 CDP 기반 증분 백업 중 선택하여 진행

Ⅰ. 백업 신청

Ⅱ. 백업설정 변경

Ⅲ. 복구하기

[I. 백업 신청]

- 신청 경로: ‘프로젝트’ → ‘모든 상품’ → ‘Database’ → ‘DBaaS 선택’ → ‘상품 신청’ → 필수 정보 입력
- DBaaS 서비스 목록: EPAS, PostgreSQL, MariaDB, MySQL, Microsoft SQL Server, Tibero (DBaaS에 따라 제공되는 백업 방식과 백업 위치가 상이할 수 있습니다.)
- DB 기능 활용 백업

| 그림 8.3.5 | DB 기능 활용 백업 신청 (DBaaS 신청화면)

A. 백업 사용 선택: 백업 사용을 선택합니다.

B. DB 기능 활용 백업으로 백업 방식 선택: 초기값으로 설정됩니다.

- DB 자체 백업 기능을 활용하여 백업을 수행합니다.
- DB 백업 파일은 백업전용 스토리지에 저장되며, 백업 솔루션, 백업 디바이스 사용료가 포함된 별도의 백업 비용이 발생합니다.
- 백업 파일 보관 기간은 7일부터 35일까지 설정 가능합니다.
- 백업 수행주기는 매일 선택한 시간대에 Full 백업을 수행하며, Incremental 백업을 지원하지 않습니다. 단, 백업이 수행되는 분(minutes)은 Random으로 설정이 되며, 백업 종료 시간은 설정 할 수 없습니다.
- Archive 백업주기는 Archive 파일(데이터 변동분)에 대한 백업주기를 설정합니다. Archive 백업주기는 1시간을 권고하며, 5분/10분/30분 지정 시 DB성능에 영향을 줄 수 있습니다.
- 백업 수행 시작/종료 시각은 서버의 시간대 (Asia/Seoul, GMT +09:00) 기준으로 표시됩니다.

- CDP 기반 증분 백업

| 그림 8.3.6 | CDP 기반 증분 백업 신청 (DBaaS 신청화면)

A. 백업 사용 선택: 백업 사용을 선택합니다.

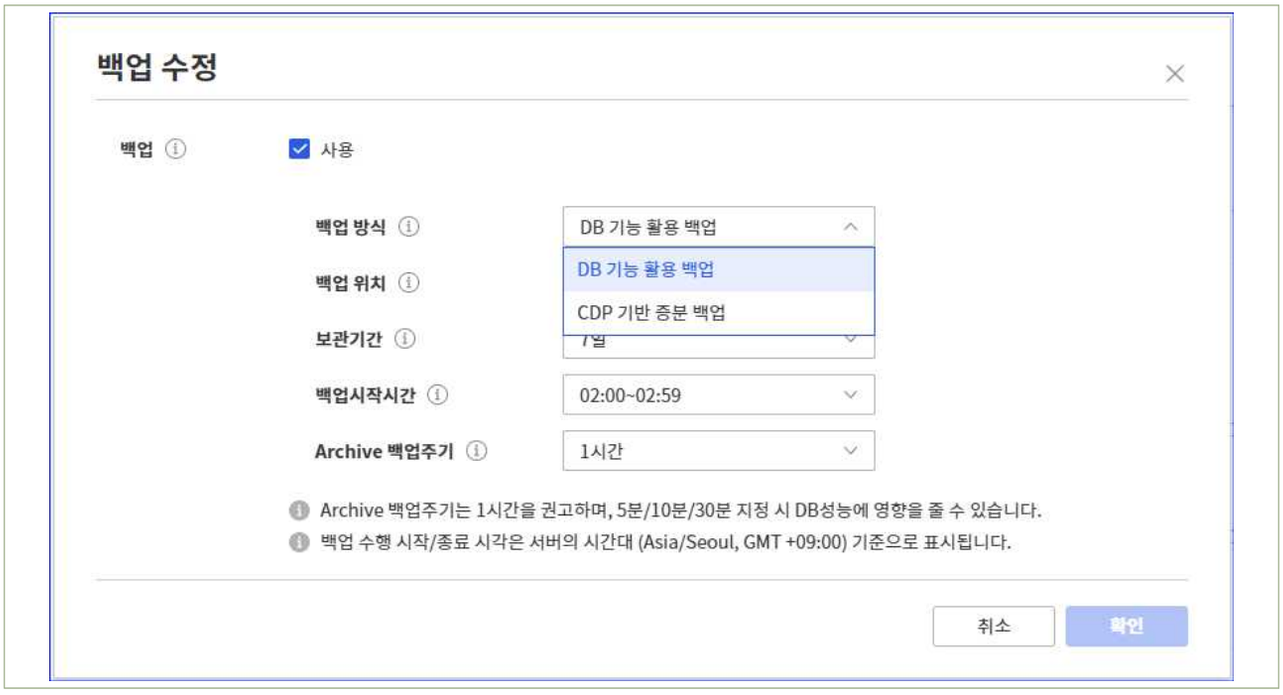
B. CDP 기반 증분 백업으로 백업 방식 선택: 설정값이 변경됩니다.

- CDP 기반 증분 백업은 전문 백업 솔루션의 기능을 활용해 증분(Incremental) 백업을 수행합니다. DB 자체 백업 대비 빠른 백업/복구를 지원하나, Snapshot 특성상 DB 성능이 약 5~9%정도 저하될 수 있습니다.
- DB 백업 파일은 백업전용 스토리지에 저장되며, 백업 솔루션, 백업 디바이스 사용료가 포함된 별도의 백업 비용이 발생합니다.

- Archive 파일은 Object Storage에 저장되며, Storage 사용에 따른 별도 비용이 발생합니다.
- 백업 파일 보관 기간은 7일부터 35일까지 설정 가능합니다.
- 백업 수행주기는 데이터 변경분에 대한 Snapshot이 6시간 / 12시간 단위로 생성됩니다.
- Archive 백업주기는 Archive 파일(데이터 변동분)에 대한 백업주기를 설정합니다. Archive 백업주기는 1시간을 권고하며, 5분/10분/30분 지정 시 DB성능에 영향을 줄 수 있습니다.
  백업 수행 시작/종료 시각은 서버의 시간대 (Asia/Seoul, GMT +09:00) 기준으로 표시됩니다.

[II. 백업설정 변경]

- 신청 경로: 프로젝트 → 모든 상품 → Database → DBaaS 선택 → 자원관리 → 상세 정보 수정
- 백업 수정 팝업창에서 백업 설정을 수정한 후, 확인을 선택(클릭).



| 그림 8.3.7 | 백업설정 변경 (DBaaS 자원관리 화면)

[III. 복구하기]

- 신청 경로: 프로젝트 → 모든 상품 → Database → DBaaS 선택 → 자원관리 → Database 복구 선택
- Database 복구 팝업창에서 복구시점을 선택한 후, 완료를 선택(클릭).

4 참고 사항

- Samsung Cloud Platform 사용자 가이드」에서는 백업 서비스 및 Database-as-a-Service(DBaaS) 상품의 Database 별 백업 가이드가 상세히 소개되어 있음. 더 자세한 내용을 알고 싶으시면 해당 가이드 참조
  (https://cloud.samsungsds.com/manual/ko/scp_user_guide.html#94434a0dc8edee79)
  (https://cloud.samsungsds.com/manual/ko/scp_user_guide.html#02ca2b60bf6f170b)

1 기준

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

2 설명

- 백업을 통해 보관되고 있는 전산자료에 대해 무결성이 보장되어야 한다.

  - 예시

    1) 백업 파일 훼손에 대한 탐지 및 알람 설정

    2) 백업 기능(객체 잠금 등)을 통해 무결성 보장 등

3 우수 사례

1) 백업 파일 훼손에 대한 탐지 및 알람 설정 / 2) 백업 기능(객체 잠금 등)을 통해 무결성 보장 등 : N/A (알람기능 미제공)

- 알람기능 미제공

4 참고 사항

- N/A

1 기준

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

2 설명

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

  - 예시

    1) 백업 작업 로그 저장

    2) 백업대상, 백업주기, 백업담당자 등 정책 수립

    3) 정상적인 백업 수행 여부에 대한 모니터링 등

3 우수 사례

1) 백업 작업 로그 저장

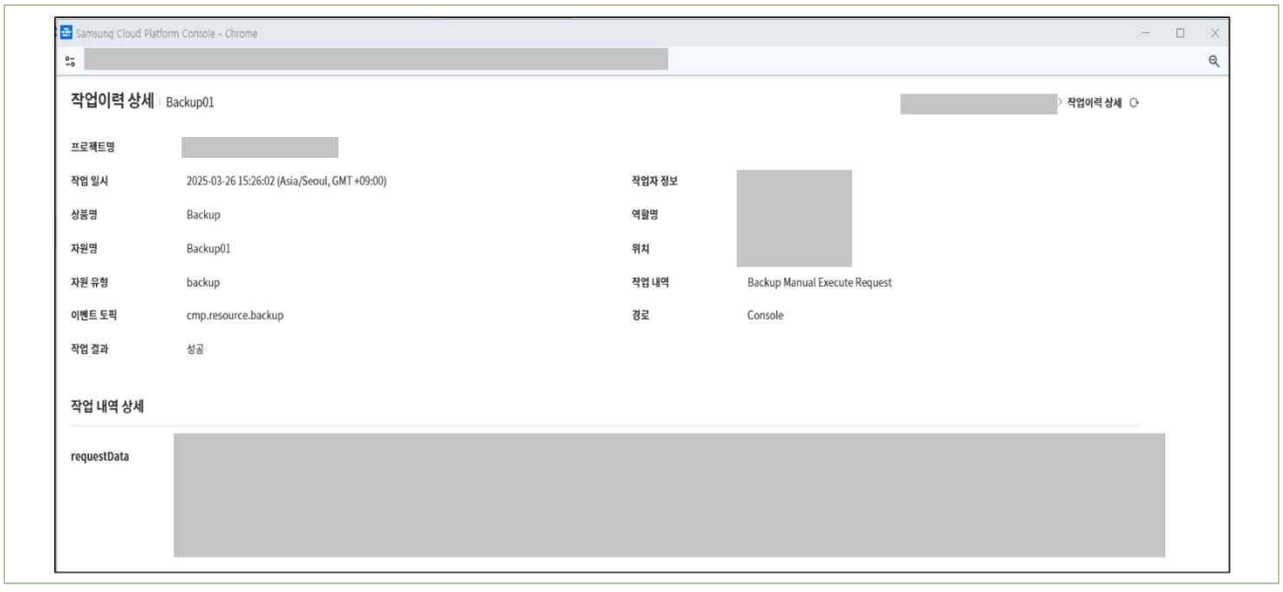
- 백업 관련한 모든 작업(생성, 삭제, 수정 등)에 대해 관련내역을 저장

  ① Backup 관련 모든 작업이력을 저장 및 조회(상세조회)할 수 있습니다.

  - 신청 경로 : '모든상품' → 'Storage' → 'Backup' → 'Backup' → 'Backup 상세' → '작업이력'
  - Backup 관련한 작업이력(생성, 삭제, 수정)과 작업의 상세내용을 조회
  - 검색 영역에 찾고자 하는 검색어를 입력하여 검색할 수 있습니다.
  - 상세검색을 클릭하여 작업 일시, 작업 결과, 경로, 작업자명으로 검색할 수 있습니다

| 그림 8.5.1 | Backup 상세 (작업이력)

A. 작업일시: 해당작업을 수행한 일시가 조회됩니다
B. 자원명: Backup 작업을 수행한 자원명이 조회됩니다.
C. 작업내역: 모든 Backup관련 작업에 대한 내역이 조회됩니다.
(Backup 생성, 삭제, 수정, 복원 등)
D. 작업결과: 해당작업의 결과를 조회합니다.
E. 해당 작업을 클릭하면, 작업이력 상세 Popup 화면에서 상세작업 내역이 조회됩니다.



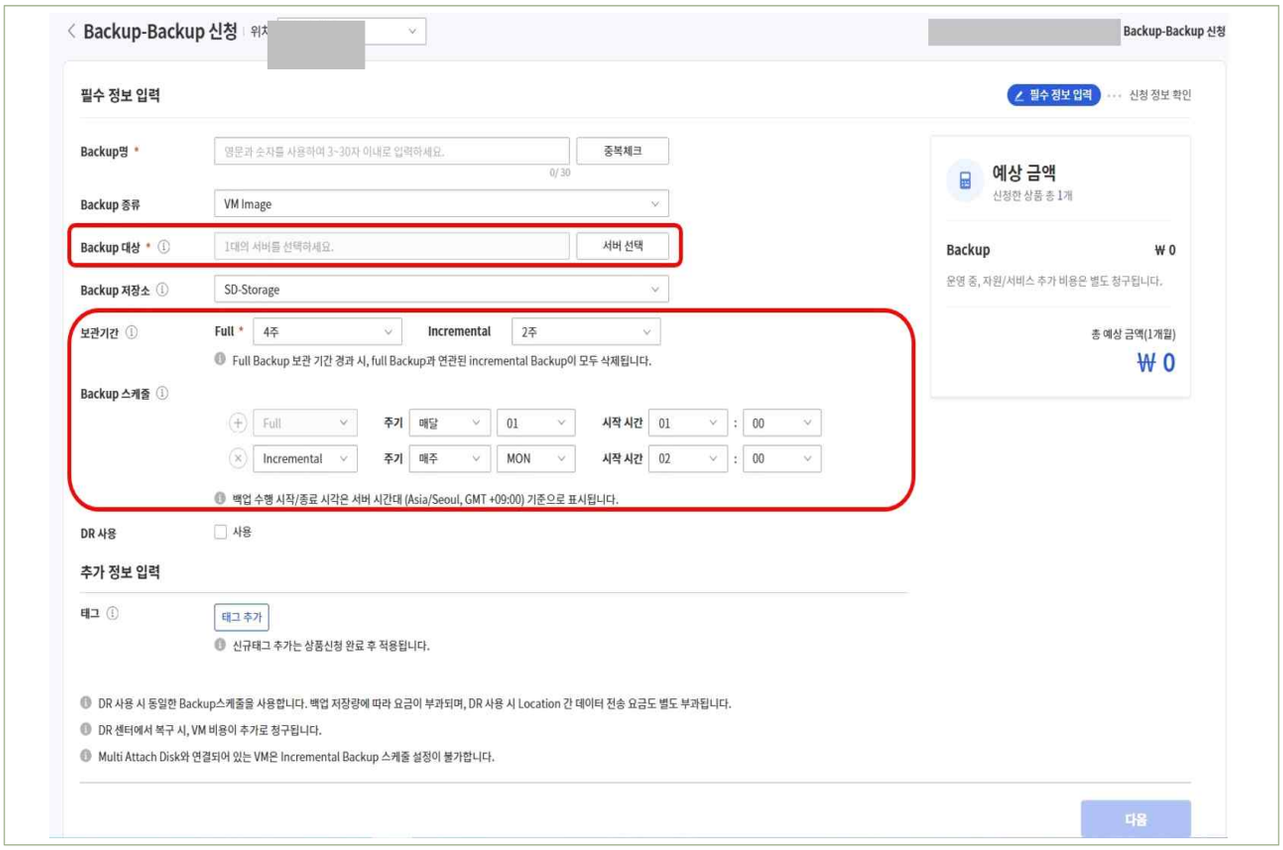
| 그림 8.5.2 | 작업이력 상세

2) 백업대상, 백업주기, 백업담당자 등 정책 수립

- 백업대상, 백업주기 등 백업관련 정책을 생성하고 수정할 수 있음

① Backup 신청 시, 백업대상, 백업주기 등 관련 정책을 생성합니다.

- 신청 경로 : '모든상품' → 'Storage' → 'Backup' → 'Backup' → '상품 신청'



| 그림 8.5.3 | Backup 신청

A. Backup 대상: '서버 선택'을 클릭한 후 정상 운영 중(Running 상태)인 Virtual Server를 선택

| 그림 8.5.4 | Backup 신청 (Backup 대상 선택)

B. 보관기간: Full Backup과 Incremental Backup의 보관기간을 각각 설정합니다.

- Full Backup 보관 기간 경과 시, Full Backup과 연관된 Incremental Backup이 모두 삭제됩니다.
- Incremental 보관 기간은 Full 보관 기간과 같거나 보다 짧게 설정해 합니다.
- Incremental Backup 사용 시, Full Backup 보관 기간의 권장 설정 기간은 다음과 같습니다(예시는 하단 Note 참고).
  (Full 주기가 매 주인 경우: Incremental 보관 기간+1주)
  (Full 주기가 매 달인 경우: Incremental 보관 기간+4주)
- 월 단위는 31일을 기준으로 합니다
  (2개월-62일, 3개월-93일, 6개월-186일).

C. Backup 스케줄: 백업 유형을 선택한 후, 백업 주기와 횟수, 시간을 설정합니다.

- Full: 전체 데이터 백업으로, 시스템 당 1개만 설정할 수 있습니다.
- Incremental: 변동 내용만 백업합니다. Full 백업 설정 후 추가할 수 있습니다(최대 6개). Multi Attach를 사용 중인 VM의 경우에는 설정할 수 없습니다.
- 백업 주기는 중복해서 설정할 수 없습니다.
- 기준 시간은 한국 표준시(KST)입니다.

② Backup 상세 정보에서 Backup 스케줄을 조회하고 수정할 수 있습니다.

- 신청 경로 : '모든상품' → 'Storage' → 'Backup' → 'Backup' → 'Backup 상세' → '스케줄

| 그림 8.5.5 | Backup 상세 (스케줄)

A. 스케줄명: 스케줄 이름을 조회합니다.

B. Backup 구분 : Full/Incremental 구분을 조회합니다.

C. 주기 : 매달/매주/일간격 구분을 조회합니다.

D. 주기일정 : 주기에 따른 상세일정을 조회합니다.

- 매달(1~31), 매주(MON~SUN), 일간격((1~100일중 선택)

E. ‘스케줄 변경’을 클릭하여 스케줄을 추가하거나 변경할 수 있습니다.

| 그림 8.5.6 | Backup 스케줄 변경

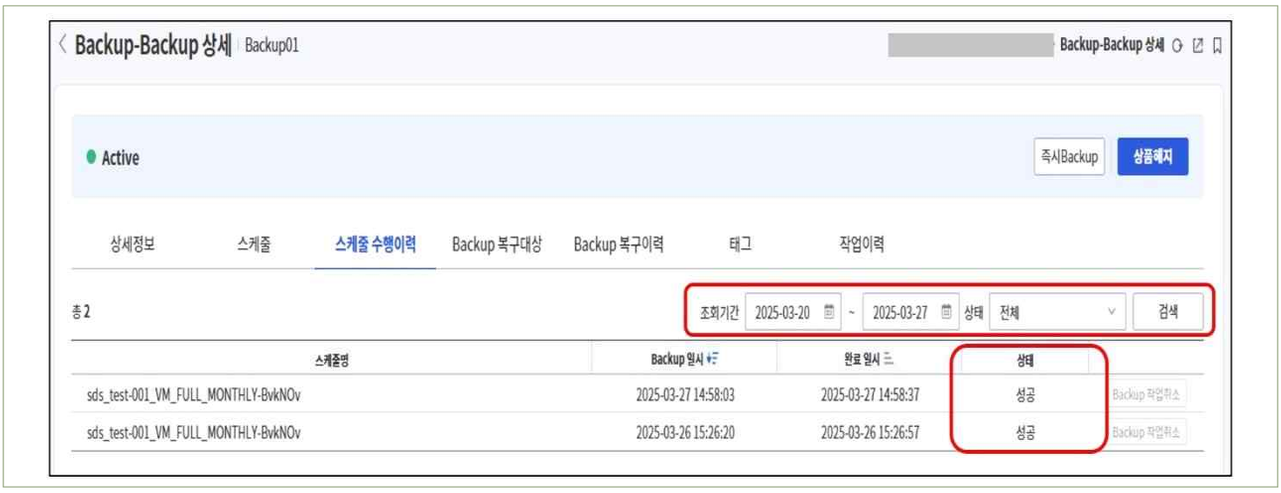
- 스케줄을 추가하려면 ‘+’ 클릭한 후 백업 유형과 주기, 그리고 시작 시간을 설정합니다.
- 스케줄을 삭제하려면 스케줄 옆에 있는 ‘X’를 클릭합니다.
- 백업 방식: 백업 방식을 설정합니다. 최대 6개까지 추가할 수 있습니다.
  (Full: 전체 데이터를 백업합니다. 시스템 당 1개만 설정할 수 있습니다.)
  (Incremental: 변동 내용만 백업합니다. Full 백업을 설정한 후, 추가가능.)
- 주기: 백업 주기를 설정합니다. 백업 주기는 중복하여 설정할 수 없습니다.
- 시작시간: 백업을 시작하는 시간을 설정합니다. 30분 단위로 선택할 수 있습니다.

3) 정상적인 백업 수행 여부에 대한 모니터링 등

- 특정 기간 동안의 백업 스케줄 수행 여부를 모니터링 할 수 있음

① 스케줄 수행이력을 통해 수행여부 및 상태(성공, 실패, 진행 중)를 확인할 수 있습니다.

- 신청 경로 : ‘모든상품’ → ‘Storage‘ → ‘Backup‘ → ‘Backup’ → ‘Backup 상세‘ → ‘스케줄 수행이력’



| 그림 8.5.7 | Backup 상세 (스케줄 수행이력)

A. 조회기간: 기간 영역에 검색할 기간을 설정합니다.

B. 상태: 백업 상태(성공, 부분성공, 실패, 진행 중)로 상세 검색할 수 있습니다.

C. ‘상태’로 정상적인 백업 수행 여부에 대한 모니터링 가능합니다.

4 참고 사항

- Samsung Cloud Platform 사용자 가이드」에서는 백업 자료 관리(생성/변경/삭제 등) 관련 내역을 기록하고 관리하는 활용 가이드가 소개되어 있음.
- 더 자세한 내용을 알고 싶으시면 해당 가이드 참조 (https://cloud.samsungsds.com/manual/ko/scp_user_guide.html#94434a0dc8edee79)

1 기준

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

2 설명

- 중요한 금융회사 전산자료는 보안이 강화된 원격 저장소에 보관하여야 한다.
  - 예시.
  1) 클라우드 서비스 제공자(CSP)의 DR 서비스 이용
  2) 금융회사 자체 데이터센터로 소산하여 보관 등

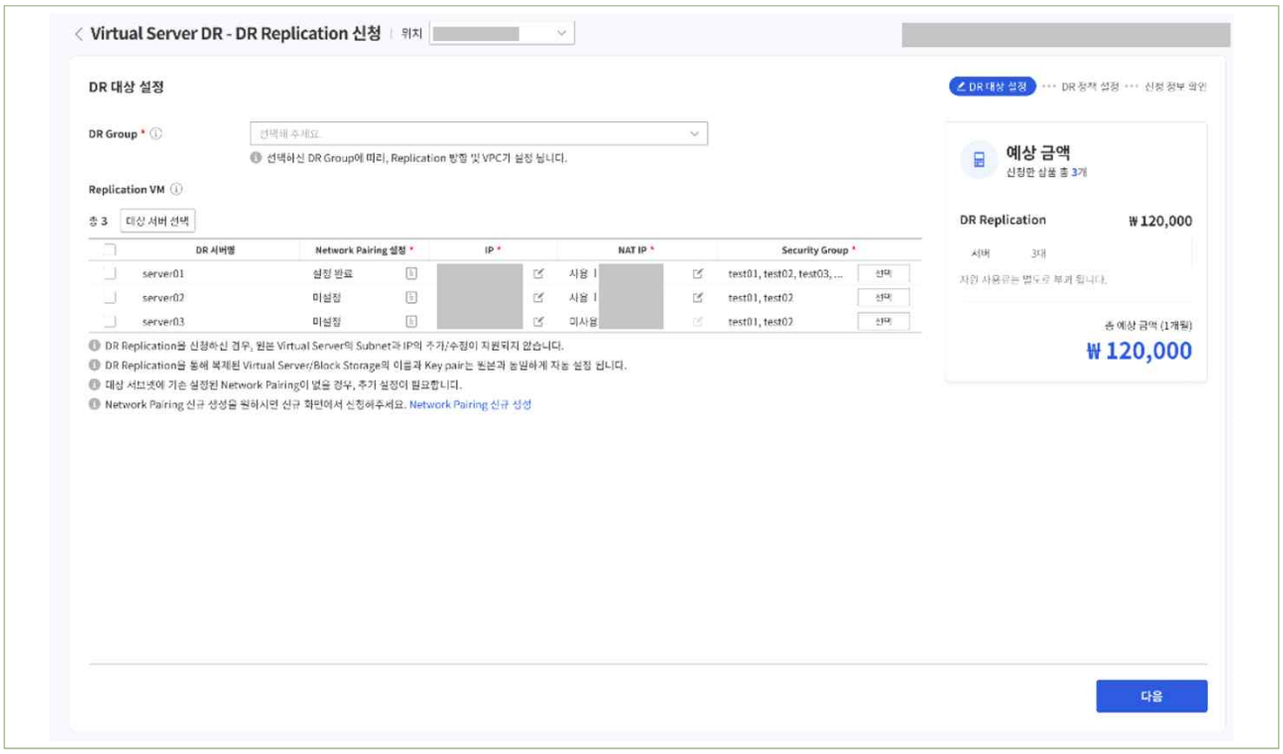
3 우수 사례

1) Virtual Server DR 서비스 이용

- Virtual Server DR은 현재 사용중인 위치와 다른 리전에 Virtual Server 및 연결된 Block Storage를 복제하고, 재해 상황을 대비한 계획 수립 및 테스트, 그리고 재해 상황 발생 시 실제 복구 가능.
  ① DR Replication: DR Replication을 생성하여 다른 위치(Region)에 있는 Virtual Server를 복제하고 동기화할 수 있습니다.
  Ⅰ. DR Replication 신청
  Ⅱ. DR Replication 상세 정보 확인
  Ⅲ. DR Replication 삭제

[I. DR Replication 신청]

- 신청 경로: 프로젝트 → 모든 상품 → Compute → Virtual Server DR → DR Replication → 상품 신청



| 그림 8.6.1 | DR Replication 신청 (DR 대상 설정)

A. DR Group: Replication VM을 적용할 DR Group을 선택합니다.
  - 원하는 DR Group이 없을 경우, 새로 생성할 수 있습니다.

B. 대상 서버 선택: 복제할 Virtual Server를 선택하세요.
  - DR 적용 중이거나 Block Storage의 Multi-attach가 연결된 Virtual Server는 선택할 수 없습니다.
  - 원본 Virtual Server에 연결된 Block Storage의 암호화 사용 여부가 서로 다를 경우, DR Replication을 생성할 수 없습니다.
  - DR Replication을 신청한 원본 Virtual Server에는 Block Storage를 추가할 수 없습니다. 필요한 경우, DR Replication을 해지하고 Block Storage를 추가하세요.

C. DR 서버명: 복제할 Virtual Server의 이름이 표시됩니다.
  - 대상 서버 선택을 클릭하여 복제할 Virtual Server를 선택합니다.
  - 대상 서버는 10개까지 선택할 수 있습니다.

D. Network Pairing 설정 상태가 표시됩니다

- 오른쪽 아이콘을 클릭하여 원본 네트워크와 DR 네트워크의 VPC, 서브넷 정보를 확인할 수 있습니다.

E. IP: 편집 버튼을 클릭하여 IP 정보를 설정합니다.
- 자동 생성, 원본 VM과 동일, 입력을 선택할 수 있습니다.
- 입력을 선택하면 IP를 직접 입력할 수 있습니다.

F. NAT IP: 편집 버튼을 클릭하여 NAT IP의 사용 여부를 설정합니다.
- 사용으로 설정한 경우, 자동 생성을 선택하거나 Reserved IP 목록에서 선택할 수 있습니다.

G. Security Group: 복제할 Virtual Server에 적용할 Security Group을 선택합니다.
- 선택을 클릭하여 적용할 Security Group을 선택합니다.

H. 예상 금액: 선택한 구성에 대한 예상 금액을 표시합니다.

| 그림 8.6.2 | DR Replication 신청 (DR 정책 설정)

A. DR위치: DR Group에서 설정한 DR 위치가 표시됩니다.

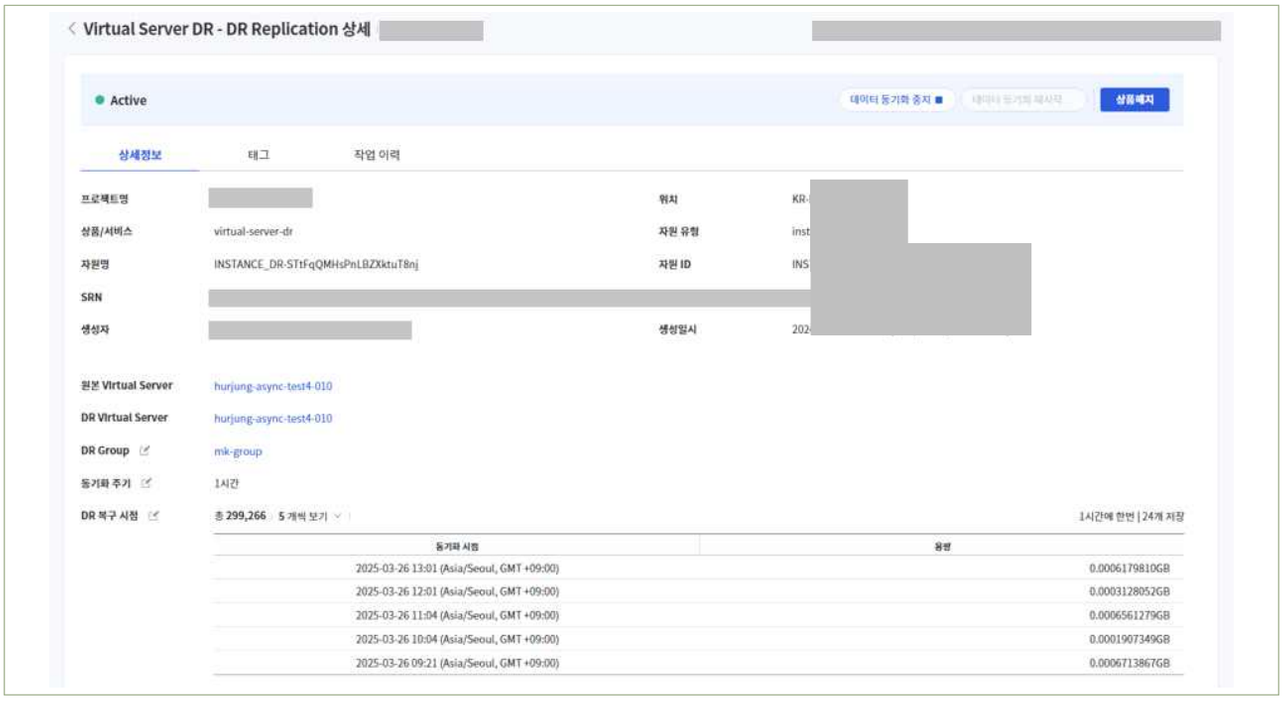
B. 동기화 주기: 동기화 주기를 설정합니다
- 최소 5분, 최대 24시간 까지 설정할 수 있습니다.

C. DR 복구 시점: DR 복구 시점 사용 시 데이터 저장 주기와 저장 수량을 설정할 수 있습니다.
- 데이터 저장 주기: 최소 1시간, 최대 24시간까지 설정할 수 있으며, 동기화 주기보다 짧게 설정할 수 없습니다.

· 데이터 저장 수량: 최소 1개, 최대 24개까지 설정할 수 있습니다.

[II. DR Replication 상세 정보 확인]

– 확인 경로: 프로젝트 → 자원 관리 → Compute → Virtual Server DR → DR Replication



| 그림 8.6.3 | DR Replication 상세 정보 확인

A. 상태 표시: DR Replication의 상태를 표시합니다.

· Creating: DR Replication을 생성 중입니다.

· Active: DR Replication에 포함된 서버가 모두 정상적으로 운영 중입니다.

· Editing: DR Replication의 정보를 수정 중입니다.

· Deleting: DR Replication을 삭제 중입니다.

· Sync Error, RPO Error: 데이터 동기화가 목표한 시간 내에 진행되지 않았습니다. 동기화 주기를 변경하거나 원본 Virtual Server의 용량을 확인하세요.

B. 데이터 동기화 중지: 원본 서버와 DR Replication의 데이터 동기화를 중지합니다.

C. 데이터 동기화 재시작: 원본 서버와 DR Replication의 데이터 동기화를 시작합니다.

D. 상품 해지: DR Replication을 해지할 수 있습니다.

E. 상세정보: DR Replication에 대한 기본 정보와 상태, 소속된 자원 정보를 확인하고 변경할 수 있습니다.

· 프로젝트 및 상품 정보: 프로젝트 이름, 위치, 생성 일시, 수정 일시 등, 프로젝트에 대한

기본적인 정보를 표시합니다.

- Virtual Server 정보: 원본 Virtual Server와 DR Virtual Server 이름이 표시됩니다. 이름을 클릭하면 해당하는 Virtual Server의 상세 페이지로 이동합니다.
- DR Group: DR Replication이 적용된 DR Group 이름이 표시됩니다.
- 동기화 주기: DR Replication의 동기화 주기가 표시됩니다.
- DR 복구 시점: DR 복구 시점에 설정된 주기에 따라 진행한 동기화 현황이 표시됩니다.

[III. DR Replication 삭제하기]

- 신청 경로: '프로젝트' → '자원 관리' → 'Compute' → 'Virtual Server DR' → 'DR Replication' → '상품 해지'

② Virtual Server DR Recovery Plan: DR을 사용하여 모의 훈련이나 재해 복구를 진행하거나 관련 계획을 생성하여 관리할 수 있습니다.

Ⅰ. DR Recovery Plan 생성

Ⅱ. DR Recovery Plan 상세 정보 확인

Ⅲ. DR 모의 훈련 수행

- 모의 훈련 시작
- 모의 훈련용 자원 정리

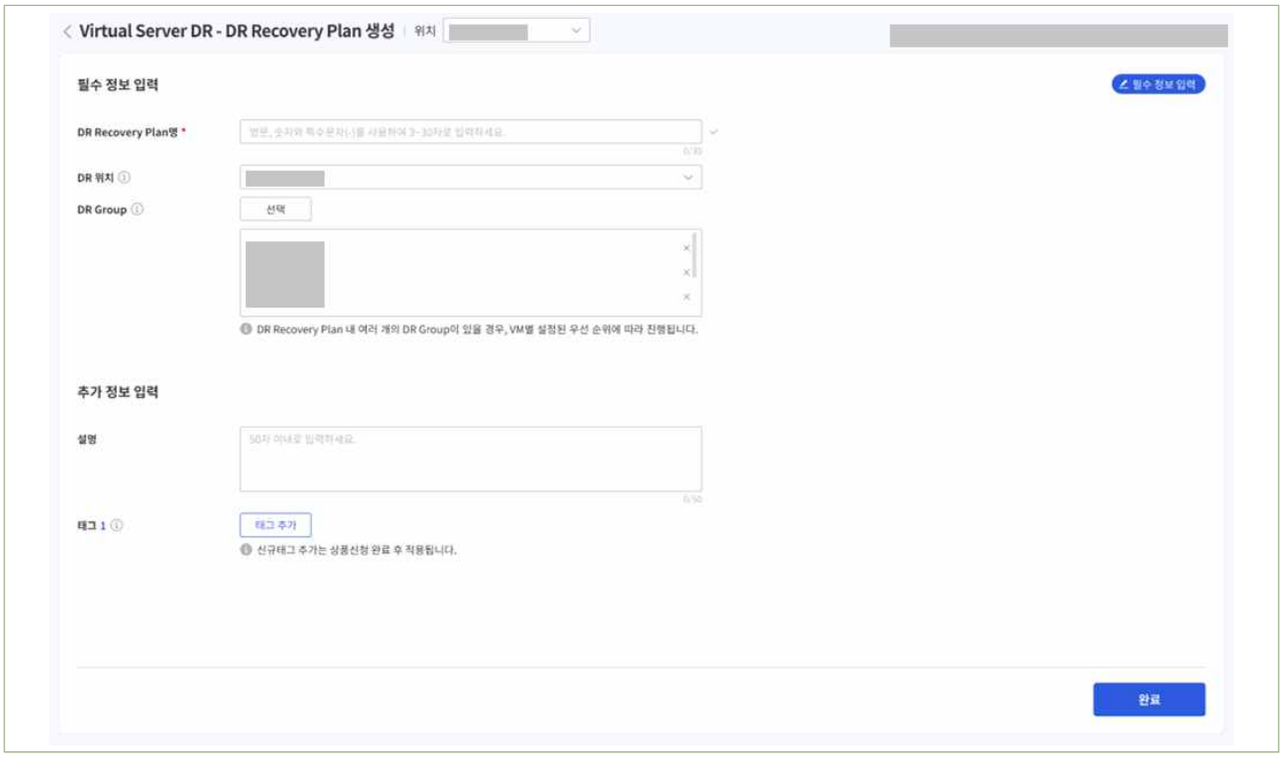
Ⅳ. 재해 복구 수행

- 재해 복구 시작
- 재해 복구 완료

Ⅴ. DR Recovery Plan 삭제

[I. DR Recovery Plan 생성]

- 신청 경로: '프로젝트' → '모든 상품' → 'Compute' → 'Virtual Server DR' → 'DR Recovery Plan' → 'Plan 생성'



| 그림 8.6.4 | DR Recovery Plan 생성

A. DR Recovery Plan명: DR Recovery Plan의 이름을 입력합니다.

B. DR 위치: DR Recovery Plan을 실행할 DR의 위치를 선택합니다.

C. DR Group: DR Recovery Plan으로 실행할 DR Group을 선택합니다.

- 여러 개의 DR Group을 선택할 수 있습니다.

D. 설명: DR Recovery Plan에 대한 설명을 입력합니다.

E. 태그: 태그 정보를 입력합니다.

[II. DR Recovery Plan 상세 정보 확인]

- 확인 경로: '프로젝트' → '자원 관리' → 'Compute' → 'Virtual Server DR' → 'DR Recovery Plan'

| 그림 8.6.5 | DR Recovery Plan 상세 확인

A. 상태 표시: DR Recovery Plan의 상태를 표시합니다.

- Creating: DR Recovery Plan을 생성 중입니다.

- Active: DR Recovery Plan이 포함된 서버가 모두 정상적으로 운영 중입니다.
- Editing: DR Recovery Plan의 정보를 수정 중입니다.
- Deleting: DR Recovery Plan을 삭제 중입니다.

B. 모의 훈련 수행: DR Group 내 Virtual Server의 복구 우선 순위를 설정하고 모의 복구 훈련을 수행할 수 있습니다.

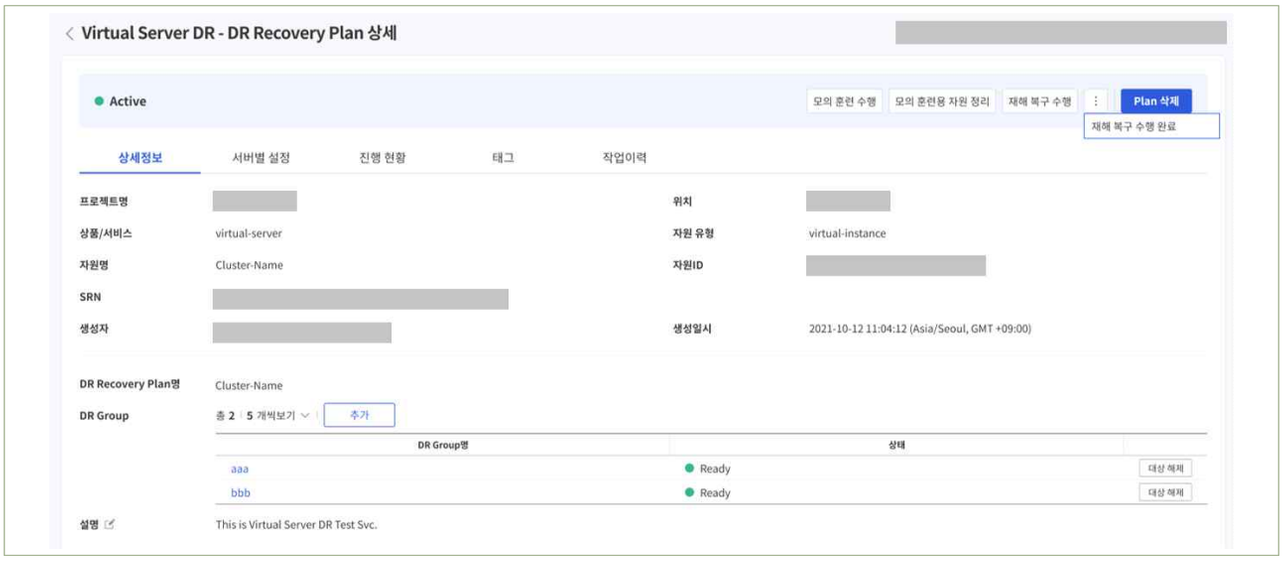
C. 모의 훈련용 자원 정리: 모의 훈련을 종료하고 DR 위치의 Virtual Server를 끌 수 있습니다.

D. 재해 복구 수행: DR Group 내 Virtual Server의 복구 우선 순위를 설정하고 재해 복구를 수행할 수 있습니다.

E. 재해 복구 수행 완료: 재해 복구를 완료하고 서비스를 정상 운영할 수 있습니다.

- 재해 복구를 완료하면 해당 하는 DR Recovery Plan과 Snapshot은 삭제됩니다.

F. Plan 삭제: DR Recovery Plan을 삭제할 수 있습니다.



| 그림 8.6.6 | DR Recovery Plan 상세 확인 (상세 정보 탭)

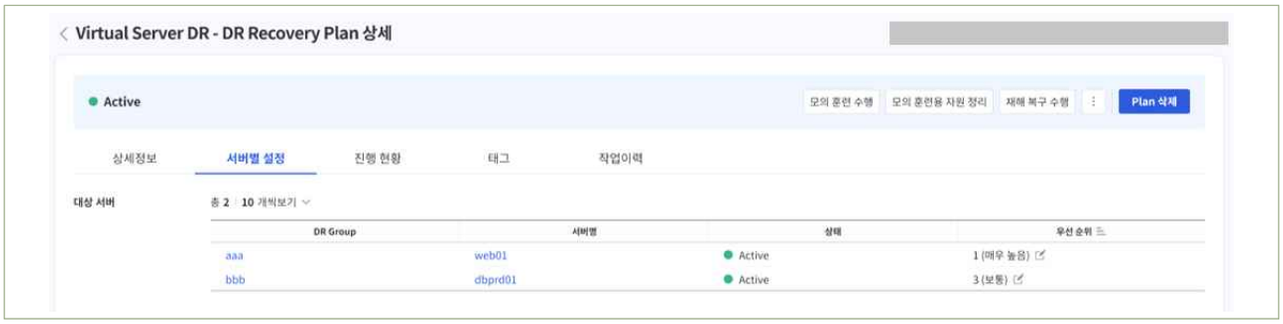
A. 상세정보: DR Recovery Plan에 대한 기본 정보와 상태, 소속된 자원 정보를 확인하고 변경할 수 있습니다.

B. 프로젝트 및 상품 정보: 프로젝트 이름, 위치, 생성 일시, 수정 일시 등, 프로젝트에 대한 기본적인 정보를 표시합니다.

C. DR Recovery Plan명: DR Recovery Plan의 이름이 표시됩니다.

D. DR Group: DR Recovery Plan이 적용된 DR Group 목록이 표시됩니다.

- 추가를 클릭하여 DR Group를 추가할 수 있습니다.
- 대상 해제를 클릭하면 해당 DR Group을 DR Recovery Plan에서 제외할 수 있습니다.



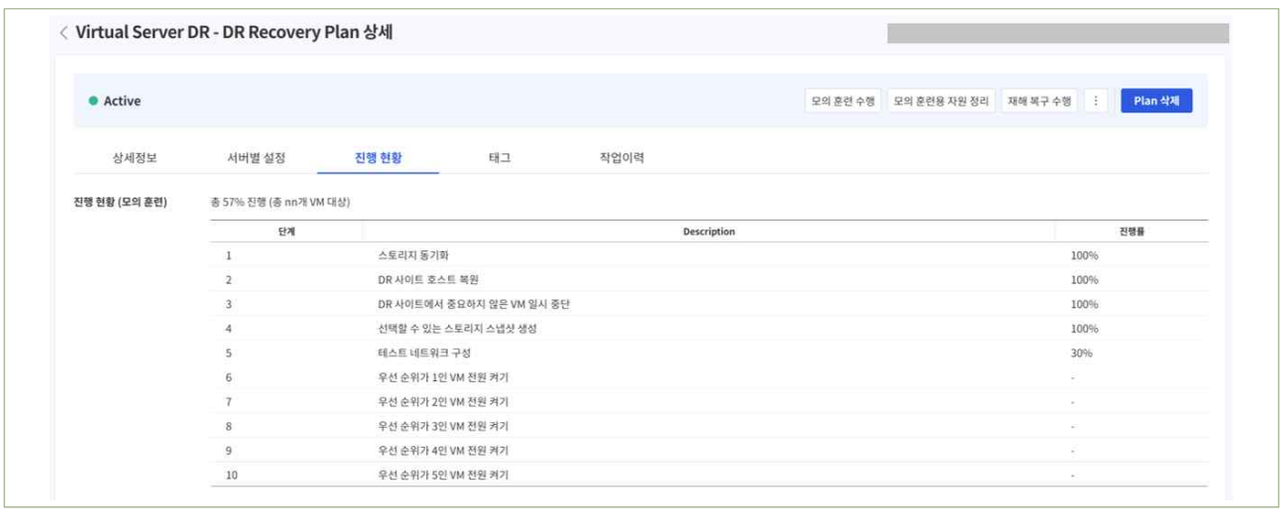
| 그림 8.6.7 | DR Recovery Plan 상세 확인 (서버별 설정 탭)

A. 서버별 설정: DR Recovery Plan이 적용된 DR Group 정보와 DR Replication 자원의 복구 현황이 표시됩니다.

B. 상태: 표시되는 DR Replication 자원 복구 현황은 다음과 같습니다.

- Active: DR Replication 정상 수행 중
- Tested: 모의 훈련 수행 완료
- Recovered: 재해 복구 수행 완료
- Completed: 재해 복구 수행 후, 재해 복구 수행 완료를 클릭하여 완료 신청

C. 우선순위: 우선 순위에 있는 버튼을 클릭하여, 해당 서버의 복구 우선 순위를 변경할 수 있습니다.



| 그림 8.6.8 | DR Recovery Plan 상세 확인 (진행 현황 탭)

A. 진행 현황: 모의 훈련이나 재해 복구 시 진행 현황을 확인할 수 있습니다.

- 진행 현황 표시는 1분 단위로 변경됩니다.
- 복구 작업의 종류(모의 훈련, 모의 훈련용 자원 정리, 재해 복구)에 따라 단계가 다르게 표시됩니다.

[III. DR 모의 훈련 수행 – 모의 훈련 수행]

- 신청 경로: ‘프로젝트’ → ‘모든 상품’ → ‘Compute’ → ‘Virtual Server DR’ → ‘DR Recovery Plan’ → 모의 훈련 수행

| 그림 8.6.9 | 모의 훈련 수행

A. 우선 순위: 모의 훈련 진행 시 복구 우선 순위를 설정합니다.

B. DR 복구 시점: DR 복구 시점을 설정합니다.

C. 모의 훈련 진행 현황은 해당 Recovery Plan의 상세 페이지의 진행 현황 탭에서 확인할 수 있습니다.

[III. DR 모의 훈련 수행 – 모의 훈련용 자원 정리]

- 신청 경로: 프로젝트 → 모든 상품 → Compute → Virtual Server DR → DR Recovery Plan → 모의 훈련용 자원 정리

| 그림 8.6.10 | 모의 훈련용 자원 정리

A. 모의 훈련용 자원 정리 진행 현황은 해당 Recovery Plan의 상세 페이지의 진행 현황 탭에서 확인할 수 있습니다.

B. 모의 훈련이 끝나면 DR 위치의 Virtual Server가 Off 상태로 전환됩니다.

[IV. 재해 복구 수행 – 재해 복구 수행]

- 신청 경로: 프로젝트 → 모든 상품 → Compute → Virtual Server DR → DR Recovery Plan → 재해 복구 수행

| 그림 8.6.11 | 재해 복구 시작

A. 우선 순위: 복구 우선 순위를 설정합니다.

B. DR 복구 시점: DR 복구 시점을 설정합니다.

C. 재해 복구 진행 현황은 해당 Recovery Plan의 상세 페이지의 진행 현황 탭에서 확인할 수 있습니다.

[IV. 재해 복구 수행 – 재해 복구 완료]

- 신청 경로: 프로젝트 → 모든 상품 → Compute → Virtual Server DR → DR Recovery Plan → 재해 복구 수행 완료

| 그림 8.6.12 | 재해 복구 완료

A. 재해 복구를 완료하면 해당 하는 DR Recovery Plan과 Snapshot은 삭제됩니다.

B. 원본 위치의 VPC와 서브넷은 해당 페이지에서 직접 삭제해야 합니다.

[V. DR Recovery Plan 삭제]

- 신청 경로: 프로젝트 → 모든 상품 → Compute → Virtual Server DR → DR Recovery Plan → Plan 삭제

| 그림 8.6.13 | DR Recovery Plan 삭제

③ DR Group: DR 대상 서버의 용도, 위치, VPC 등을 기준으로 그룹화하여 관리할 수 있습니다.

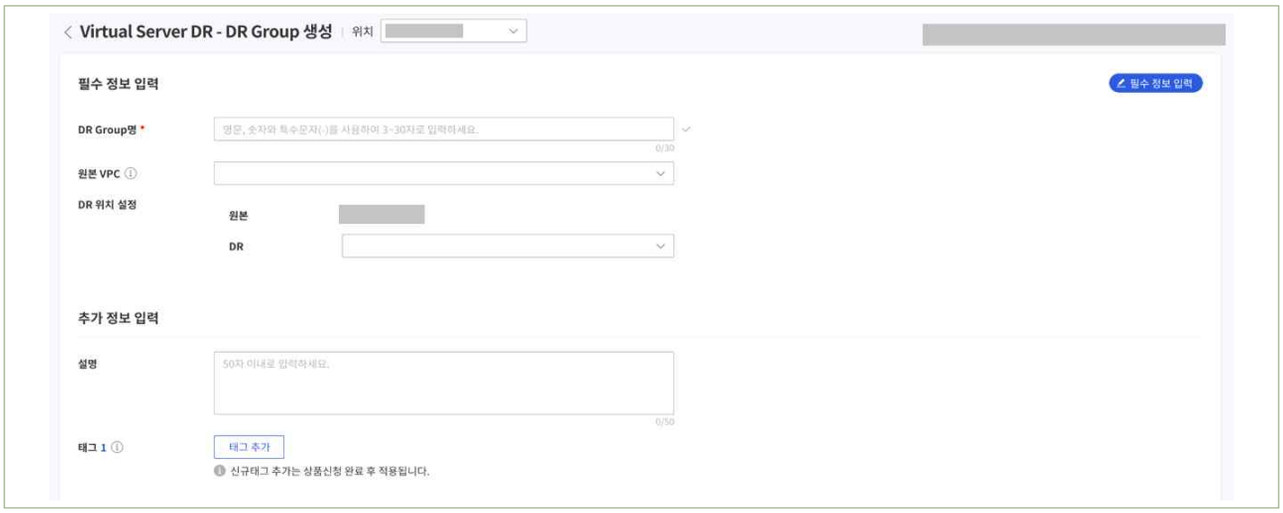
Ⅰ. DR Group 생성

Ⅱ. DR Group 상세 정보 확인

Ⅲ. DR Group 삭제

[I. DR Group 생성]

- 신청 경로: 프로젝트 → 모든 상품 → Compute → Virtual Server DR → DR Group → DR Group 생성



| 그림 8.6.14 | DR Group 생성

A. DR Group명: DR Group의 이름을 입력합니다.

B. 원본 VPC: DR Group에 포함할 Virtual Server의 원본 VPC를 선택합니다.

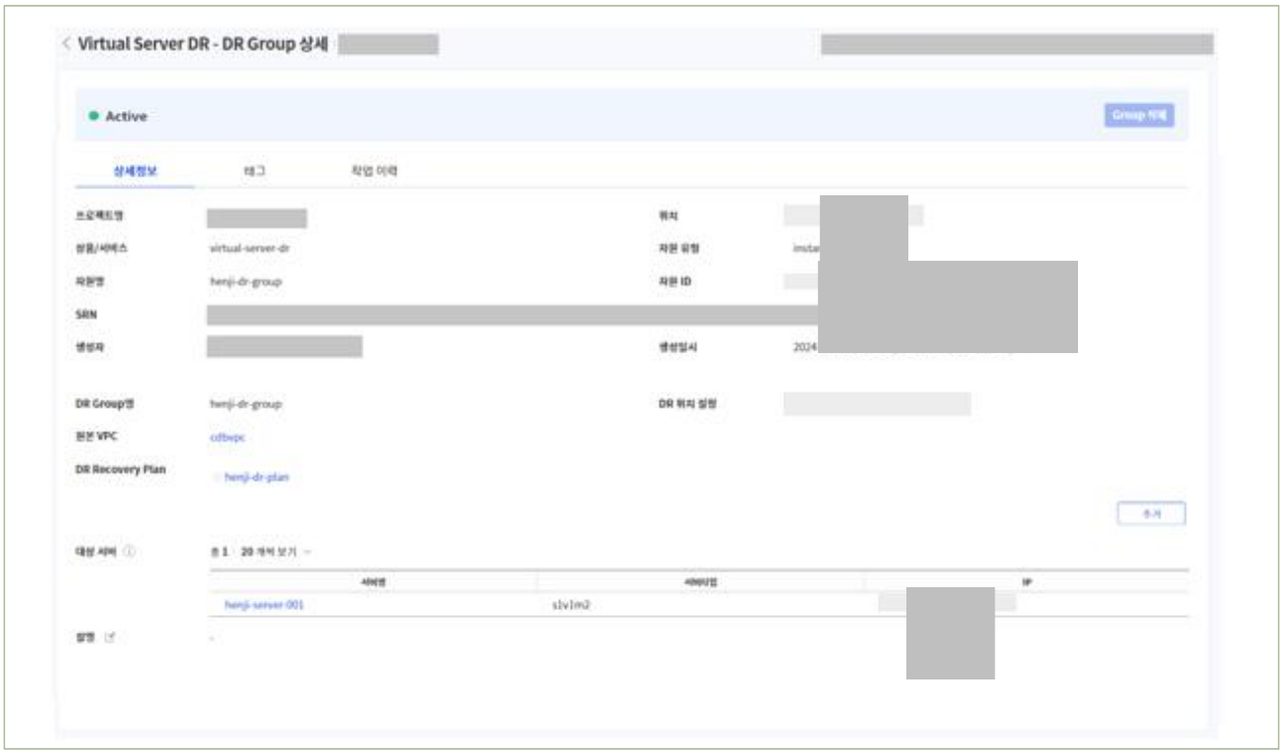
C. DR 위치 설정: DR 위치를 설정합니다.

D. 설명: DR Group에 대한 설명을 입력합니다.

E. 태그: 태그 정보를 입력합니다.

[II. DR Group 상세 정보 확인]

- 확인 경로: 자원관리 → 모든 상품 → Compute → Virtual Server DR → DR Group



| 그림 8.6.15 | DR Group 상세 정보 확인

A. 상태 표시: DR Group의 상태를 표시합니다.
  - Creating: DR Group을 생성 중입니다.
  - Active: DR Group에 포함된 서버가 모두 정상적으로 운영 중입니다.
  - Editing: DR Group의 정보를 수정 중입니다.

B. Group 삭제: DR Group을 삭제할 수 있습니다.

C. 프로젝트 및 상품 정보: 프로젝트 이름, 위치, 생성 일시, 수정 일시 등, 프로젝트에 대한 기본적인 정보를 표시합니다.

D. DR Group 정보: DR Group에 대한 기본 정보가 표시됩니다.

E. DR Recovery Plan: DR Group이 포함된 Recovery Plan 목록이 표시됩니다.
  - Recovery Plan 이름 옆의 X 클릭하여 목록에서 삭제할 수 있습니다.
  - 추가를 클릭하여 Recovery Plan을 추가할 수 있습니다. 하나의 DR Group에 여러 개의 Recovery Plan을 추가할 수 있습니다.

F. 대상 서버: DR Group에 포함된 서버 목록이 표시됩니다.
  - DR Replication 상세 정보 페이지에서 대상 서버를 추가하거나 삭제할 수 있습니다.

[III. DR Group 삭제]

- 신청 경로: 자원관리 → 모든 상품 → Compute → Virtual Server DR → DR Group → Group 삭제

③ Network Pairing: 원본 서버와 DR 서버의 서브넷 관계를 미리 설정하여 관리할 수 있습니다.

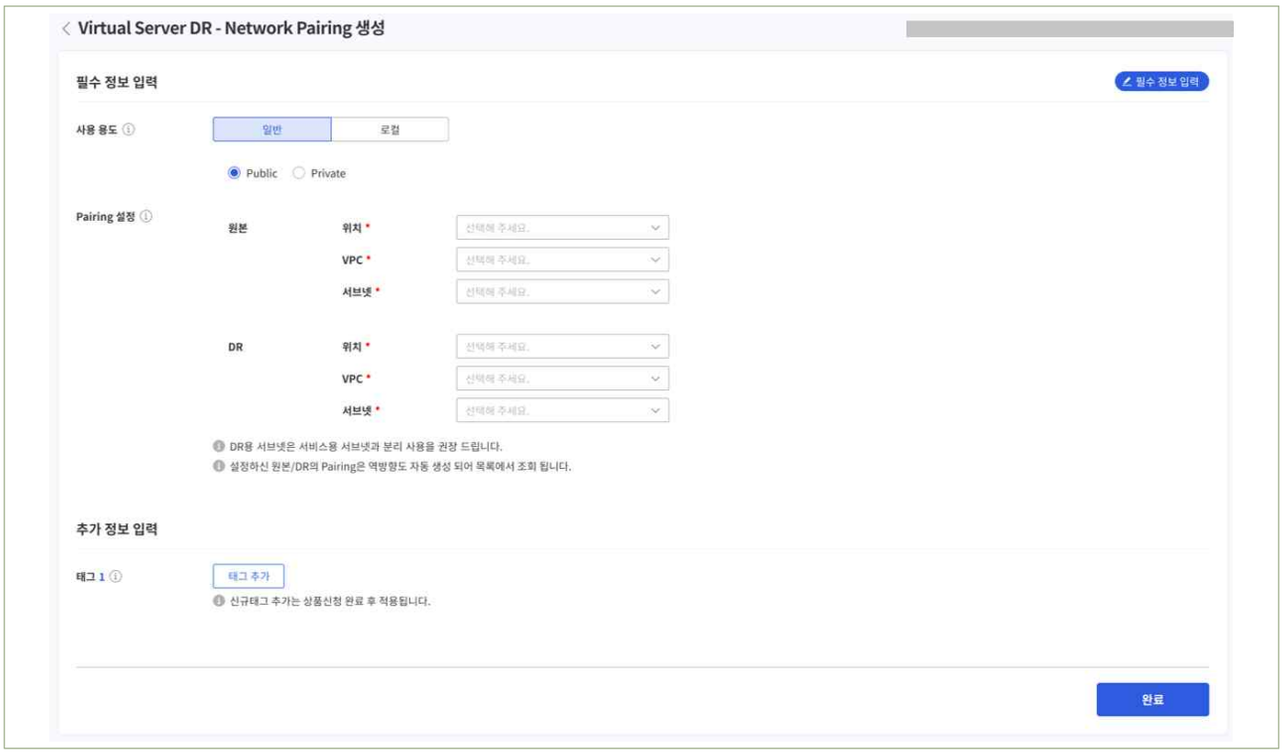
Ⅰ. Network Pairing 생성

Ⅱ. Network Pairing 목록 확인

Ⅲ. Network Pairing 삭제

[I. Network Pairing 생성]

- 신청 경로: 프로젝트 → 모든 상품 → Compute → Virtual Server DR → Network Pairing → Pairing 생성



| 그림 8.6.16 | Network Pairing 생성

A. 사용 용도: Pairing을 설정할 서브넷의 사용 용도 정보를 선택합니다.

- 원본과 DR의 서브넷 용도가 동일하게 설정되어 있어야 Pairing을 설정할 수 있습니다.
- 일반 용도를 선택하면 Public과 Private 중 하나를 선택할 수 있습니다.

B. Pairing 설정: Pairing을 설정할 원본과 DR의 서브넷을 선택합니다.

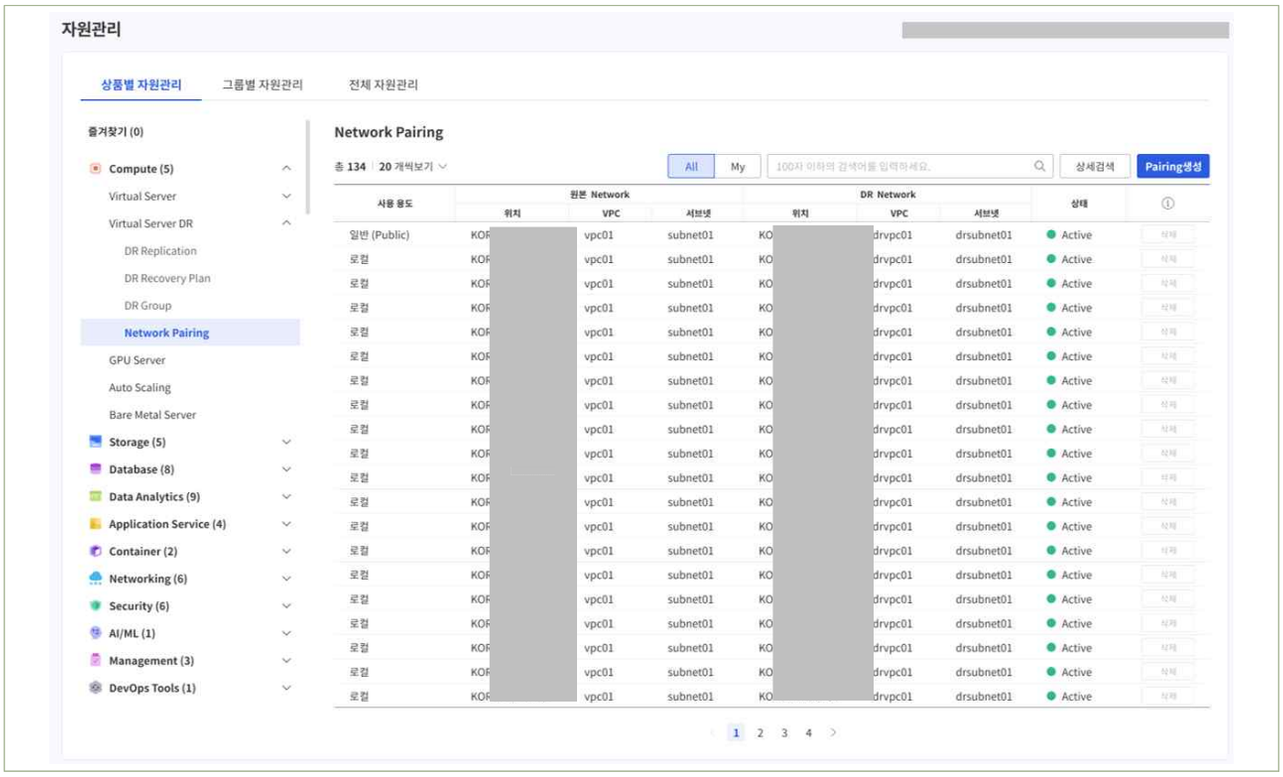
- 서브넷은 하나의 Network Pairing에만 적용할 수 있습니다.

・ 다른 Network Pairing에 적용된 서브넷은 선택할 수 없습니다.

C. 태그: 태그 정보를 입력합니다.

[II. Network Pairing 목록 확인]

- 확인 경로: 자원관리 → 모든 상품 → Compute → Virtual Server DR → Network Pairing



| 그림 8.6.17 | Network Pairing 목록 확인

A. ALL: 모든 Network Pairing 자원이 표시됩니다.

B. MY: 로그인한 사용자가 생성한 Network Pairing 자원이 표시됩니다.

C. 상세 검색: 검색어를 입력하거나 작업 일시, 작업 결과, 경로, 작업자명으로 상세 검색할 수 있습니다.

D. Pairing 생성: 상세정보를 확인할 항목을 선택합니다.

E. Network Pairing 정보: Network Pairing의 용도와 원본 및 DR 네트워크의 정보가 표시됩니다.

[III. Network Pairing 삭제]

- 신청 경로: Network Pairing은 사용자가 직접 삭제할 수 없습니다.

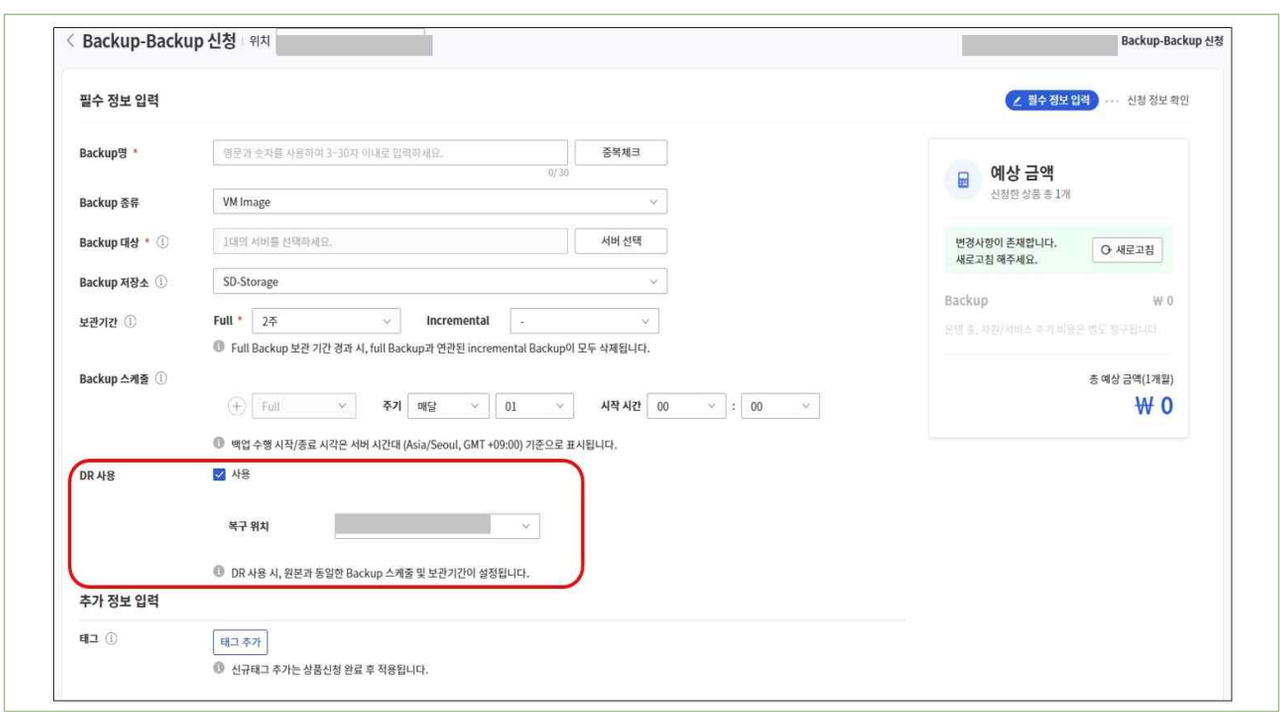
※ Network Pairing을 삭제하려면 상단 메뉴에서 물음표 버튼 → 서포트센터 → 서비스 요청 탭에서 서비스 요청을 클릭하여 Network Pairing 삭제를 신청하세요.

2) Backup 서비스의 DR 기능 이용

○ 재해 복구용 Backup 서비스를 이용하여 DR계획을 수립 및 실행할 수 있으며, 필요 시 Backup파일을 이용해 시스템을 백업할 수 있습니다

① Backup 신청을 통해서 Backup DR계획을 수립할 수 있습니다.

- 신청 경로 : '모든상품' → 'Storage' → 'Backup' → 'Backup' → '상품신청'
- Backup 서비스는 크로스 리전(cross-region) 기반의 DR(재해복구) 기능을 지원하므로, 메인 센터에서 생성한 이미지 스냅샷을 DR 센터로 복제 후 보관함으로써 지진, 태풍, 침수 등의 심각한 재난 및 재해로 인해 서비스 운영 지역에 피해가 발생한 경우에도 업무의 연속성을 원활하게 확보할 수 있습니다.
- 두 개 이상의 리전(Region)에서 서비스를 운영하는 경우에만 DR 기능을 사용할 수 있습니다.



| 그림 8.6.18 | Backup 신청

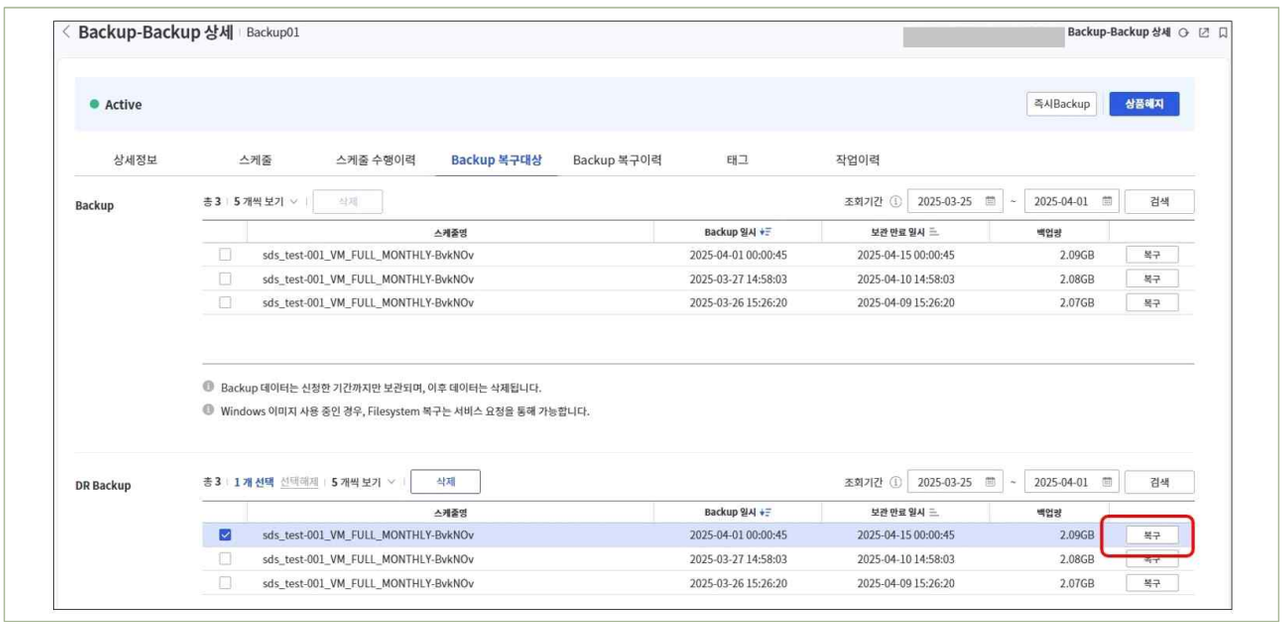
A. DR 사용: 재해 복구(DR, Disaster Recovery) 기능 사용 여부를 선택

B. 복구 위치: 재해 복구용 백업 이미지를 보관할 위치를 선택

・ DR 사용 시, Backup 스케줄 및 보관 기간이 원본 Backup과 동일하게

② DR Backup 파일 목록에서 DR Backup 파일을 이용하여 시스템을 복구할 수 있습니다.

- 신청 경로 : ‘모든상품’ → ‘Storage‘ → ‘Backup‘ → ‘Backup’ → ‘자원관리‘ → ‘상세정보‘ → ‘Backup 복구대상’

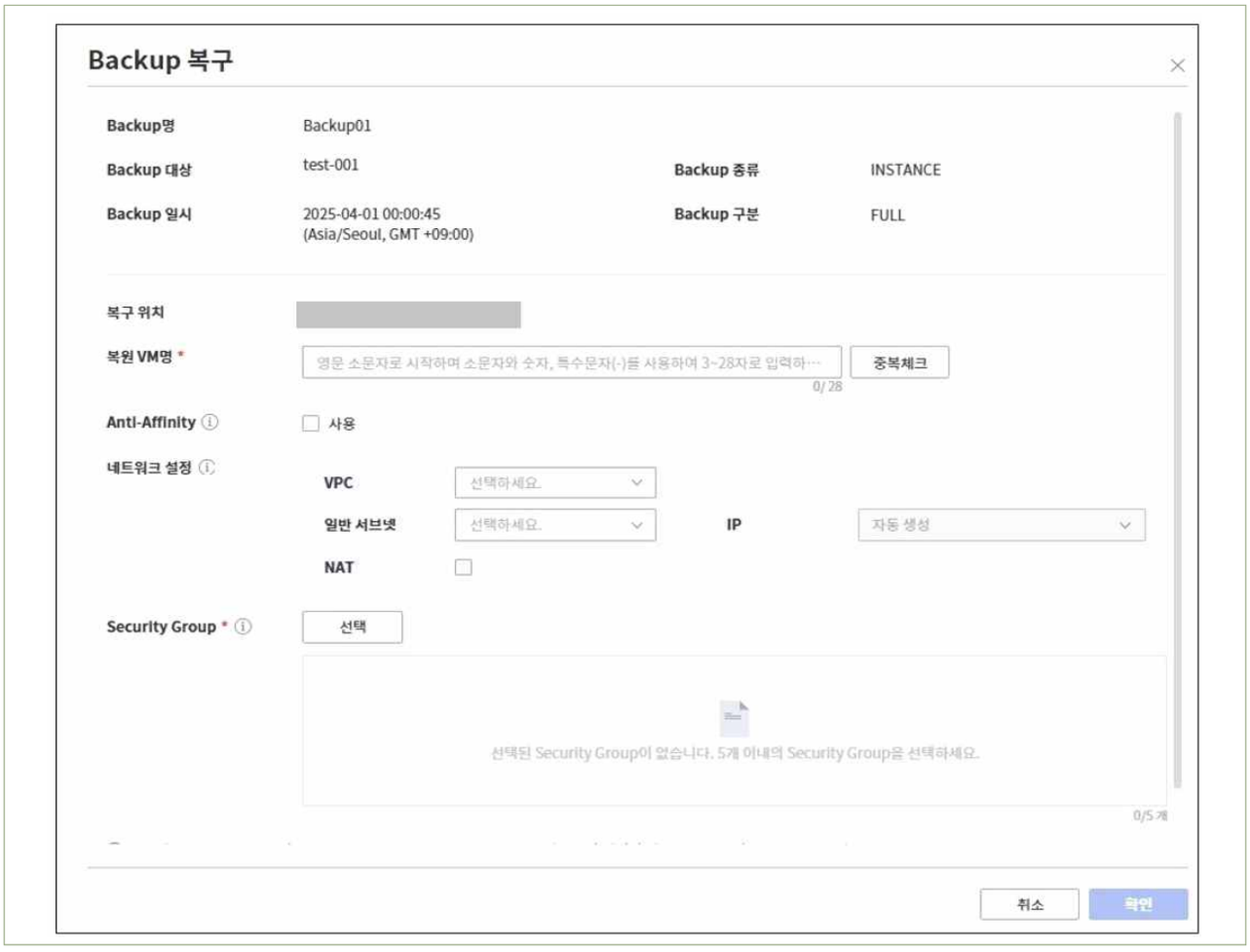


| 그림 8.6.19 | Backup 상세 (Backup 복구대상)

A. DR Backup 목록 우측 상단의 기간 영역에 검색 기간을 설정할 수 있습니다.

B. 조회 기간은 일주일로 기본 설정되어 있으며, 최대 조회기간은 한 달입니다.

C. DR Backup 파일 목록의 ‘복구’를 클릭하면 해당 DR Backup 파일을 사용하여 복구 작업을 진행할 수 있는 Popup 화면이 조회됩니다.

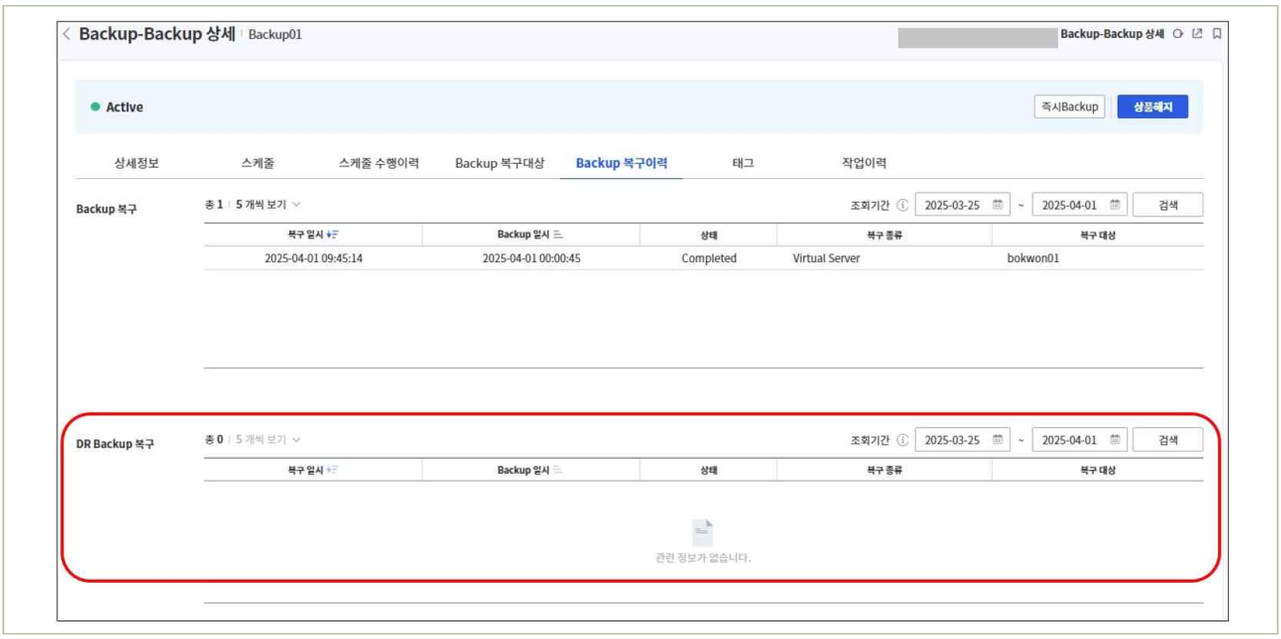


| 그림 8.6.20 | Backup 복구 상품 신청

- Backup명: 복구하고자 하는 Backup파일명을 조회합니다.
- Backup 대상: Backup 대상인 서버명을 조회합니다.
- Backup 일시: Backup을 수행했었던 일시를 조회합니다.
- 복구위치 : 복원할 위치를 조회합니다.
- 복원VM명 : DR Backup파일을 이용해 복구 후 사용할 VM (Virtual Server) 이름을 입력합니다.
- Anti-affinity: 하나의 서버그룹에 속한 서버들을 각각 다른 호스트에 배치시켜 호스트에 문제가 생겼을 경우 모든 서버들이 동시에 장애가 발생하지 않도록 합니다.
- 네트워크설정: Backup 복구를 위해서 사전에 네트워크 설정 작업이 필요합니다. (VPC, 서브넷, IP, NAT 필요)
- '확인' 클릭 시, 복원작업을 수행합니다.

③ 특정기간 동안의 복구 이력을 확인할 수 있습니다.

- 신청 경로 : ‘모든상품’ → ‘Storage‘ → ‘Backup‘ → ‘Backup’ → ‘자원관리‘ → ‘상세정보‘ → ‘Backup 복구이력’



| 그림 8.6.21 | Backup 상세 (Backup 복구이력)

A. DR Backup 복구 목록 우측 상단의 기간 영역에 검색할 기간을 설정할 수 있습니다.
B. 조회기간은 일주일로 기본 설정되어 있으며, 최대 조회기간은 한 달입니다.
C. 복구 일시: 복구작업 완료 일정과 시간을 조회합니다
D. Backup일시: DR Backup 복구 시에 사용했었던 Backup 파일이 작성되었던 일시를 조회합니다
E. 상태: Completed(완료)
F. 복구대상: DR Backup 복구 완료된(복구 후 사용할) VM (Virtual Server) 이름이 조회됩니다

4) Database-as-a-Service(DBaaS)의 Read Replica 기반 DR구성

- Replica 노드를 추가해 재난 상황에 대비하는 DR(Disaster Recovery) 환경을 구성 가능

① 사전 네트워크 설정: Multi-AZ/Region 네트워크 환경을 사전 구성

Ⅰ. 네트워크 항목 설정 (8.3.4 참고사항을 확인)

- VPC Peering 구성
- TGW Peering 구성
- Cloud WAN 구성
- Routing Table 구성
- Firewall 구성
- Security Group 규칙 추가

② Read Replica 기반 DR 구성

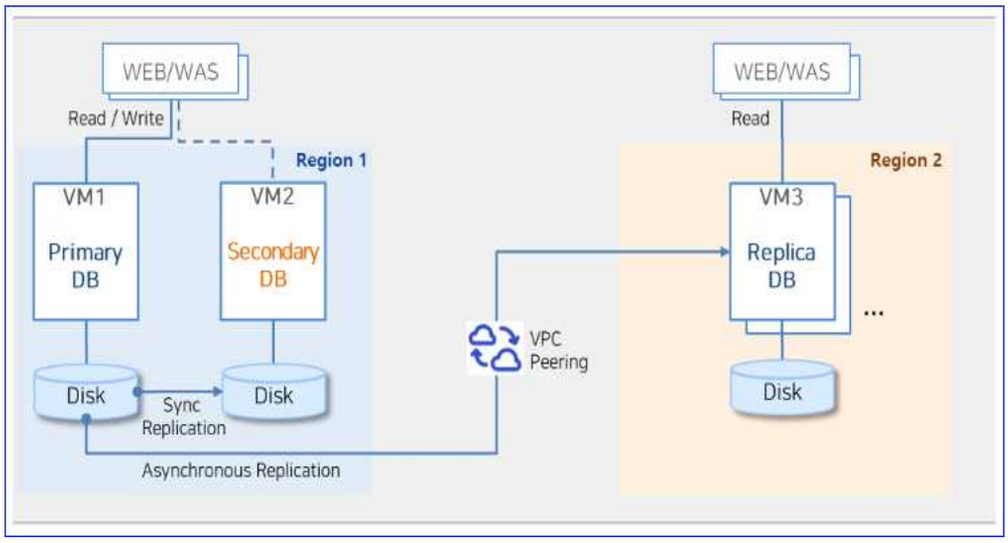
Ⅰ. Replica DR 신청하기

Ⅱ. Replica DR 구성하기

Ⅲ. Replica를 Master로 승격하기

[I. Replica DR 신청하기]

- 신청 경로: '프로젝트' → '모든 상품' → 'Database' → 'DBaaS 선택' → '상품 신청' → 필수 정보 입력
- DBaaS 서비스 목록: EPAS, PostgreSQL, MariaDB, MySQL, Microsoft SQL Server, Tibero (DBaaS에 따라 제공되는 Replica 속성이 상이할 수 있습니다.)
- Multi-AZ Replica DR 구성도



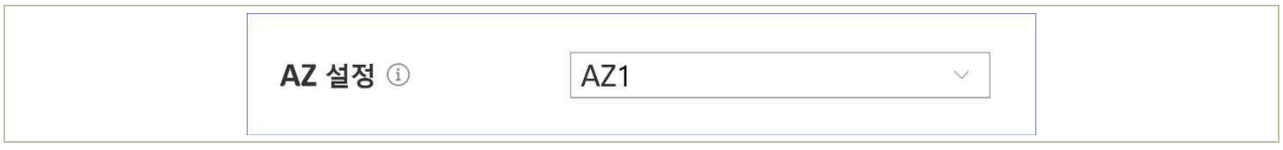
| 그림 8.6.22 | Multi-AZ Replica DR 구성도

A. 사전적 의미의 Database DR(재해복구)은 SCP의 Region 1에 운영시스템(Master DB, a.k.a. Primary DB)을 구성하고, Region 2에 Read Replica DB를 구성합니다.
  - [그림 8.6.22]의 Region 1의 운영시스템 내 Secondary DB는 HA용도
B. 평시에 비동기 복제를 통해 Master DB 정보를 원격저장소에 보관하고, 재해 발생 시 원격저장소의 Replica DB를 Master DB로 전환합니다.

- Replica 신청

| 그림 8.6.23 | Replica 구성 신청

A. Replica 구성 선택: Replica 사용을 선택합니다.
  - 서비스 신청 시점에는 동일한 VPC내에서만 구성할 수 있습니다.
  - Replica를 DR 목적으로 다른 Region에 생성하고자 할 경우 Replica 기반 DR 구성 변경하기를 참조합니다.



| 그림 8.6.24 | Multi-AZ 선택

B. Multi-AZ 선택: Replica가 위치할 AZ를 선택합니다.
  - Multi-AZ를 위한 사전 네트워크 설정이 완료된 경우 Replica가 위치할 AZ를 선택할 수 있습니다.

[II. Replica DR 구성하기]

- 신청 경로: ‘프로젝트’ → ‘모든 상품’ → ‘Database’ → ‘DBaaS 선택’ → ‘자원관리’ → 상세 정보 수정

- 드롭다운 메뉴에서 Replica구성을 선택(클릭).

| 그림 8.6.25 | Replica 구성 선택

- DR을 위한 Other-Region으로 Replica구성 변경.

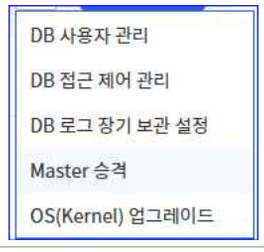
| 그림 8.6.26 | Other-Region 선택

A. Other-Region 사용 선택: 변경 가능한 Region 리스트가 나타납니다.

・ Region 1에서 Region2로 변경하면 기존 AZ 설정 내역이 변경됩니다.

[III. Replica를 Master로 승격하기]

- 신청 경로: '프로젝트' → '모든 상품' → 'Database' → 'DBaaS 선택' → '자원관리' → 상세 정보 수정
- 드롭다운 메뉴에서 Master 승격을 선택(클릭)



| 그림 8.6.27 | 복구하기 (DBaaS 자원관리 화면)

A. Master 승격 선택: 원본 DB(기존 Master)와 동기화가 중단됩니다.

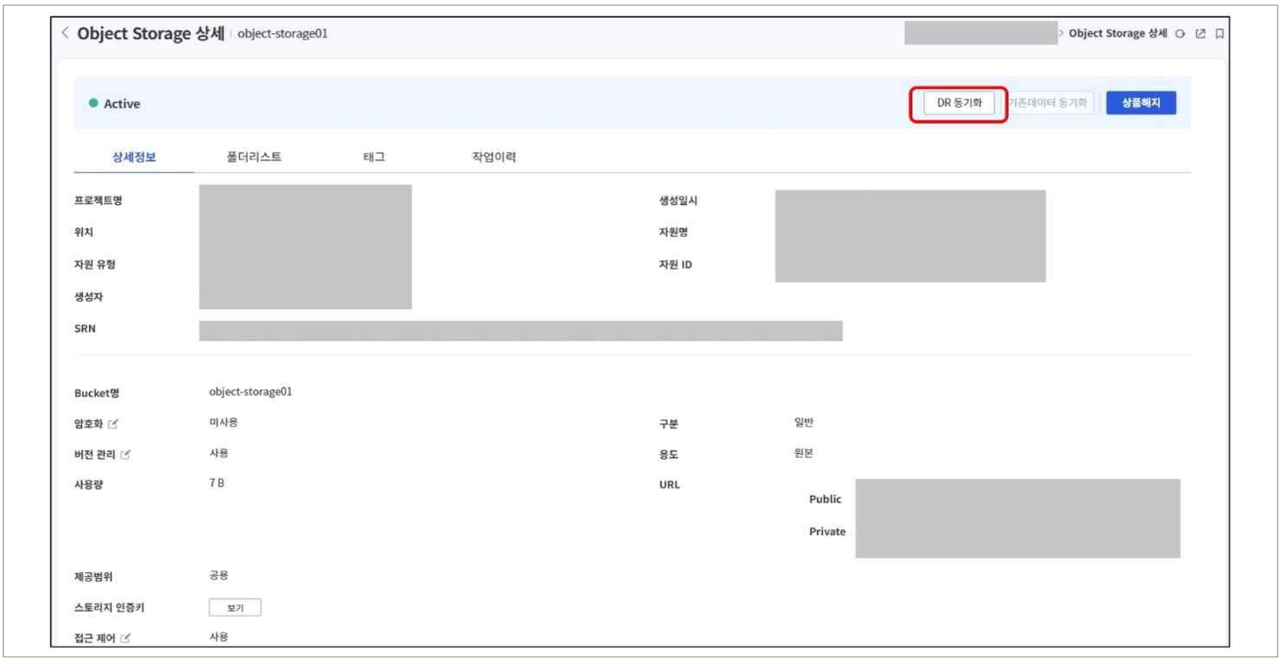
・ 승격한 Replica는 단독으로 서비스를 구성하며 인스턴스 유형은 Active로 변경됩니다.

5) Object Storage 서비스의 DR 기능 이용

- 데이터베이스 Backup본은 Object Storage에 저장되며, Object Storage에 저장된 Back Up 파일은 DR을 이용하여 원격지에 안전하게 보관할 수 있다.

① 재해복구(DR, Disaster Recovery) 기능을 사용하면 원본 Object Storage (버킷)의 복제본 버킷을 설정해 버킷 내 파일을 동기화해서 원격지에 안전하게 보관할 수 있습니다.

- 신청 경로 : '모든상품' → 'Storage' → 'Object Storage' → 'Object Storage' → 'DR동기화'
- Object Storage의 상세현황을 조회하며, 해당 Object Storage에 대해 원격지에 DR 파일을 생성합니다.



| 그림 8.6.28 | Object Storage 상세

A. 'DR동기화' 클릭 시, DR을 설정할 수 있는 Popup화면이 조회됩니다.

| 그림 8.6.29 | DR 동기화 상품 신청

B. DR을 설정하려면 해당 버킷이 다음 조건을 만족해야 합니다.
- 원본 버킷과 복제본 버킷이 서로 다른 위치(region)에 속해 있어야 합니다.
- 원본 버킷과 복제본 버킷 모두 복제본 설정이 없는 상태이며, 다른 버킷의 복제본이 아니어야 합니다.
- 원본 버킷과 복제본 버킷 모두 버전(version) 기능이 활성화 되어 있어야 합니다.

C. 복제본 버킷의 위치 정보와 이름을 버킷명을 선택한 후, 확인을 클릭하면 해당 원격지 위치에 DR파일이 생성되어 안전하게 보관됩니다.

4 참고 사항

- 「Samsung Cloud Platform 사용자 가이드」에서는
  - Virtual Server DR 활용 가이드
  - Backup 서비스의 DR 기능과 복구 관련 활용 가이드
  - Database-as-a-Service(DBaaS) 상품의 Database 별 사전 네트워크 설정, Read Replica 기반 DR 구성 가이드가 상세히 소개되어 있음.
- 더 자세한 내용을 알고 싶으시면 해당 가이드 참조

(https://cloud.samsungsds.com/manual/ko/scp_user_guide.html#getting_started_with_virtual_server_dr)
(https://cloud.samsungsds.com/manual/ko/scp_user_guide.html#94434a0dc8edee79
(https://cloud.samsungsds.com/manual/ko/scp_user_guide.html#02ca2b60bf6f170b)

1 기준

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

2 설명

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

  - 예시

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

    2) 이중화 구성 시 원격 안전지역 등을 고려

3 우수 사례

1) Database-as-a-Service(DBaaS)의 고가용성(High Availability)구성

- 고가용성 구성을 사용하면 DB 인스턴스가 Active DB(Primary DB)와 Standby DB(Secondary DB)로 구분되어 구성하고, Multi-AZ을 설정할 수 있는 위치를 사용하는 경우 사용자는 Active DB와 Standby DB가 위치할 AZ을 각각 선택하여 HA를 구성 가능

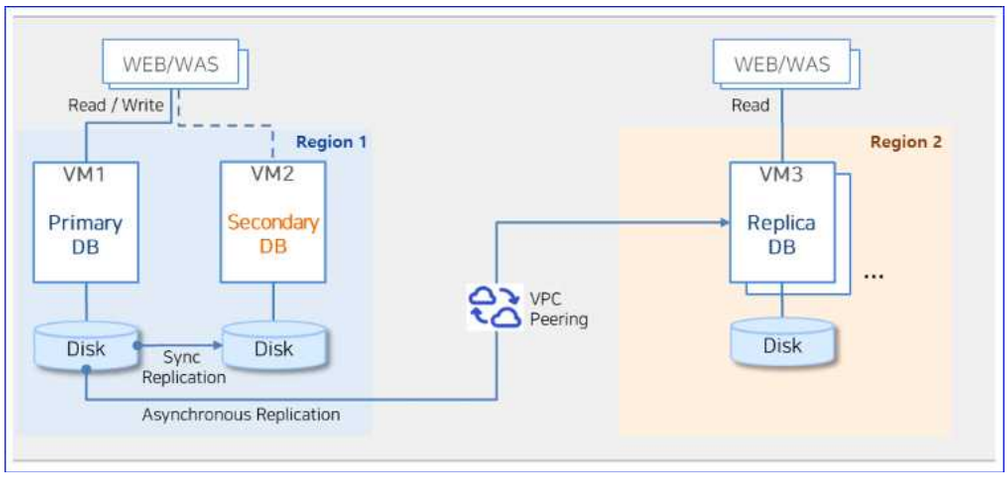
  ① 고가용성 구성

  Ⅰ. 고가용성 신청하기

  Ⅱ. Active DB와 Standby DB를 Switch Over 하기

  [I. 고가용성 신청하기]

  - 신청 경로: ‘프로젝트’ → ‘모든 상품’ → ‘Database’ → ‘DBaaS 선택’ → ‘상품 신청’ → 필수 정보 입력
  - DBaaS 서비스 목록: EPAS, PostgreSQL, MariaDB, MySQL, Microsoft SQL Server, Tibero (DBaaS에 따라 제공되는 고가용성 속성이 상이할 수 있습니다.)
  - 고가용성 구성도 ([그림 8.6.1] Multi-AZ Replica DR 구성도와 동일)



| 그림 8.7.1 | 고가용성 구성도

A. 고가용성 구성에서 전체 DB 워크로드를 Active DB(Primary DB)가 담당하고 Standby DB(Secondary DB)는 Active DB를 실시간으로 복제합니다.

B. 평상시 Switch Over기능을 통해 Active DB와 Standby DB를 상호 전환할 수 있으며, Active DB에 장애 발생 시 자동 Switch Over(Failover)가 발생하여 Standby DB가 Active DB로 전환됩니다.

- 고가용성 신청

| 그림 8.7.2 | Replica 구성 신청

A. 고가용성 사용 선택: 고가용성 사용을 선택합니다.

· 동일한 사양의 서버로 구성된 클러스터를 생성합니다.

[II. Active DB와 Standby DB를 Switch Over 하기]

- 신청 경로: '프로젝트' → '모든 상품' → 'Database' → 'DBaaS 선택' → '자원관리' → '상세 정보'
- Switch Over 버튼 선택(클릭)

| 그림 8.7.3 | Replica 구성 신청

A. Switch Over 선택: Active DB(Primary DB)와 Standby DB(Secondary DB)를 바꿀 수 있습니다.

B. Active DB 장애 시 자동으로 Failover(Switch Over)가 발생합니다.

4 참고 사항

- 「Samsung Cloud Platform 사용자 가이드」에 Database-as-a-Service(DBaaS) 상품의 Database 별 고가용성(High Availability) 구성 가이드를 참조 (https://cloud.samsungsds.com/manual/ko/scp_user_guide.html#02ca2b60bf6f170b)

금융분야 상용 클라우드컴퓨팅서비스 보안 관리 참고서 (삼성SDS)

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

〈비 매 품〉

금융분야
상용 클라우드컴퓨팅서비스 보안 관리 참고서