2026 – 비정기 – AGR – 클라우드평가 -708

금융분야
상용 클라우드컴퓨팅서비스
보안 안내서

NHN Cloud

금융보안원
FINANCIAL SECURITY INSTITUTE

NHN CLOUD

CONTENTS

1. 가상자원 관리

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

1 가상자원 관리

1 기준

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

2 설명

- 이용자 가상자원 생성 시 최초 계정에 대한 비밀번호 규칙을 수립하여야 한다.

  - 예시

    1) 비밀번호는 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설정
    2) 분기별 1회 이상 변경
    3) 가상자원 마다 관리자(root, administrator) 계정은 비밀번호를 다르게 설정

3 우수 사례

- NHN Cloud에서는 최초 가상자원 로그인은 SSH key를 이용한 방식을 제공하고 있습니다. SSH key를 이용한 로그인 방법은 '1.5 가상자원 접속 시 보안 방안 수립' 항목에서 가이드 합니다.

4 참고 사항

- 마켓플레이스 내 3rd-party 「시스템접근제어 및 계정관리솔루션」을 사용하면 가상자원 접근 계정에 대한 ID/PW 관리 등의 통제 정책 적용이 가능합니다.
- NHN Cloud 마켓플레이스

1 기준

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

2 설명

- 이용자 가상자원에 접근하는 계정에 대한 로그인 규칙을 수립하여야 한다.

  - 예시

    1) 로그인 오류에 따른 보안통제 방안 수립(5회이상 로그인 실패 시 계정 잠김 등)

3 우수 사례

- NHN Cloud에서는 최초 가상자원 로그인은 SSH key를 이용한 방식만 제공하고 있습니다. SSH key를 이용한 로그인 방법은 '1.5 가상자원 접속 시 보안 방안 수립' 항목에서 가이드 합니다.

4 참고 사항

- 마켓플레이스 내 3rd-party 「시스템접근제어 및 계정관리솔루션」을 사용하면 가상자원 접근 계정에 대한 ID/PW 관리 등의 통제 정책 적용이 가능합니다.
- NHN Cloud 마켓플레이스

1 기준

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

2 설명

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

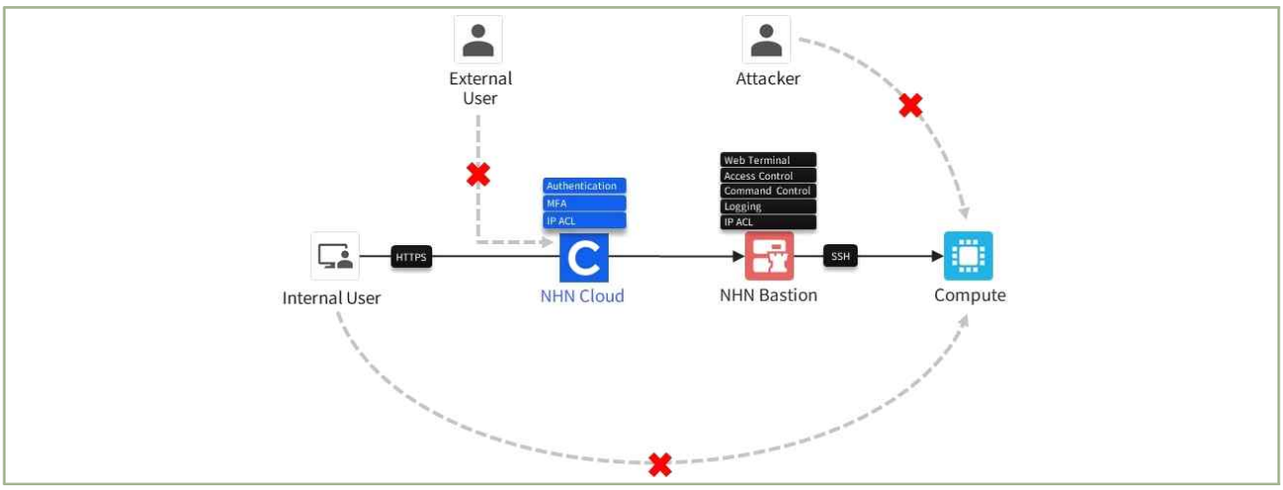
  - 예시

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

3 우수 사례

- NHN Cloud에서는 최초 가상자원 로그인은 SSH key를 이용한 방식만 제공하고 있습니다. SSH key를 이용한 로그인 방법은 '1.5 가상자원 접속 시 보안 방안 수립' 항목에서 가이드 합니다.
- NHN Bastion 서비스를 이용하여 NHN Cloud 인스턴스 접근 시 SSH 접근을 제어하거나 허용 또는 차단할 명령어를 등록할 수 있습니다.

  ① NHN Bastion을 통한 로그인 통제 방안

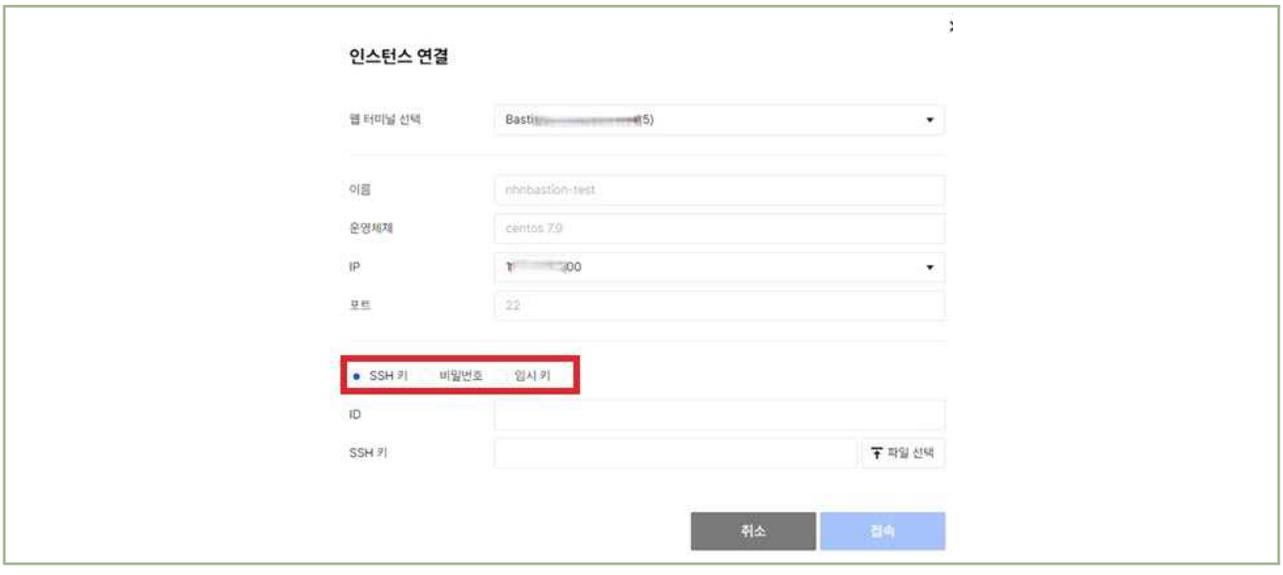


| 그림 1-3-1 | NHN Bastion 서비스 구성도

A. 사용자는 부여된 접근 통제 정책을 기반으로 현재 접속할 수 있는 서버들만 볼 수 있습니다.

| 그림 1-3-2 | NHN Bastion 콘솔 내 서버 나열 화면

B. 세 가지 인증 방식을 제공하고 있으며 고객 환경에 맞는 인증 방식을 선택하여 사용할 수 있습니다.



| 그림 1-3-3 | NHN Bastion을 통한 인스턴스 연결 인증 방법 선택

② NHN Bastion을 통한 명령어 통제 방안

A. NHN Bastion은 관문 서버 형태로 동작하여 웹터미널에 입력한 명령어를 제한하는 기능을 갖추고 있습니다.

| 그림 1-3-4 | NHN Bastion의 명령어 통제 기능 적용

B. 금지 또는 허용 명령어를 입력하고 우선 순위를 지정하여 정책을 관리할 수 있습니다.

우선순위	사용자	접근 대상	명령어 정책
#1	user A	Instance A	[금지] shutdown
#2	user A	Instance A, Instance B	[허용] cd
#3	user B	Instance A	[금지] reboot

| 그림 1-3-5 | 명령어 통제 적용 예시

가) 위의 그림에서 user A는 instance A 접근이 가능하고, shutdown 명령어만 사용 불가, 그 외 명령어는 사용이 가능합니다.

나) user A는 instance B 접근이 가능하고, cd 명령어만 사용 가능, 그 외 명령어는 사용이 불가합니다.

다) user B는 instance A 접근이 가능하고, reboot 명령어만 사용 불가, 그 외 명령어는 사용이 가능하고, instace B에는 접근이 불가합니다.

4 참고 사항

- 마켓플레이스 내 3rd-party 「시스템접근제어 및 계정관리솔루션」을 사용하면 가상자원 접근 계정에 대한 ID/PW 관리, 2-factor 인증 등의 통제 정책 적용이 가능합니다.
- NHN Cloud 마켓플레이스

1 기준

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

2 설명

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

  - 예시

    1) 가상자원 접속 가능한 공인IP(외부)대역 점검 및 제거
    2) 접근가능한 IP 또는 IP 대역대 설정
    3) VPC 및 보안그룹을 통한 내부 네트워크 대역대 접근 설정

3 우수 사례

- **(가상자원관리시스템)**

  - 가상자원에 직접 SSH로 접근하는 것을 차단 또는 관리하기 위해서는 외부와의 통신을 가능하게 하는 Floating IP(FIP)와 인스턴스의 접근통제 정책을 결정하는 Security Groups(SG)를 같이 관리해야 합니다.
  - Network ACL(NACL)을 통해 VPC 또는 Subnet에 대한 접근통제 정책 적용도 가능하며, Security Advisor 서비스를 통해 SG의 설정을 점검할 수 있습니다.

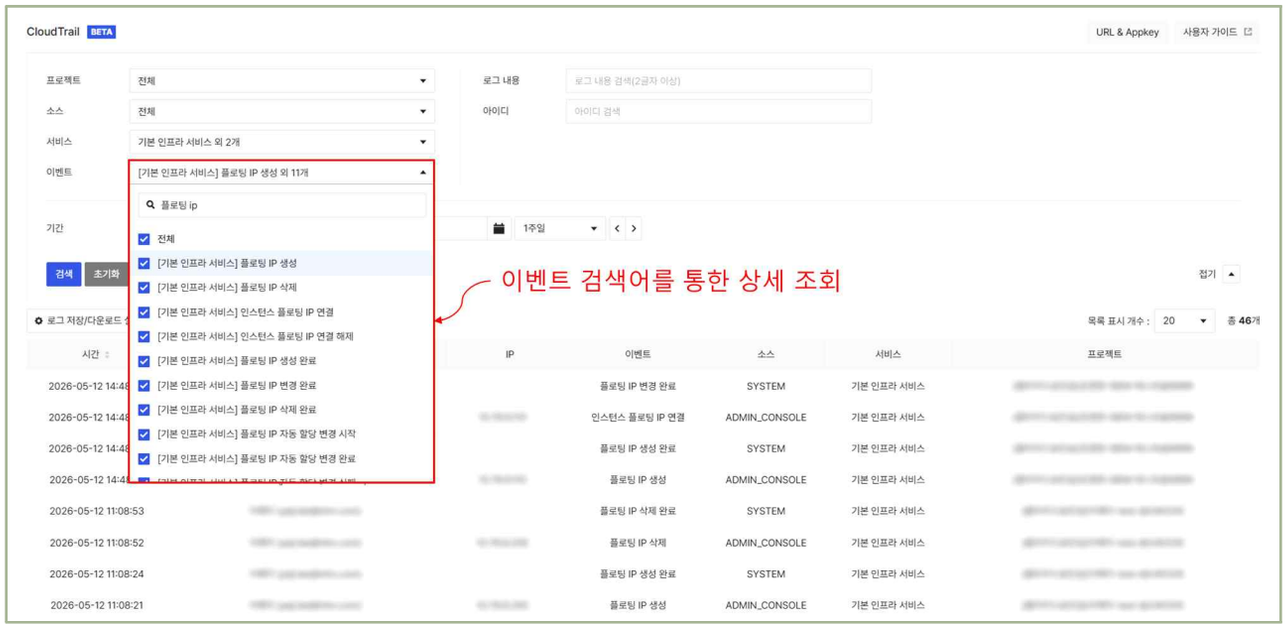
  ① Floating IP를 통한 관리 방안

  A. Floating IP 서비스 메뉴에서 생성한 FIP 및 FIP가 연결된 인스턴스 name을 확인할 수 있습니다.

  B. FIP 목록 및 연결된 장치(인스턴스 명)의 변화를 주기적으로 확인하면 불필요한 가상자원의 직접 연결을 확인할 수 있습니다.

| 그림 1-4-1 | Floating IP 메뉴 내 FIP 목록 조회

C. 실시간으로 불필요한 FIP 연결을 확인하지 못한 경우 FIP 발급/삭제 등의 로그를 CloudTrail을 통해 조회할 수 있습니다.



| 그림 1-4-2 | CloudTrail을 통한 공인 IP 발급 및 변경/삭제 로그 조회

D. CloudTrail log를 통해 세부 내용을 확인하려면 '로그 저장/다운로드 설정'을 설정하여 내용을 확인하여야 합니다.

가) OBS에 CloudTrail log를 저장하는 경우 저장 경로는 '저장 컨테이너명:년:월:일:시'로 저장됩니다.

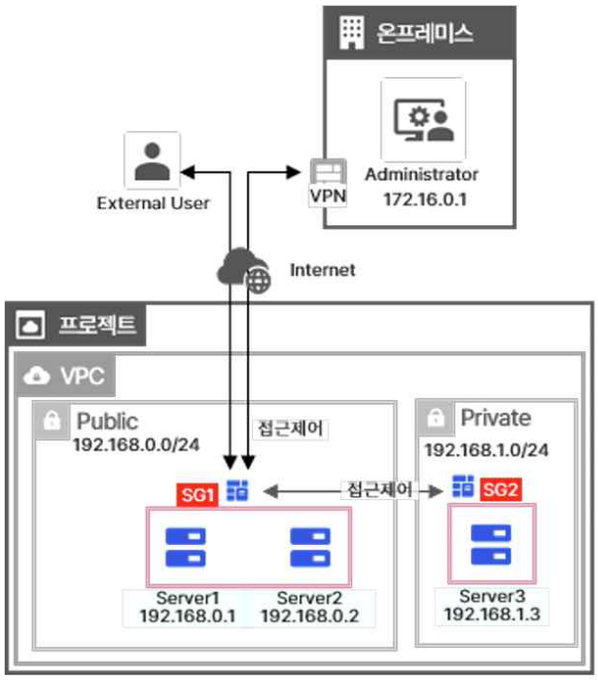
E. CloudTrail log 다운로드 방법은 nhn cloud '콘솔 사용자 가이드'를 참고하시기 바랍니다. (CloudTrail 사용 가이드)

| 그림 1-4-3 | OBS에 다운로드한 CloudTrail log 확인

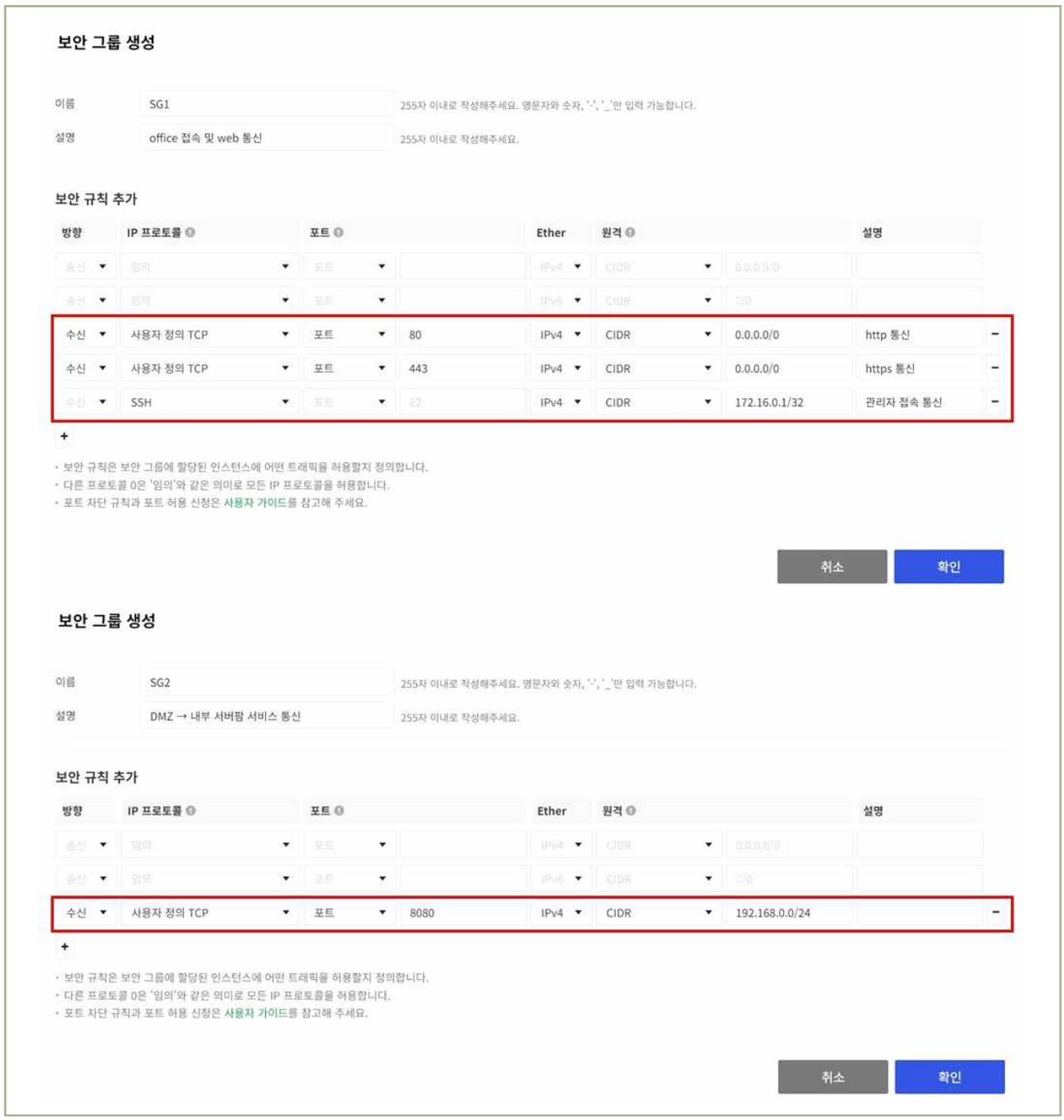
② Security Groups를 통한 관리 방안

- Security Groups는 stateful로 동작하기에 규칙으로 한 번 연결된 세션은 반대 방향의 규칙이 없더라도 허용됩니다.
- 개별 인스턴스 별로 적용할 수 있으며, Protocol, IP, Port 기준으로 제어할 수 있습니다.

A. '그림 1-4-4 Security Groups 적용 예시'의 구성에서 SG1 과 SG2의 설정은 다음과 같이 설정이 가능합니다. (그림은 「NHN Cloud 네트워크 아키텍처 보안가이드」에서 발췌)



| 그림 1-4-4 | Security Groups 적용 예시



| 그림 1-4-5 | Security Groups 생성 예시

※ '그림 1-4-5 Security Groups 생성 예시'에 default로 들어가 있는 송신 정책은 SG 생성 후 삭제할 수 있습니다.

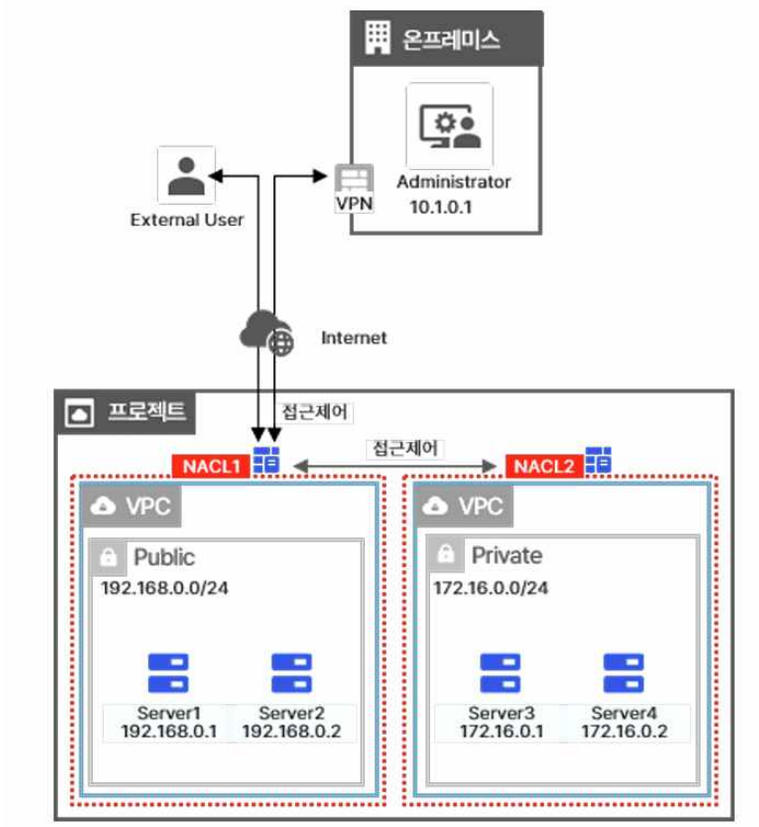
B. '그림 1-4-4 Security Groups 적용 예시'에서 Server3는 192.162.0.0/24 에서만 접근이 가능하고, 172.16.0.1 에서는 직접 접근이 불가능합니다.

C. 이처럼 외부에서 직접 접근할 필요가 없는 경우 Security Groups를 적용하여 접근통제를 구현할 수 있습니다.

③ Network ACL을 통한 관리 방안

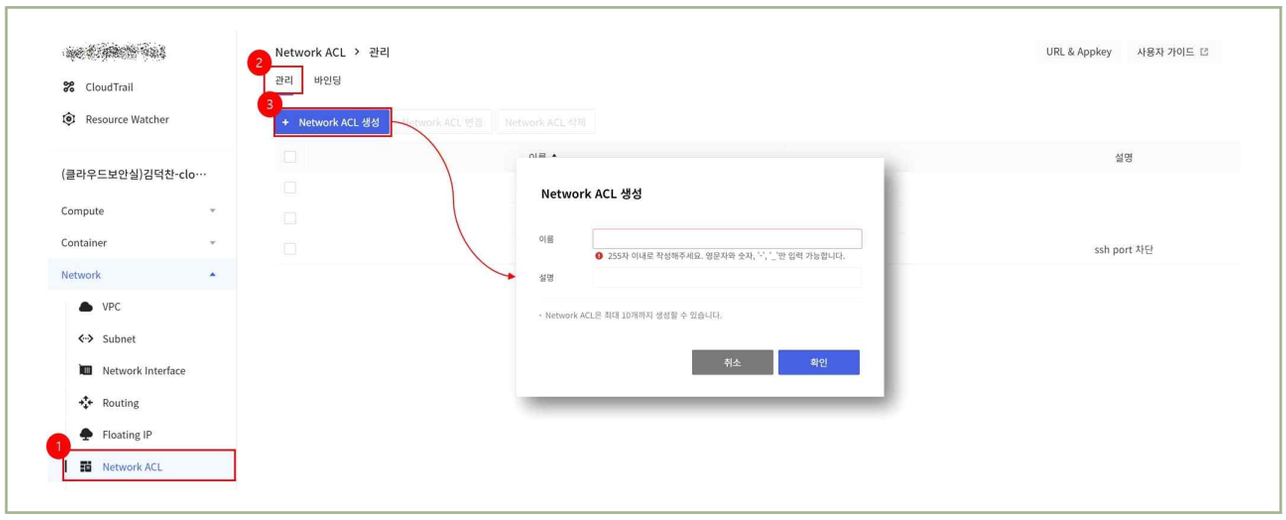
- Network ACL 상품의 경우 판교와 평촌 리전에서 서비스를 제공하고 있습니다.
- VPC 별로 ACL 정책을 binding 하여 적용할 수 있으며, 여러 network에 ACL을 binding 시킬 수 있습니다.
- 한 프로젝트에 최대 10개의 ACL을 생성할 수 있으며, 최대 100개의 Rule을 생성할 수 있습니다.
- 송신/수신 방향에 따라 NACL과 SG의 정책을 잘 확인해야 통신이 정확히 동작합니다.

A. '그림 1-4-6 NACL 구성 예시'의 아키텍처를 기반으로 Netwrok ACL 설정을 진행하겠습니다. (그림은 「NHN Cloud 네트워크 아키텍처 보안가이드」에서 발췌)



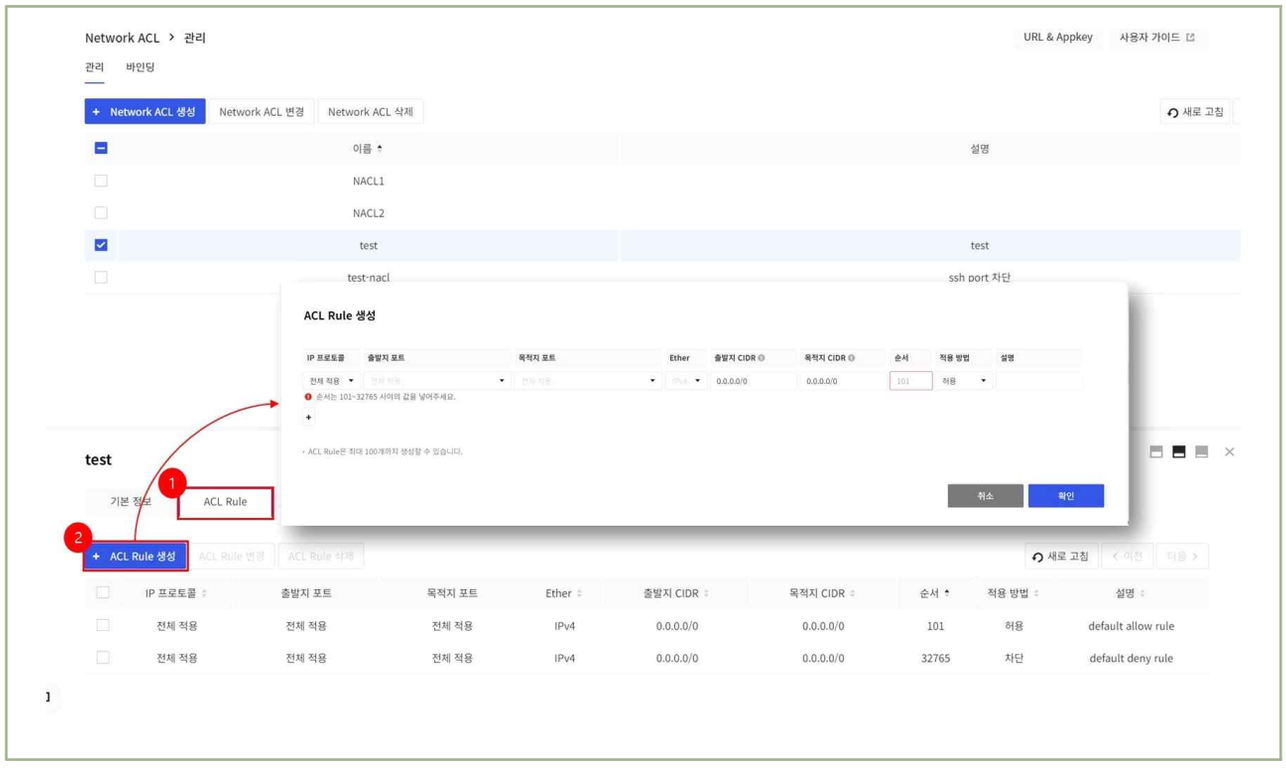
| 그림 1-4-6 | NACL 구성 예시

B. 평촌/판교 리전에서 [Network 〉〉 Network ACL]를 클릭한 후, 관리 탭의 'Network ACL 생성'을 클릭합니다.



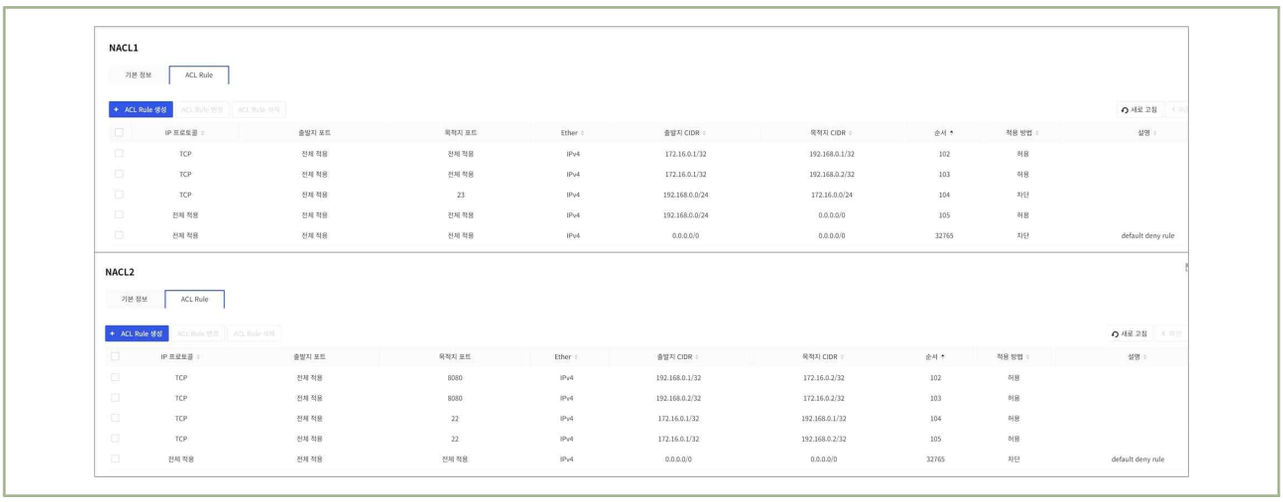
| 그림 1-4-7 | Network ACL 생성

C. 생성된 NACL을 클릭한 후 아래쪽 메뉴의 ACL Rule 탭을 클릭, 'ACL Rule 생성'을 클릭하여 ACL Rule을 생성합니다.



| 그림 1-4-8 | NACL Rule 생성

D. 출발지 CIDR 및 목적지 CIDR, 포트, 허용/차단 여부 등을 고려하여 정책을 수립합니다.



| 그림 1-4-9 | NACL ACL Rule 설정 예시

④ Security Advisor 이용 방법

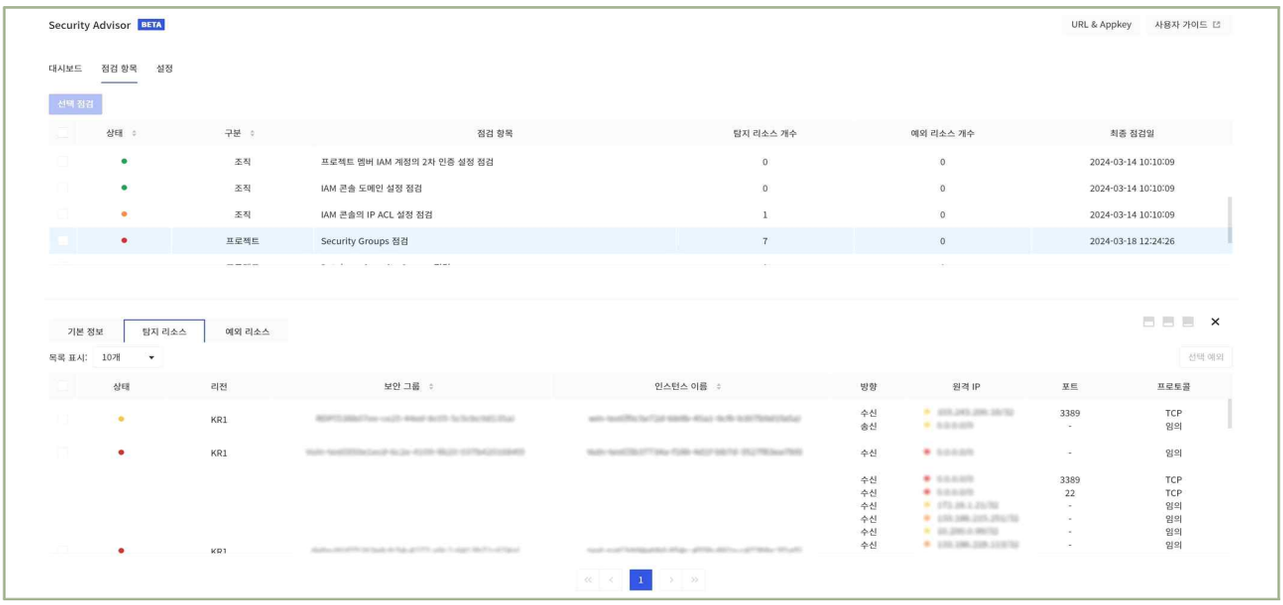
- Security Advisor는 고객이 생성한 NHN Cloud 조직 및 프로젝트 리소스의 보안 설정 상태를 점검하고 권장 가이드를 제시하는 서비스로, 주요 기능으로 Security Groups를 점검하여 인스턴스에 적용된 보안 규칙을 확인하는 기능을 제공합니다.

A. [Security 〉〉 Security Advisor] 메뉴의 '점검 항목'을 클릭, Security Groups 점검이 선택되어 있는지 확인한 후 '선택 점검'을 클릭하여 점검을 시작합니다.

| 그림 1-4-10 | Security Advisor 점검

B. 점검이 완료되면 '탐지 리소스 개수'에 취약점이 존재하는 수를 표시합니다.

C. 'Security Groups 점검' 항목을 클릭하여 취약한 Security Groups를 확인합니다.



| 그림 1-4-11 | Security Groups 점검 결과

| 그림 1-4-12 | Security Advisor 항목 내 Security Groups 점검 항목 정보

4 참고 사항

- 「NHN Cloud 네트워크 아키텍처 보안가이드」에서 더 많은 접근통제 방법에 대해 다루고 있습니다. 더 자세한 내용을 알고 싶으시면 해당 가이드를 추가로 참조 바랍니다.

1 기준

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

2 설명

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

  - 예시

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

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

3 우수 사례

- **(가상자원관리시스템)**

① NHN Cloud 에서는 인스턴스 로그인 시 비밀번호를 이용한 로그인 방식 대신 키 페어를 이용한 로그인 방식만 지원하고 있습니다.

※ 키 페어

SSH 접속을 위한 공개키(PKI) 기반의 키 쌍으로 공개키와 개인키로 구성되며, ID/PW의 취약한 인증방식 대신 키 페어를 이용하여 개인 키 파일을 소유한 사람만 접속할 수 있는 방식입니다.

Pem key의 관리가 매우 중요하며, 다음의 보호조치들을 추가로 적용할 수 있습니다.

ㄱ. key 분실에 대비하여 안전한 장소에 key를 백업 저장

ㄴ. key 유출 시 해당 key로 로그인하는 모든 인스턴스에 접근이 가능하므로, 인터넷 또는 이메일로 타인에게 전달 금지

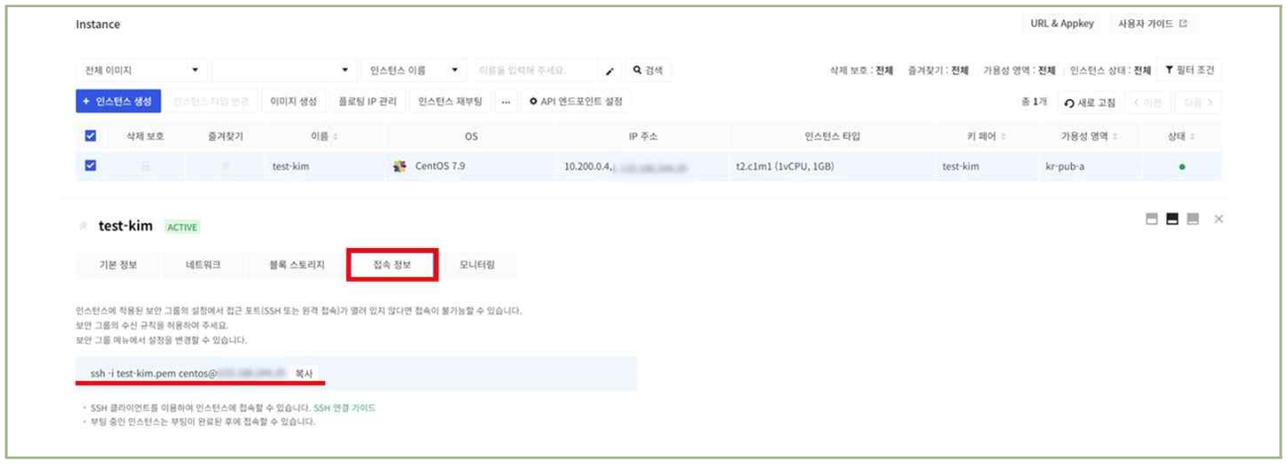
ㄷ. 유출이 의심되는 경우 인스턴스 키 페어 변경 기능을 이용하여 유출된 키 페어 변경

② '그림 1-5-1 키 페어 이용 또는 신규 생성 가능'과 같이 신규 키 페어를 생성하거나 기존에 이용하던 키 페어를 이용하여 접속을 설정할 수 있습니다. 참고로 한번 다운로드 받은 키 페어는

다시는 다운로드 받을 수 없습니다.

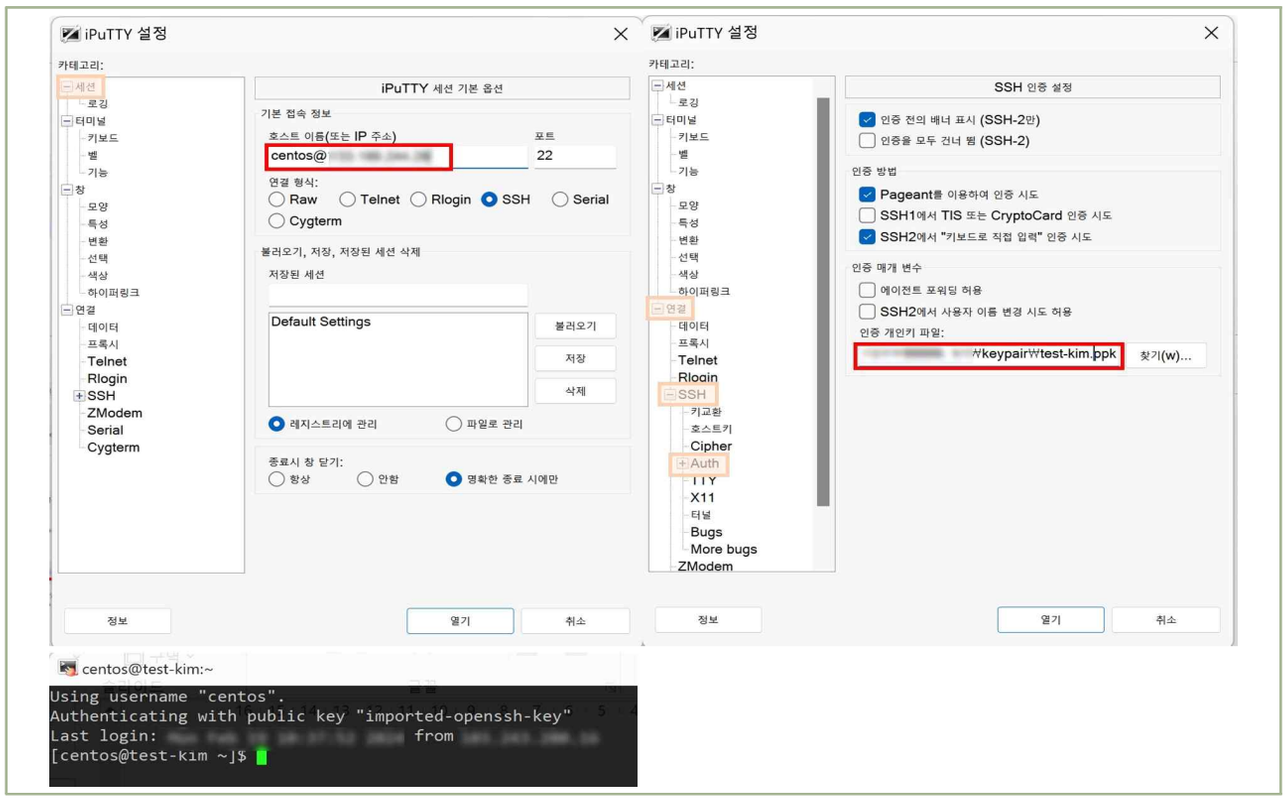
| 그림 1-5-1 | 키 페어 이용 또는 신규 생성 가능

③ 인스턴스 생성 후 콘솔에서 접속 정보를 확인할 수 있습니다.



| 그림 1-5-2 | 접속 정보 확인 방법

④ 확인된 접속 정보를 바탕으로 접속프로그램(putty 등)을 이용하여 인스턴스에 키 페어를 이용하여 접속할 수 있습니다.

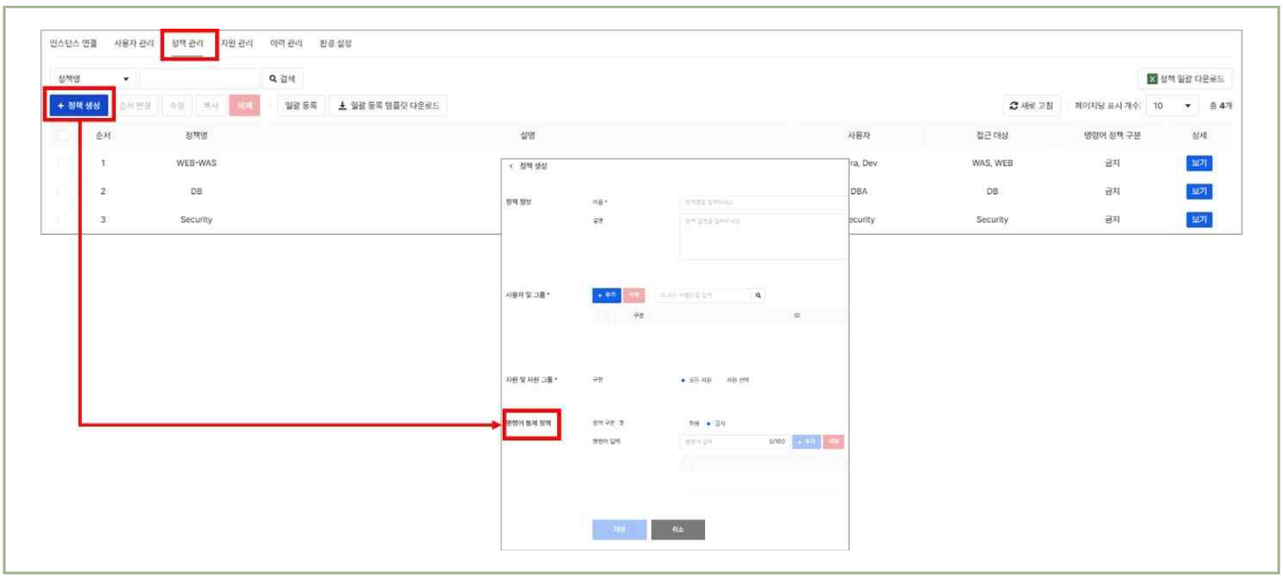


| 그림 1-5-3 | putty를 이용한 접속 설정 및 접속 성공 화면

※ Putty 등 pem 키를 사용하지 못하는 SSH tool의 경우 ppk 파일로 변환하여야 하며, puttygen 등을 이용하여 ppk 파일로 변환할 수 있습니다.

⑤ NHN Bastion 서비스를 이용하여 서버 접근 인증 제어가 가능합니다(1.3 참조). 추가 기능으로 사용자에 대한 명령어 통제 정책을 적용할 수 있습니다. 명령어 통제는 화이트리스트 또는 블랙리스트 방식으로 제공합니다.

- [NHN Bastion 〉〉 정책 관리] 메뉴에서 “정책 생성”(정책이 이미 생성되어 있을 경우 “수정” 클릭하여 정책 변경) 클릭 후 사용자 또는 사용자 그룹에게 적용할 명령어 통제 정책을 추가합니다.



| 그림 1-5-4 | NHN Bastion 명령어 통제 정책 추가

- NHN Bastion 서비스는 각 세션의 사용자 ID, IP 주소, 연결 시간, 수행 중인 작업 등을 실시간으로 표시하며 의심스러운 활동이 감지될 경우, 관리자는 즉시 해당 세션을 차단하거나 강제 종료할 수 있습니다. 또한 각 세션에서 실행된 명령어 전체 목록, SFTP를 통한 모든 파일 업로드/다운로드 활동을 추적할 수 있으며 모든 로그는 암호화 기능을 제공하고 있습니다. 상세 내용은 사용자 가이드(NHN Bastion 사용자 가이드)를 통해 추가 확인 가능합니다.

(API)

① NHN Cloud는 API를 통해 가상자원을 생성 및 관리 할 수 있도록 지원하고 있습니다.

② API를 이용하려면 token을 발급받아야 하며, 사전에 “테넌트 ID”, “API 비밀번호”를 설정 및 확인하여야 합니다.

| 그림 1-5-5 | API 사용을 위한 API 엔드포인트 설정

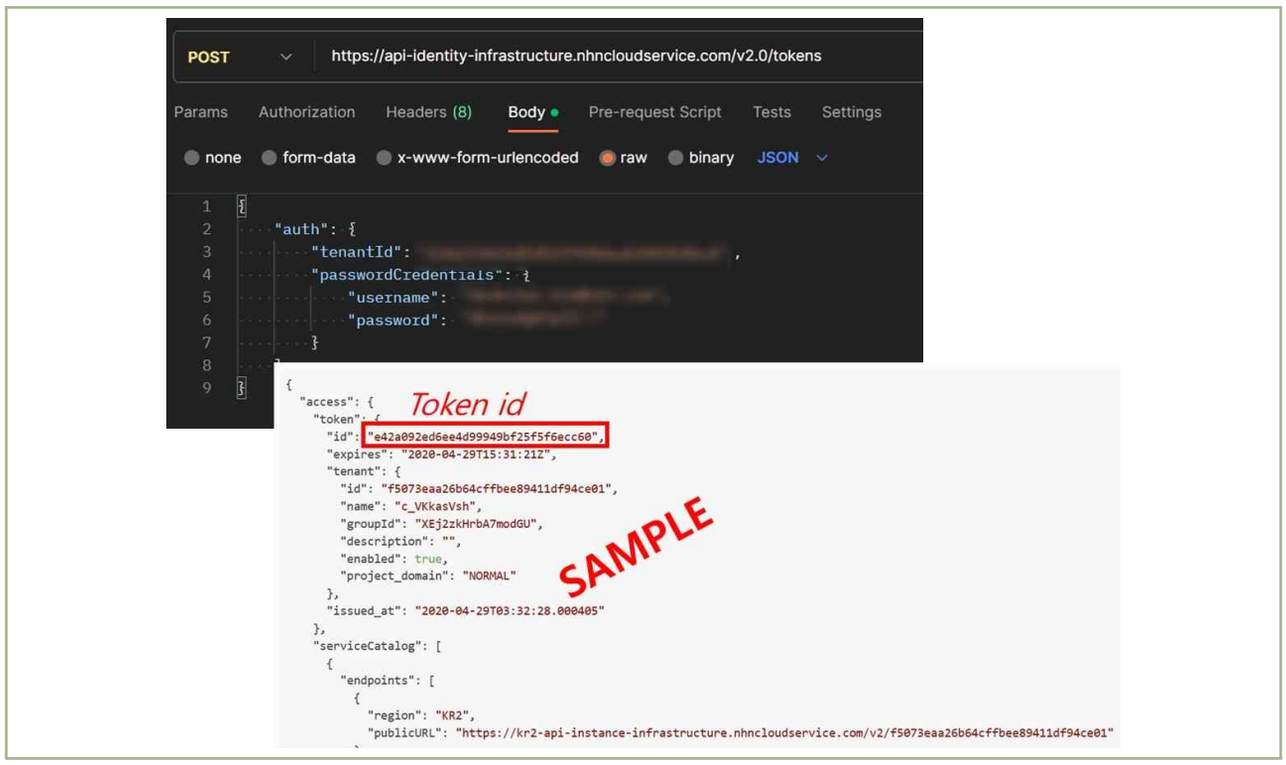
③ 설정한 API 엔드포인트 정보를 활용하여 token을 발급받을 수 있습니다.

④ 홈페이지 사용자가이드의 [Compute 〉〉 Instance 〉〉 API 사용 준비] 메뉴에서 token을 발급받기 위한 API 정보를 확인합니다.

| 그림 1-5-6 | Token 발급 API 예시 확인

⑤ '그림 1-5-6 Token 발급 API 예시 확인'의 정보를 바탕으로 API 정보를 작성합니다.

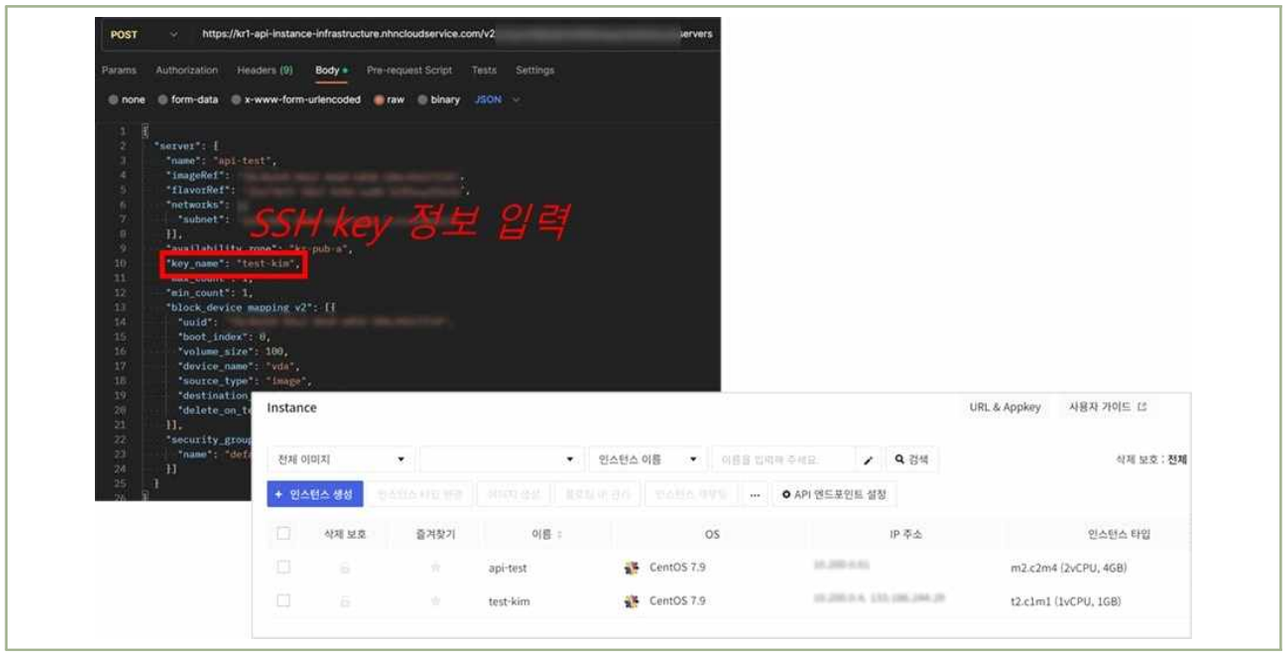
"tenantID" 와 "password"는 'API 엔드포인트 설정'에서 설정한 정보를 입력하고, "username"은 API를 사용하고자 하는 계정 명(nhncloud 회원의 경우 이메일, IAM 회원의 경우 회원 id)을 입력하여 토큰을 발급받습니다.



| 그림 1-5-7 | API 사용을 위한 token 생성

⑥ '그림 1-5-7 API 사용을 위한 token 생성'에서 발급받은 토큰으로 인스턴스 생성 API를 작성, 인스턴스를 생성할 수 있습니다.

※ *토큰의 유효 시간은 12시간이며, 토큰 유출 시 피해가 발생할 수 있으므로 각별한 주의가 필요합니다.*



| 그림 1-5-8 | API를 통한 인스턴스 생성

⑦ NHN Cloud의 사용자 가이드(API)를 참고하여 다양한 API의 예시를 확인할 수 있으며, 해당 예시 내 일부 내용을 수정하여 API를 호출할 수 있습니다.

4 참고 사항

- ID/PW로 로그인하려면 서버 생성 후 config 파일 수정이 필요합니다. OS 종류 및 버전별로 설정하는 방법이 다르기에 정확한 설정방법을 확인하고 config 파일을 수정하면, ID/PW로 로그인하도록 설정할 수 있습니다.
- 마켓플레이스 내 3rd-party 「시스템접근제어 및 계정관리솔루션」을 사용하면 가상자원 접근 계정에 대한 ID/PW 관리 등의 통제 정책 적용이 가능합니다.
- NHN Cloud 마켓플레이스

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 가상자원별 접근통제 방안을 수립하여야 한다.

  - 예시

    1) 가상자원 종류별 접근통제 방안 수립(ex. IAM을 통한 접근권한 관리)

       - 모든 가상자원에 접근 가능한 Role에 대해서는 최소한에 인원에 대해서만 부여

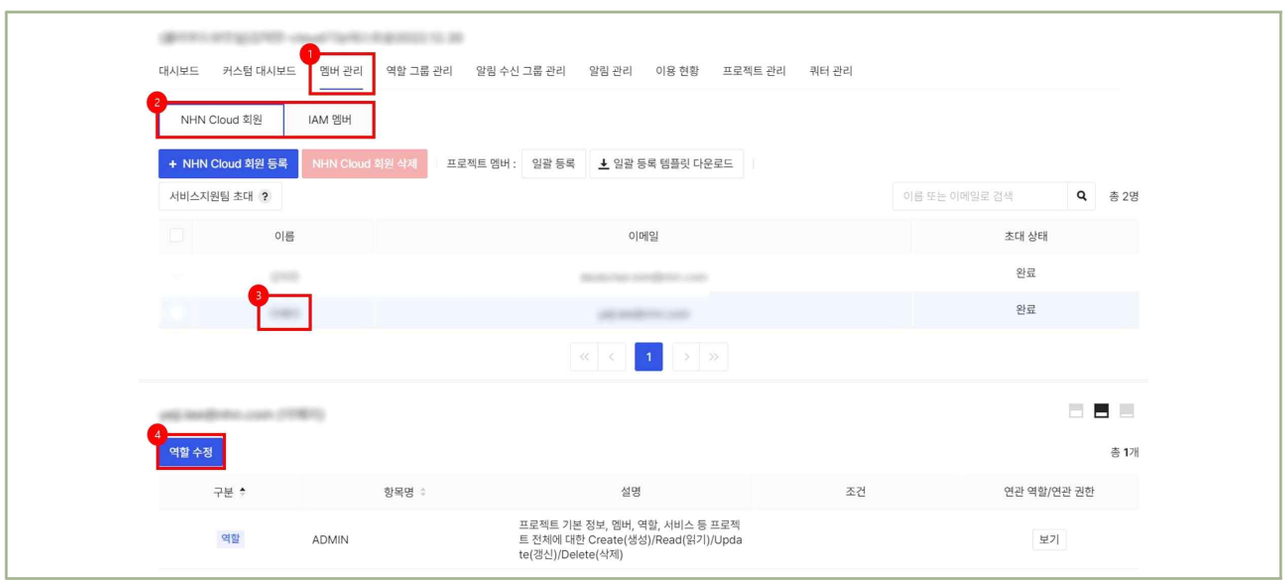
3 우수 사례

- **(가상자원관리시스템)**

  ① Console 사용자의 서비스 권한 관리

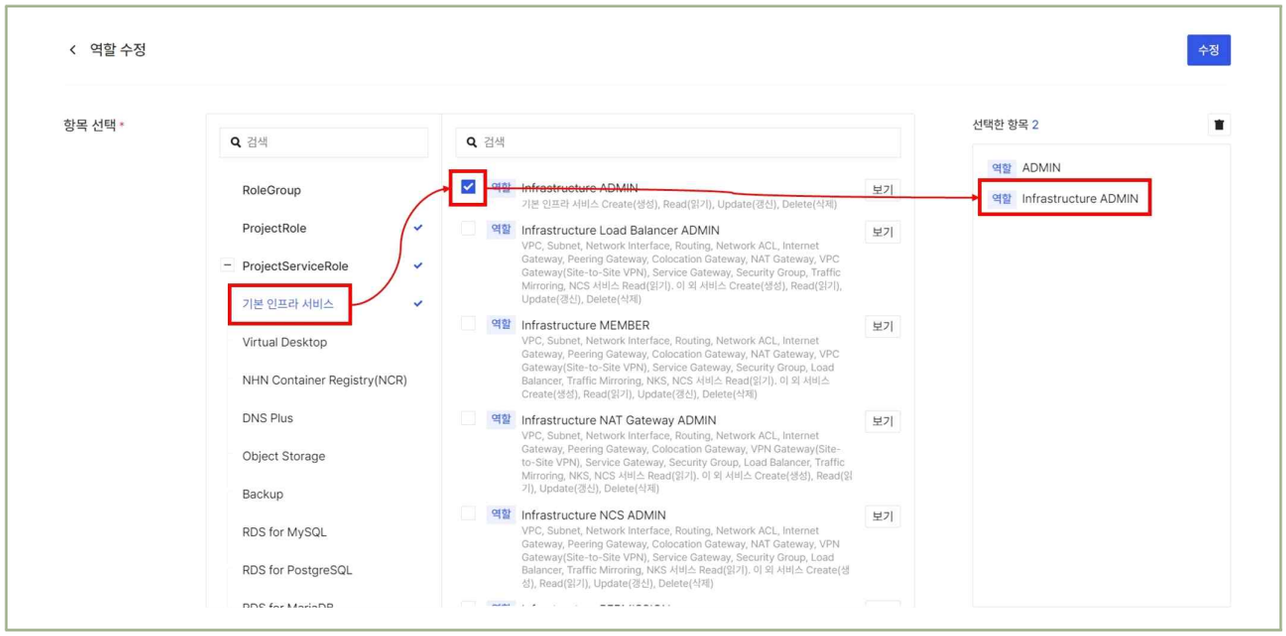
  A. NHN Cloud의 Console은 서비스별로 권한을 관리할 수 있습니다.

  B. [프로젝트 〉〉 멤버 관리 〉〉 NHN Cloud 계정 또는 IAM 계정 〉〉 이름 클릭 〉〉 역할 수정]을 클릭하면, 프로젝트 내 이용가능한 서비스 및 서비스 권한을 설정할 수 있습니다.



| 그림 1-6-1 | Console 사용자의 서비스별 역할 설정

C. 기본적인 가상자원 서비스인 compute 서비스 및 network 서비스, storage 서비스, database 서비스, security 서비스는 '기본 인프라 서비스'로 역할이 통합되어 설정되어 있으며, 그 외 서비스는 별도로 서비스 권한을 설정할 수 있습니다.



| 그림 1-6-2 | 서비스 별 권한 설정 화면

D. '기본 인프라 서비스'의 권한 중 'Infrastructure ADMIN' 권한은 필요한 최소한의 인원에게만 부여하여 가상자원을 생성할 수 있는 인원을 제한하고, 개발 부서는 생성된 자원을 이용하는 형태로만 서비스를 이용하도록 할 수 있습니다.

② Instance 사용자의 권한 관리

A. 고객이 생성한 가상자원 Instance의 계정 관리는 보안 책임 공유 모델(SSRM) 상 이용자의 책임 영역입니다.

B. 다만 OS 내 사용자 계정을 추가하고, 계정별 권한을 차등으로 부여하는 방법으로 권한을 차등 부여할 수 있습니다.

4 참고 사항

- 마켓플레이스 내 3rd-party 「시스템접근제어 및 계정관리솔루션」을 사용하면 Instance의 사용 계정/권한 차등부여 등의 통제 정책 적용이 가능합니다. NHN Cloud 마켓플레이스

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

- **(가상자원관리시스템)**

  - NHN Cloud는 console에서 가상자원에 백신 상품을 설치할 수 있도록 서비스를 제공하고 있습니다.
  - FIP를 가지고 있는 인스턴스 대상으로만 서비스가 제공되며, windows 및 linux 계열을 제공하고 있습니다.

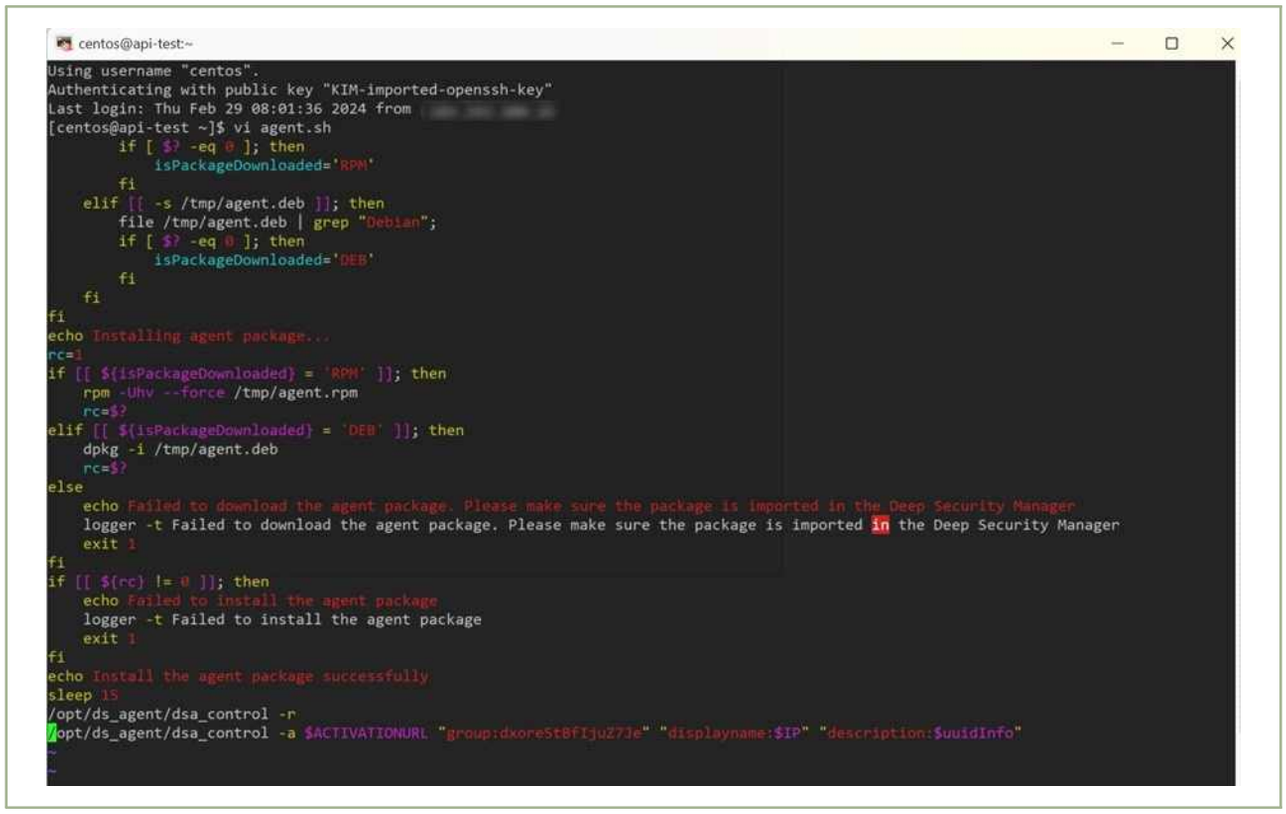
  ① Linux 시스템 백신 설치

  A. 설치를 위해서는 Instance에 스크립트 파일을 구동 시켜야 하며, 스크립트는 console에서 확인할 수 있습니다.

  B. 먼저 vaccine 서비스를 활성화하고, instance OS를 선택하여, 설치 스크립트를 복사합니다.

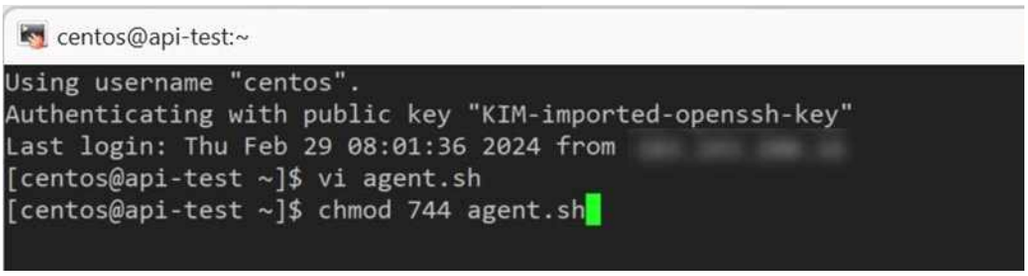
| 그림 1-7-1 | Vaccine 설치를 위한 스크립트 확인

C. Instance에 접속하여 'vi agent.sh'를 입력하여 스크립트 파일(agent.sh)을 생성/열람하여 console에서 복사한 스크립트를 붙여 넣습니다.



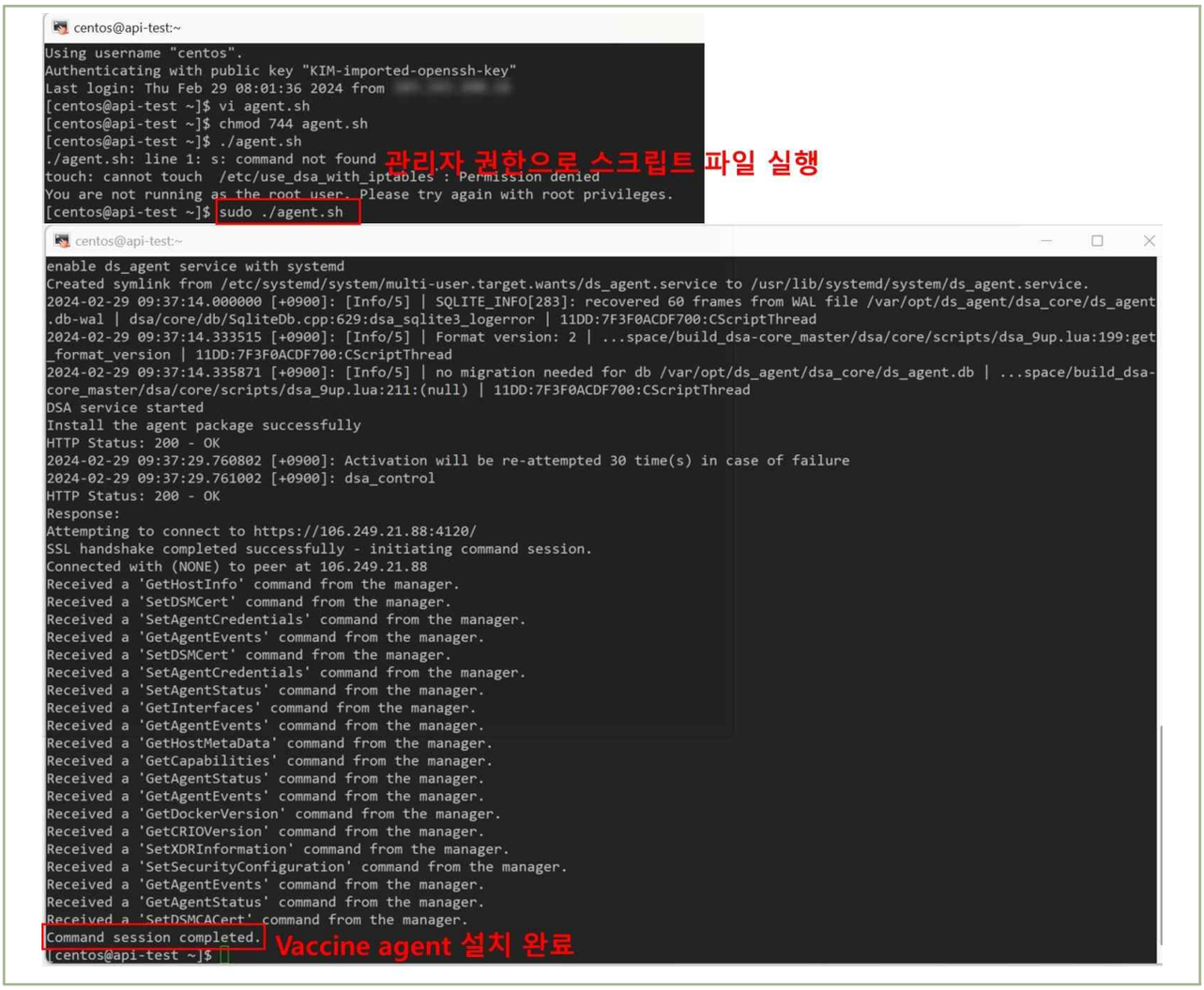
| 그림 1-7-2 | Vaccine을 설치할 instance에 설치 스크립트 파일 생성

D. 생성한 스크립트 파일의 권한을 변경합니다.



| 그림 1-7-3 | 스크립트 파일 권한 변경

E. 해당 스크립트 파일을 관리자 권한으로 실행하여 agent를 설치합니다.

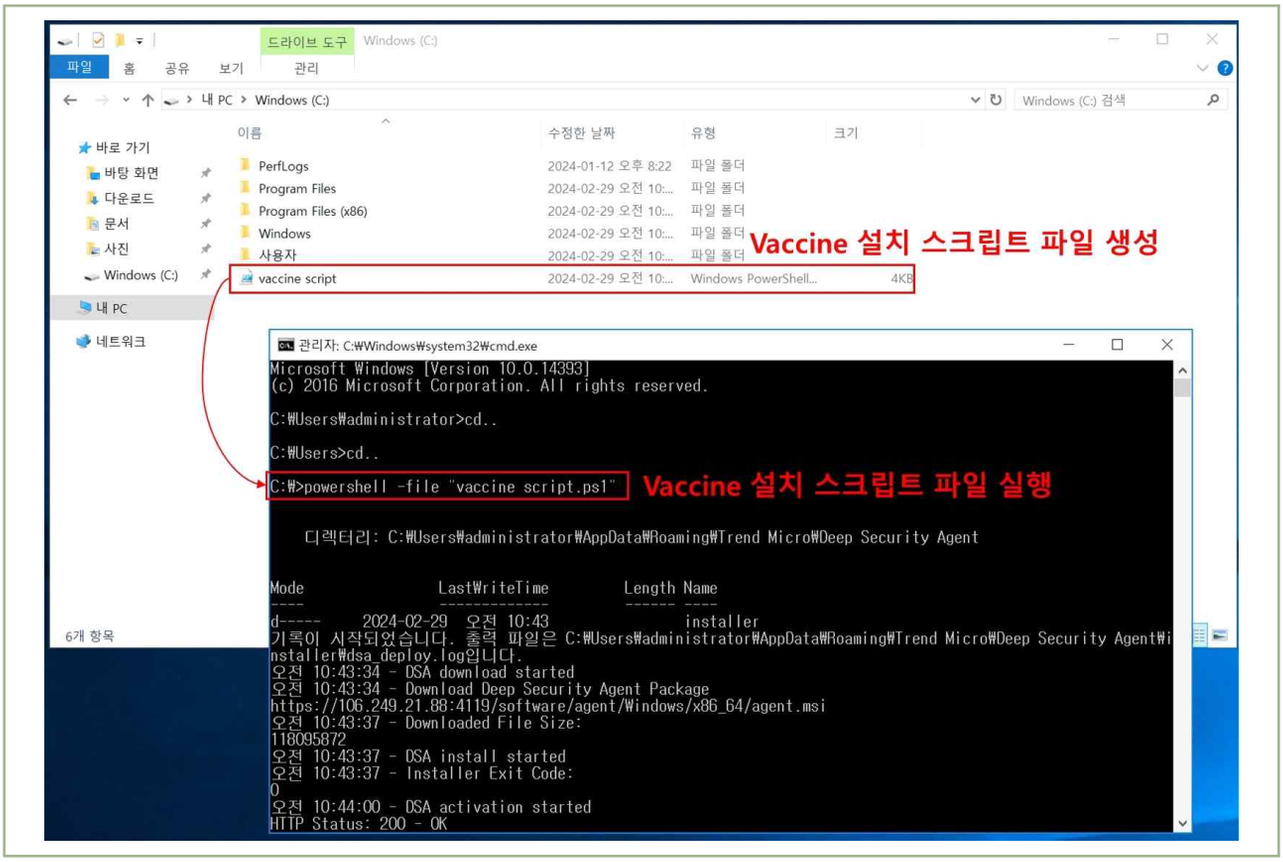


| 그림 1-7-4 | Vaccine agent 설치 스크립트 실행

F. Console의 vaccine 서비스 창에서 instance에 설치된 현황을 확인할 수 있으며, '사용 시작'을 누르면 서비스 사용이 시작됩니다. 사용 종료를 누르면 서비스 사용이 중지되며, 필요 시 agent를 삭제할 수 있습니다.

② Windows 시스템 백신 설치

A. Windows의 경우 스크립트 파일을 생성하여, console에서 복사한 스크립트를 저장한 후, 파일을 실행합니다.



| 그림 1-7-5 | Windows에서 vaccine 설치하기

B. '파일 복원', '에이전트 상태 체크', '분석 요청', '이미지 복제 시 가이드' 등의 내용은 'NHN Cloud 사용 가이드(Vaccine)'에 자세히 설명되어 있습니다.

4 참고 사항

- 백신 서비스 중 Ahnlab CPP 서비스의 경우에는 서비스 게이트웨이에 연결하여 클라이언트와 Vaccine 서버가 외부 인터넷을 경유하지 않고, 내부 네트워크로 통신할 수 있습니다.
  [Network 〉〉 Service Gateway]에서 서비스를 Vaccine으로 선택하면 Vaccine 서비스 게이트웨이가 생성되며, 해당 게이트웨이를 통해 내부 네트워크로 통신하게 됩니다.
- NHN Cloud 마켓플레이스

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 구성하여야 한다.** *** 개발, 운영, 업무 등**

2 설명

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

  - 예시

    1) 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)

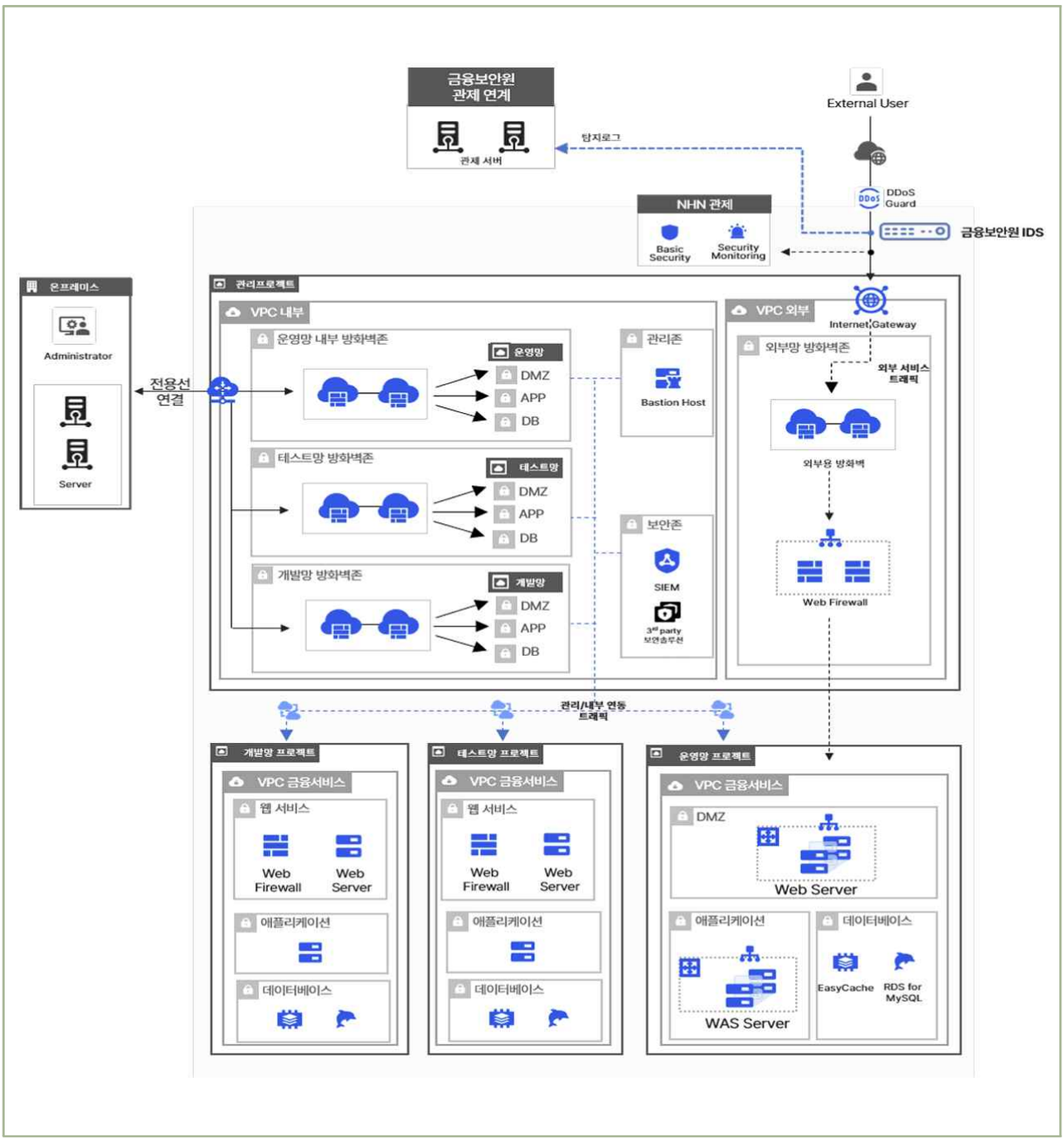
3 우수 사례

- **(가상자원관리시스템)**

  NHN Cloud에는 네트워크를 분리할 수 있는 서비스를 제공하고 있습니다. 이번 챕터에서는 네트워크 분리 서비스 및 분리된 네트워크를 연결하는 방법에 대해 알아봅니다.

  ① 프로젝트, VPC, subnet을 이용하여 네트워크 분리 구성

  A. NHN Cloud에서 제공하는 프로젝트, VPC, subnet의 서비스를 이용하여 네트워크를 분리 구성할 수 있습니다.



| 그림 2-1-1 | 금융 서비스 네트워크 아키텍처

B. '그림 2-1-1 금융 서비스 네트워크 아키텍처'에서 관리, 개발, 운영, 테스트망으로 네트워크를 크게 분리하고, VPC, subnet 서비스를 이용하여 자원에 따라 분리 배치하였으며, NHN Cloud의 VPC, subnet, peering gateway 등의 서비스를 통해 위 네트워크를 구성할 수 있습니다. (그림은 「NHN Cloud 네트워크 아키텍처 보안가이드」에서 발췌하였습니다.)

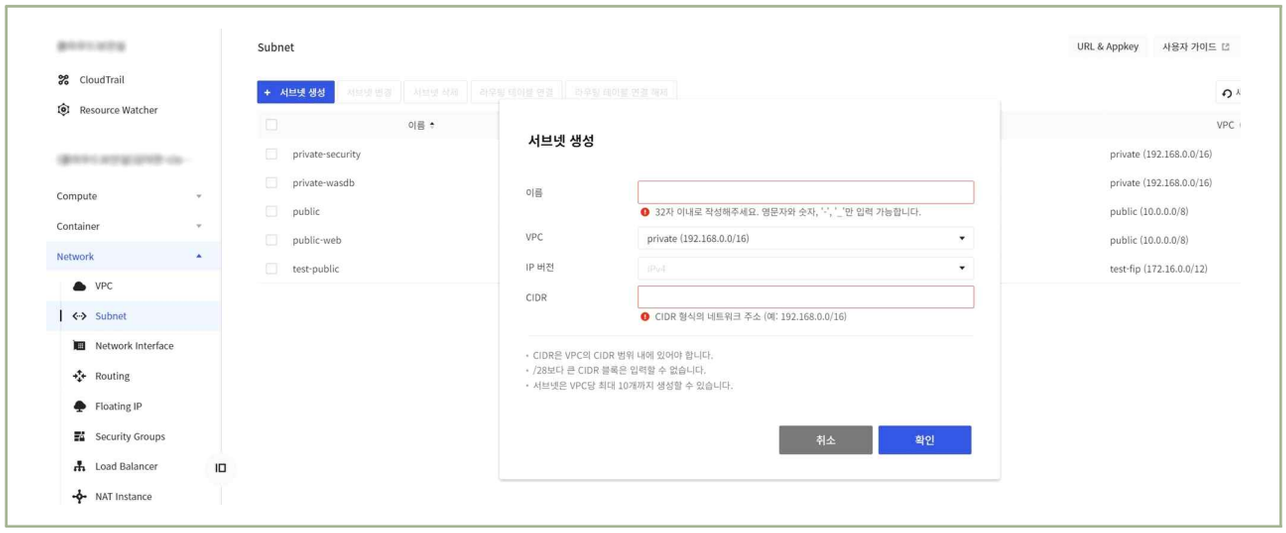
C. VPC의 경우 [Network 〉〉 VPC]에서 생성하고 관리할 수 있습니다.

| 그림 2-1-2 | VPC 생성 화면

D. VPC의 CIDR은 사설 IP 대역으로만 입력이 가능합니다.

E. Subnet의 경우 [Network 〉〉 subnet] 에서 생성하고 관리할 수 있습니다.

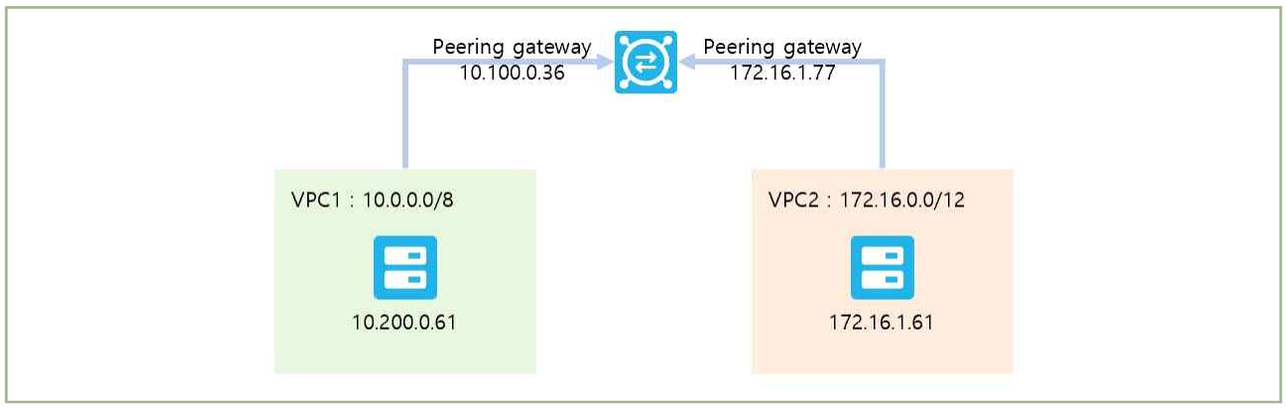
F. 계획된 네트워크 구성도를 바탕으로 VPC 및 subnet을 구성합니다.



| 그림 2-1-3 | Subnet 생성 화면

② Peering gateway를 이용하여 분리된 네트워크 연결

A. '그림 2-1-1 금융 서비스 네트워크 아키텍처'에서 '프로젝트-프로젝트', 'VPC-VPC' 간에는 peering 서비스로 서로 네트워크를 연결하고 있습니다.

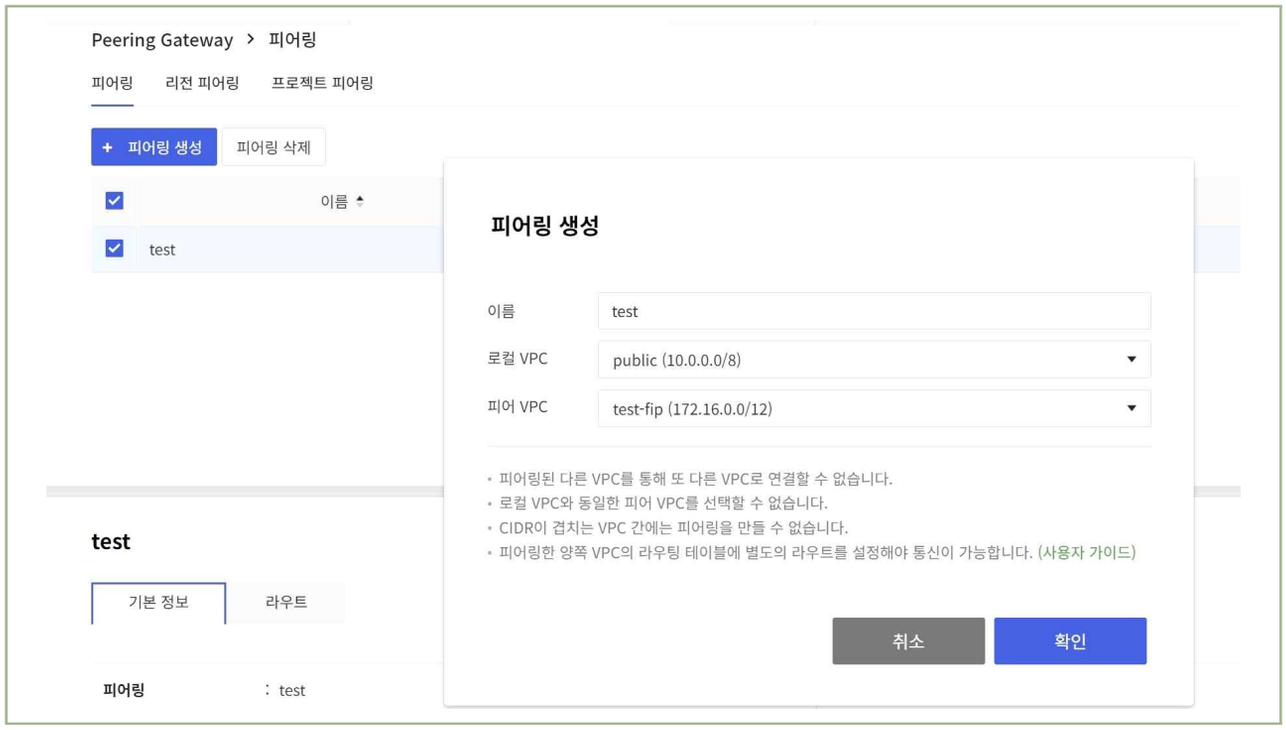


| 그림 2-1-4 | VPC Peering 구조도

B. 아래에서 설명할 VPC Peering의 구조는 '그림 2-1-4 VPC Peering 구조도'와 같습니다.

※ Peering gateway IP는 별도로 지정할 수 없습니다.

C. Peering은 [Network 〉〉 Peering Gateway] 에서 생성하고 관리할 수 있습니다.



| 그림 2-1-5 | VPC Peering 설정

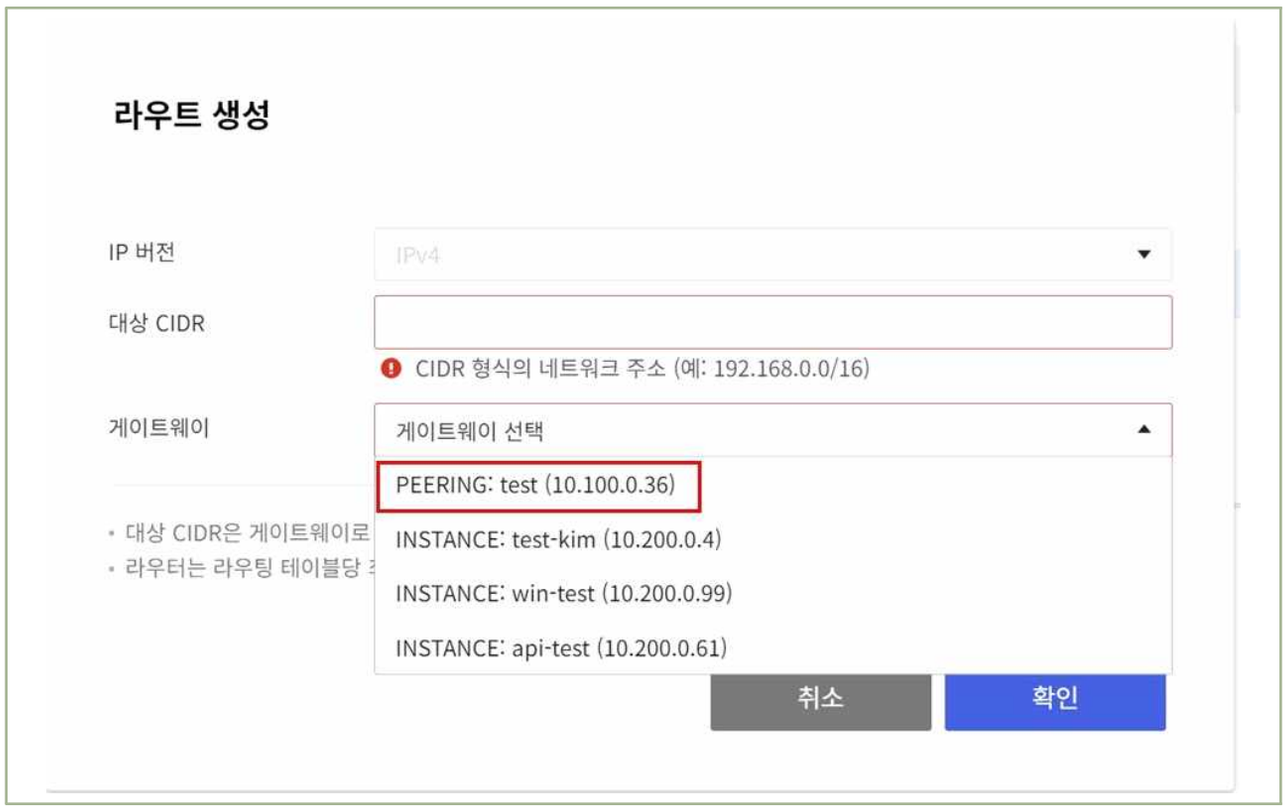
D. '그림 2-1-5 VPC Peering 설정'은 public VPC (10.0.0.0/8)와 private VPC (172.16.0.0/12)간의 peering을 생성하는 화면입니다.

※ Peering한 VPC를 통해 또 다른 VPC로 연결할 수는 없으며, CIDR가 겹치는 VPC 간에도 peering을 만들 수 없습니다. 또한 양쪽 VPC의 Routing Table에 별도의 Route를 설정하여야 통신이 가능합니다.

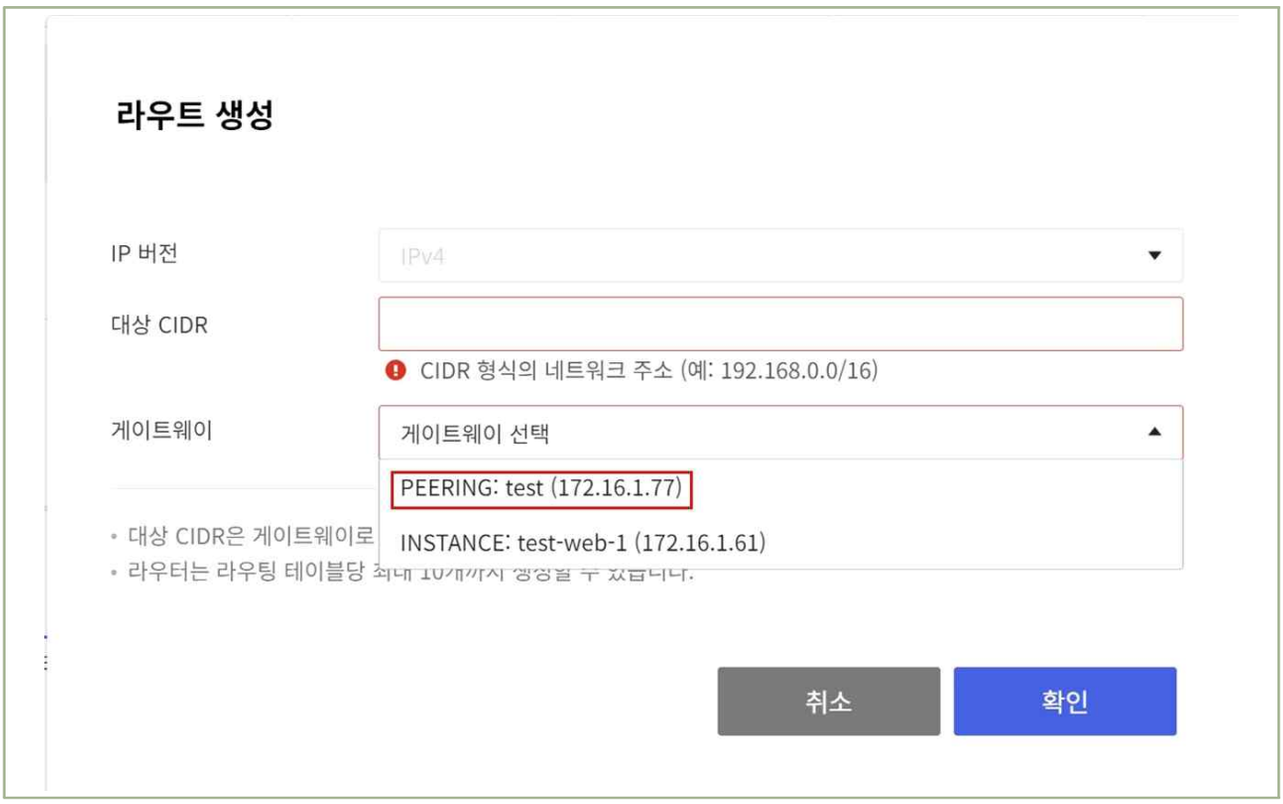
E. Peering을 생성한 후 [Network 〉〉 Routing] 에서 라우트를 생성해야 합니다.

F. 라우트는 VPC1와 VPC2 양쪽에 설정해줘야 하며, peering을 생성했다면 라우트 게이트웨이 내 'PEERING'이 생성된 것을 확인할 수 있습니다.

'그림 2-1-6 Peering(VPC1)에 대한 Route 생성'은 10.0.0.0/8 VPC의 라우트 생성 화면입니다. 10.100.0.36의 peering gateway가 생성된 것을 확인할 수 있으며, 반대쪽 VPC인 172.16.0.0/12에도 '그림 2-1-7 Peering(VPC2)에 대한 Route 생성'에서와 같이 172.16.1.77이 peering gateway로 생성된 것을 확인할 수 있습니다.

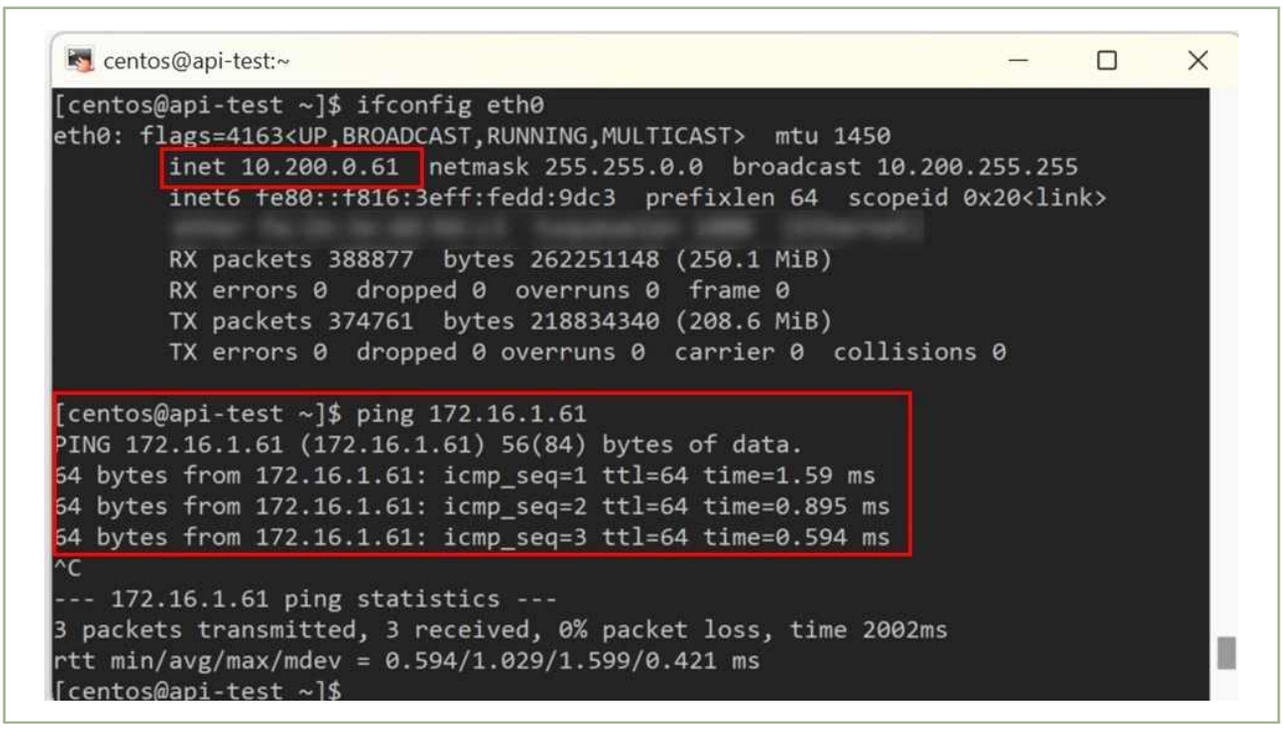


| 그림 2-1-6 | Peering(VPC1)에 대한 Route 생성



| 그림 2-1-7 | Peering(VPC2)에 대한 Route 생성

G. VPC1,2에 라우트 생성이 완료되면 VPC간 통신이 연결되는 것을 확인할 수 있습니다.



| 그림 2-1-8 | peering 통신 확인

(API)

① VPC 생성하기

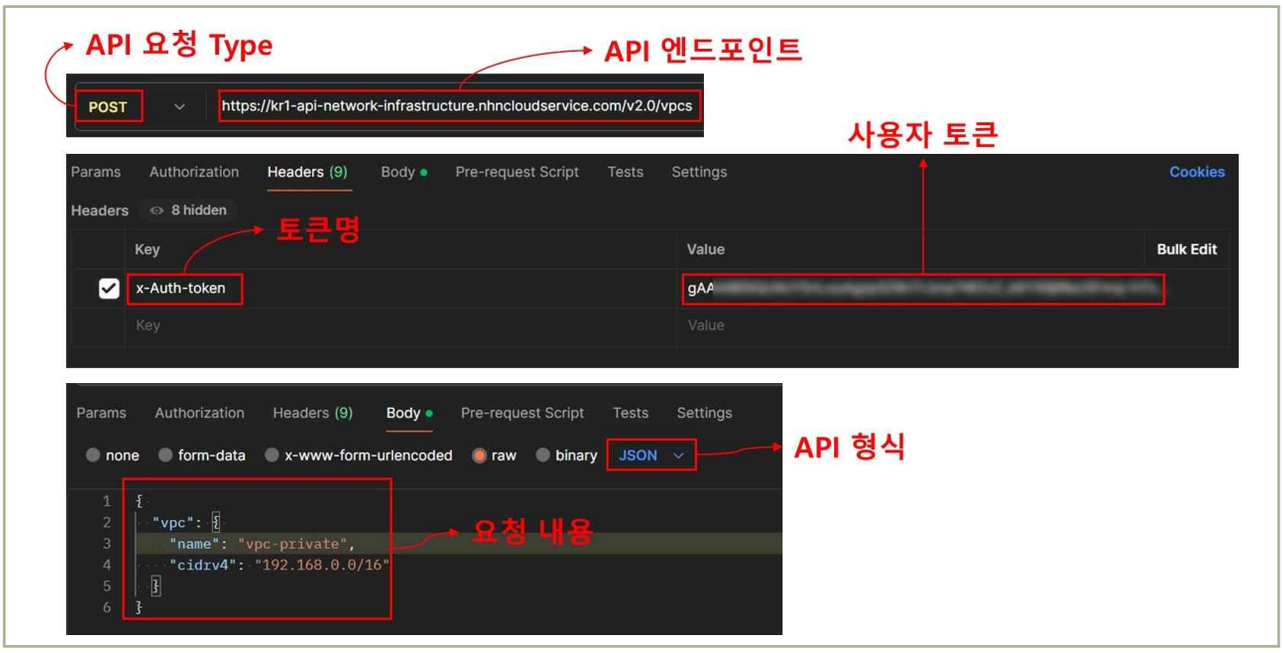
A. API를 이용하여 VPC를 생성하려면 API 엔드포인트와 토큰이 필요합니다.

B. API 엔드포인트는 NHN Cloud 홈페이지 사용자가이드에서 확인할 수 있으며, 토큰은 '1.5 가상자원 접속 시 보안 방안 수립'을 참조하여 생성합니다.

C. 사용자가이드(VPC API)에서 API 요청 Type 및 API 엔드포인트를 확인한 후 요청 예시를 참고합니다.

| 그림 2-1-9 | VPC 생성 API 예시

D. '그림 2-1-9 VPC 생성 API 예시'를 바탕으로 API를 작성합니다.



| 그림 2-1-10 | VPC 생성 API 요청문

E. 요청 결과를 확인합니다.

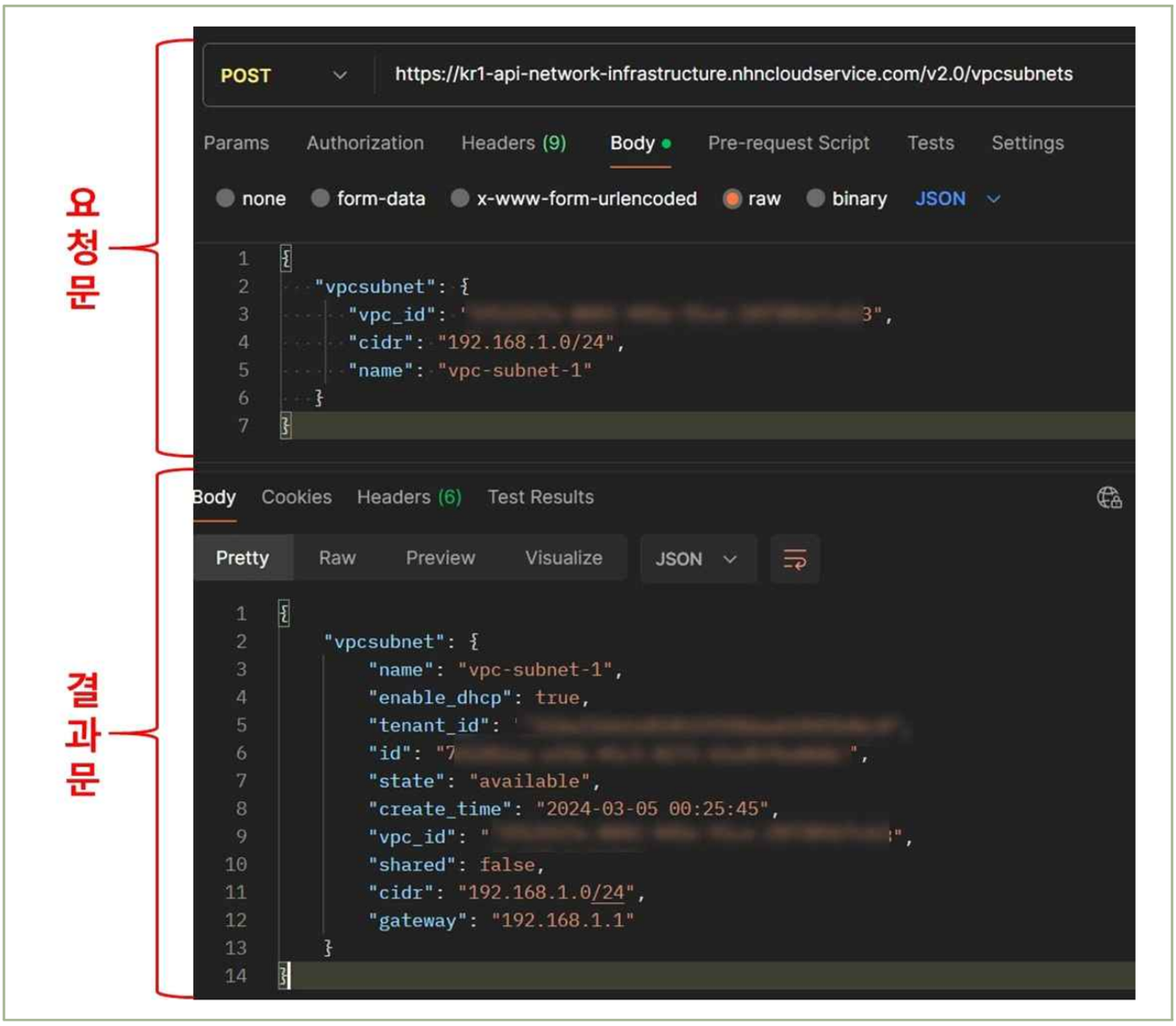
| 그림 2-1-11 | VPC 생성 결과 확인

② Subnet 생성하기

A. 사용자가이드에서 subnet 생성 API 예시를 확인합니다.

| 그림 2-1-12 | Subnet 생성 API 예시

B. '그림 2-1-12 Subnet 생성 API 예시'를 바탕으로 API를 작성하고, 결과를 확인합니다.



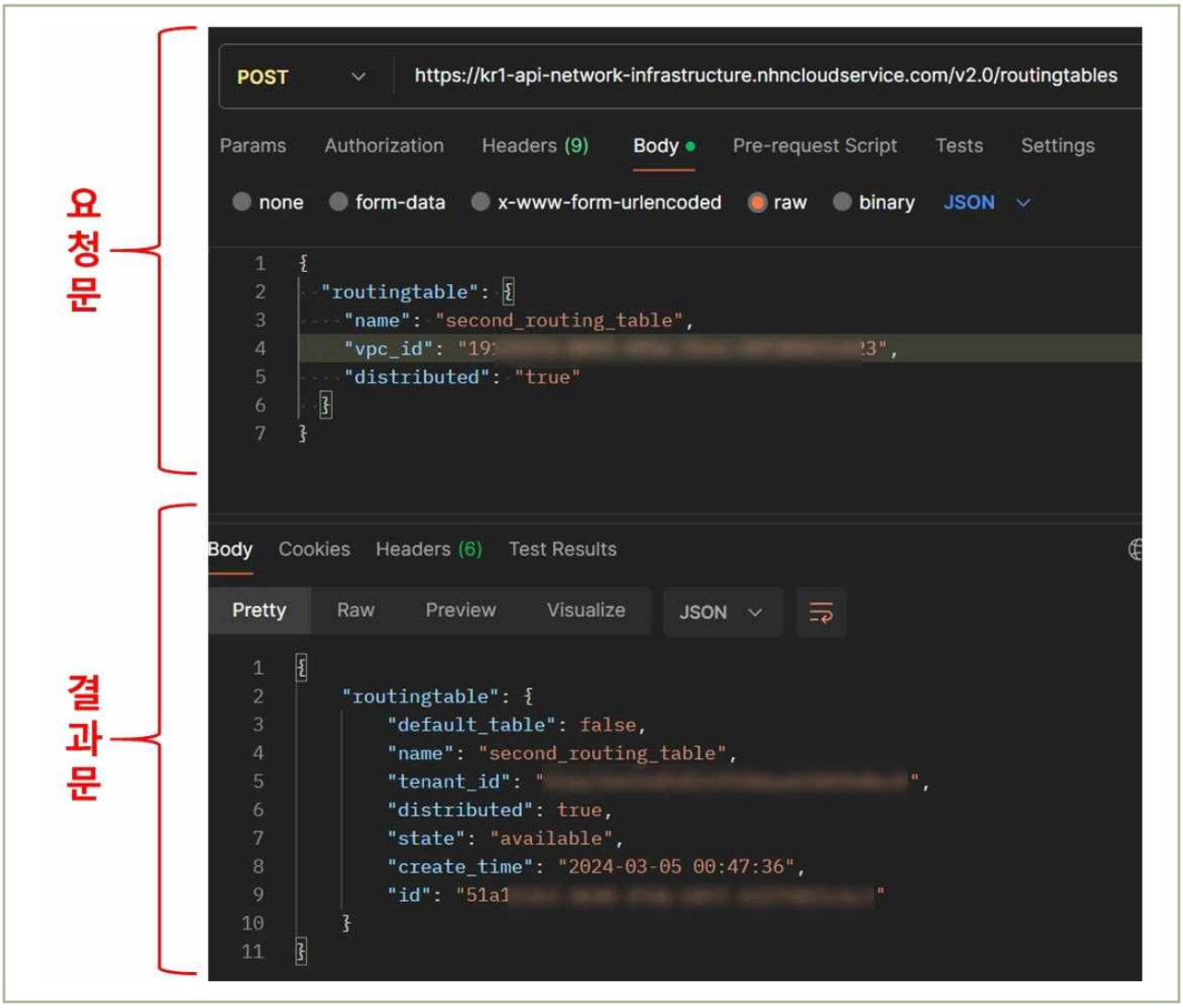
| 그림 2-1-13 | Subnet 생성 API 요청문 및 결과문

③ 라우팅 테이블 생성하기

A. 사용자가이드에서 라우팅 테이블 생성 API 예시를 확인합니다.

| 그림 2-1-14 | 라우팅 테이블 생성 API 예시

B. '그림 2-1-14 라우팅 테이블 생성 API 예시'를 바탕으로 API를 작성하고, 결과를 확인합니다.



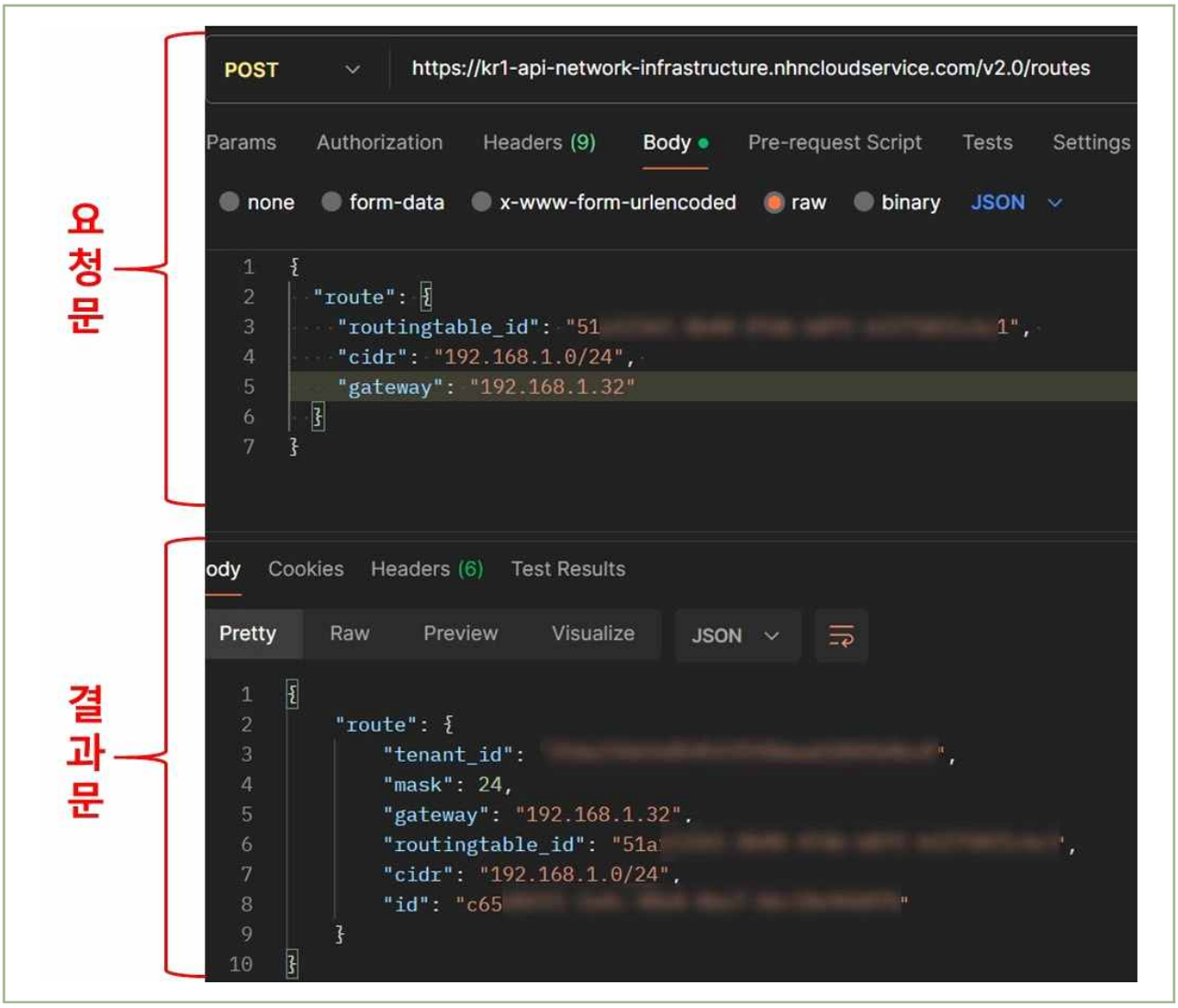
| 그림 2-1-15 | 라우팅 테이블 생성 API 요청문 및 결과문

④ 라우트 생성하기

A. 사용자가이드에서 라우트 생성 API 예시를 확인합니다.

| 그림 2-1-16 | 라우트 생성 API 예시

B. ‘그림 2-1-16 라우트 생성 API 예시’를 바탕으로 API를 작성하고, 결과를 확인합니다.



| 그림 2-1-17 | 라우트 생성 API 요청문 및 결과문

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

- **(가상자원관리시스템)**

  '2.1 업무 목적에 따른 네트워크 구성' 항목에서 VPC, subnet 등 네트워크를 분리 구성할 수 있는 서비스에 대해 확인하였습니다.

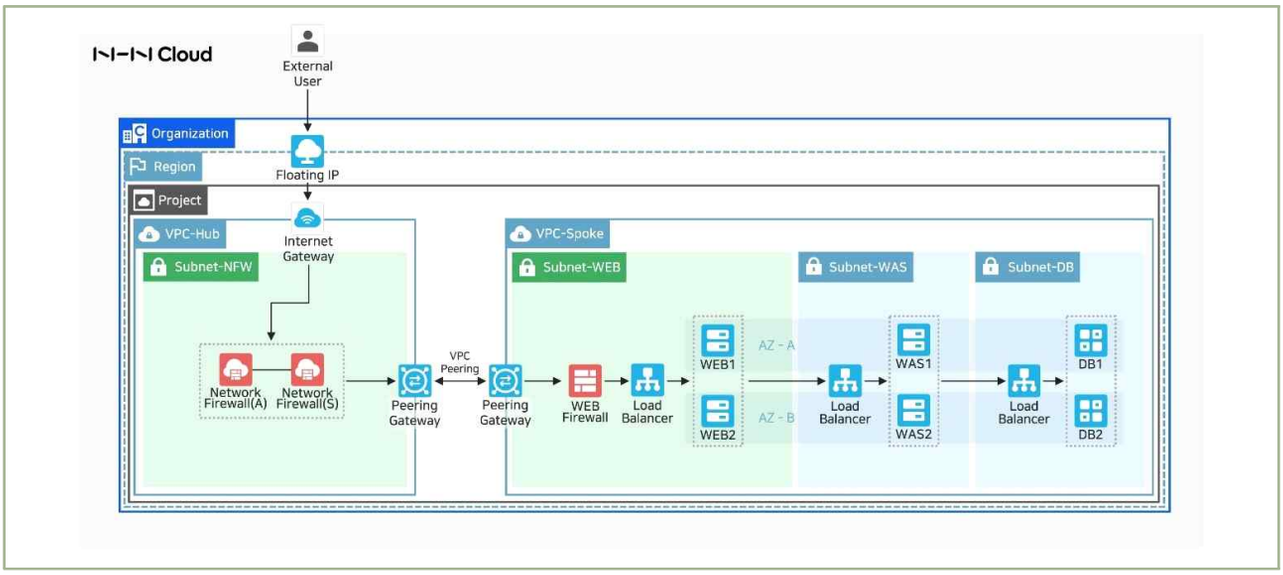
  '2.2 내부망 네트워크 보안 통제'에서는 VPC 내 네트워크를 안전하게 보호하기 위한 Network Firewall에 대해 알아보겠습니다.

  ① Network Firewall 생성하기

  - NHN Cloud에서는 Network Firewall 서비스를 이용하여 내부 네트워크에 보안 통제를 적용할 수 있습니다.

    '사용자가이드(Network Firewall)'에서는 1개의 프로젝트, 1개 이상의 프로젝트, 다른 리전 간 프로젝트 등 5개의 서비스 구성도를 제시하고 있습니다.

    네트워크 설계 시 해당 구성도를 참조할 수 있습니다.

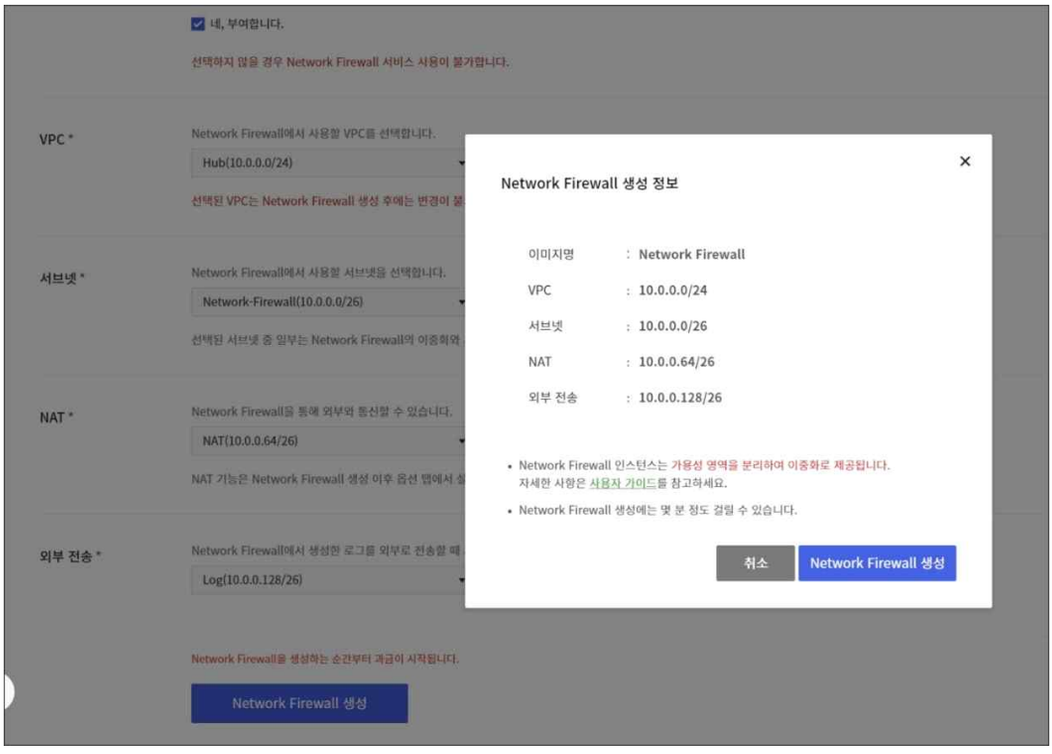


| 그림 2-2-1 | Network Firewall 서비스 구성도 예시(사용자가이드 참조)

A. [Security 〉〉 Network Firewall] 메뉴로 이동합니다.

B. 각 필수 항목을 모두 선택하고 Network Firewall 생성을 클릭합니다.

※ Network Firewall 인스턴스는 기본적으로 가용 영역을 분리하여 이중화를 제공하고 있습니다.



| 그림 2-2-2 | Network Firewall 생성 정보

C. Network Firewall은 '정책', '객체', 'NAT', '로그', '모니터', '옵션'의 탭에서 각 기능을 제공하고 있으며, 탭 별 기능은 '사용자 가이드(Network Firewall)'를 참고하시기 바랍니다.

| 그림 2-2-3 | Network Firewall 세부 메뉴

② Hub - Spoke VPC 간 연결 설정하기

A. [Network 〉〉 Routing]으로 이동하여 Spoke VPC를 선택한 후 라우팅 테이블 변경을 클릭합니다.

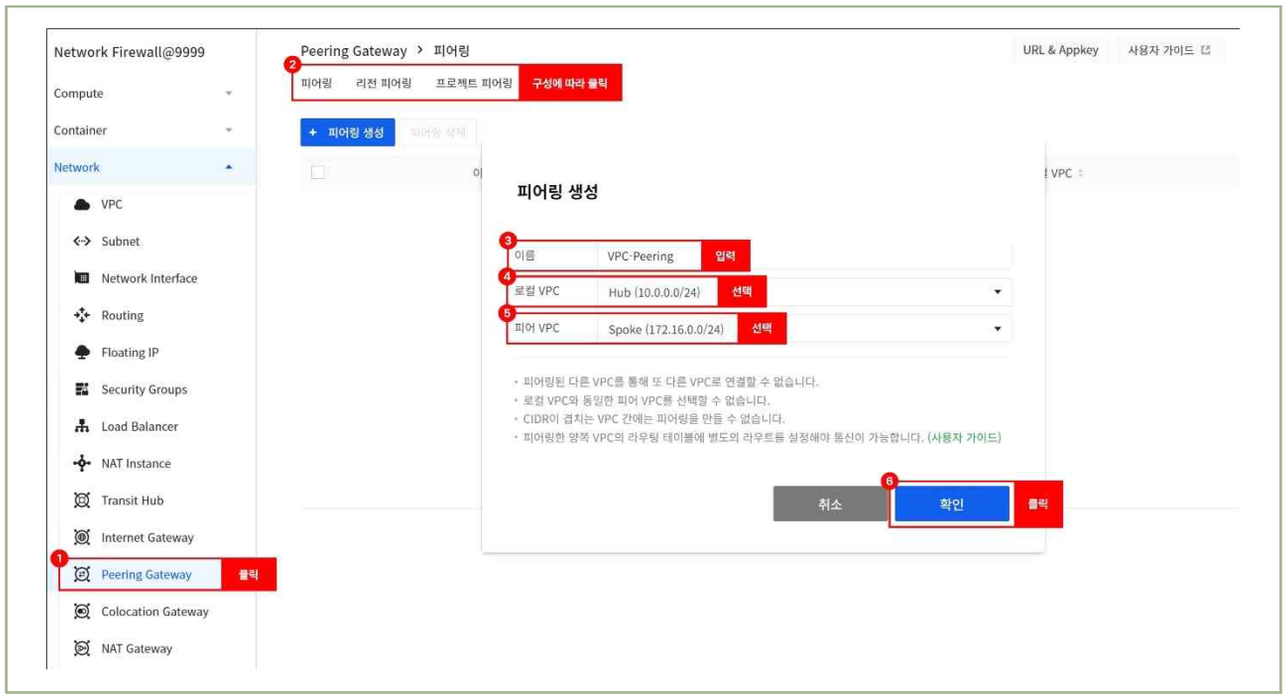
| 그림 2-2-4 | Spoke VPC 라우팅 테이블 변경

B. 라우팅 테이블 변경 탭에서 라우팅 방식을 '중앙 집중형 라우팅(CVR)'로 변경합니다.

| 그림 2-2-5 | 중앙 집중형 라우팅(CVR)로 라우팅 테이블 변경

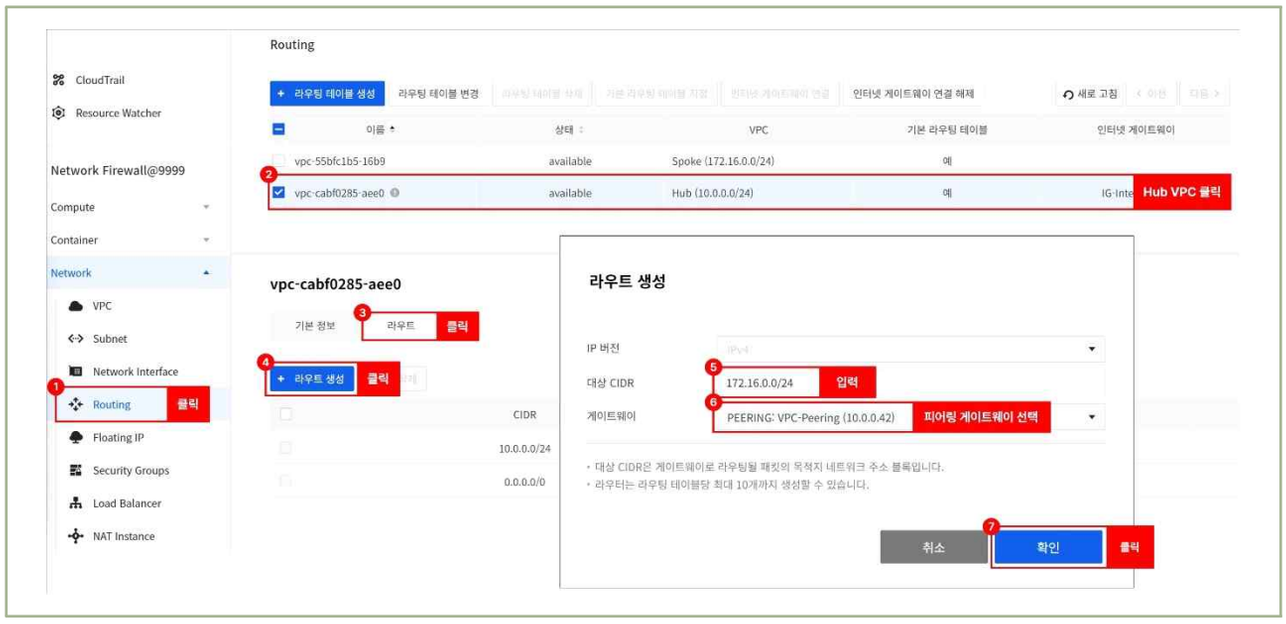
C. [Network 〉〉 Peering Gateway]로 이동하여 피어링을 생성합니다.

가) Spoke VPC가 같은 프로젝트라면 피어링을 생성하고, 다른 프로젝트라면 프로젝트 피어링을 생성합니다. 마찬가지로 다른 리전이라면 리전 피어링을 생성합니다.



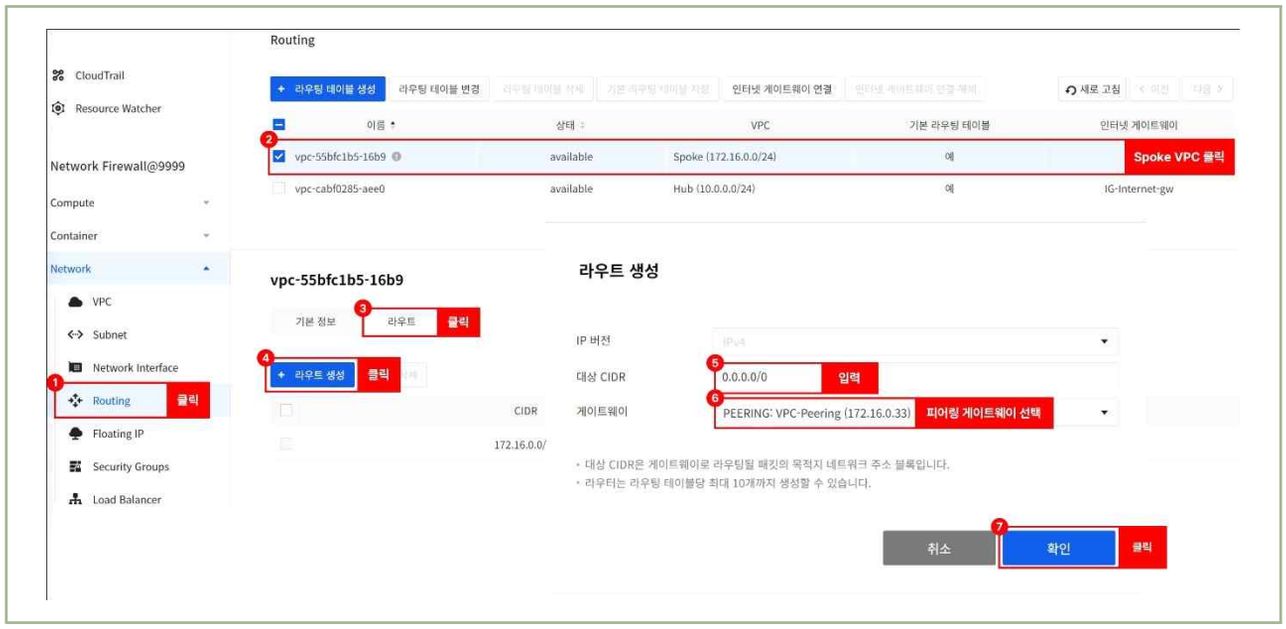
| 그림 2-2-6 | Network Firewall 연결을 위한 피어링 생성

D. [Network 〉〉 Routing]으로 이동하여 Hub VPC를 선택한 후 아래의 라우팅을 설정합니다.



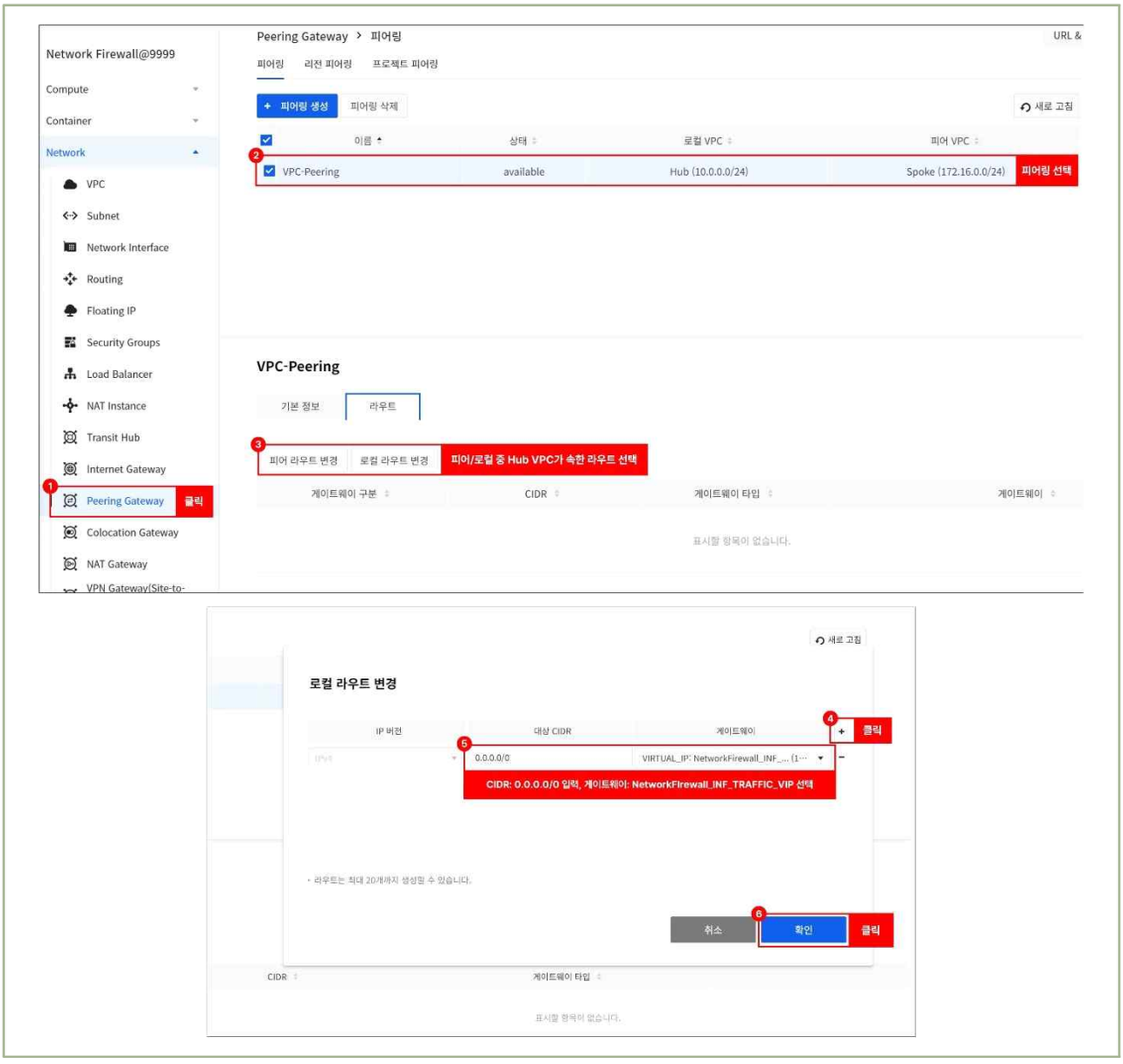
| 그림 2-2-7 | Hub VPC 라우트 설정

E. Spoke VPC를 선택한 후 아래의 라우팅을 설정합니다.



| 그림 2-2-8 | Spoke VPC 라우트 설정

F. [Network 〉〉 Peering Gateway]로 이동하여 라우팅을 설정합니다.



| 그림 2-2-9 | Network Firewall 경유 라우트 설정

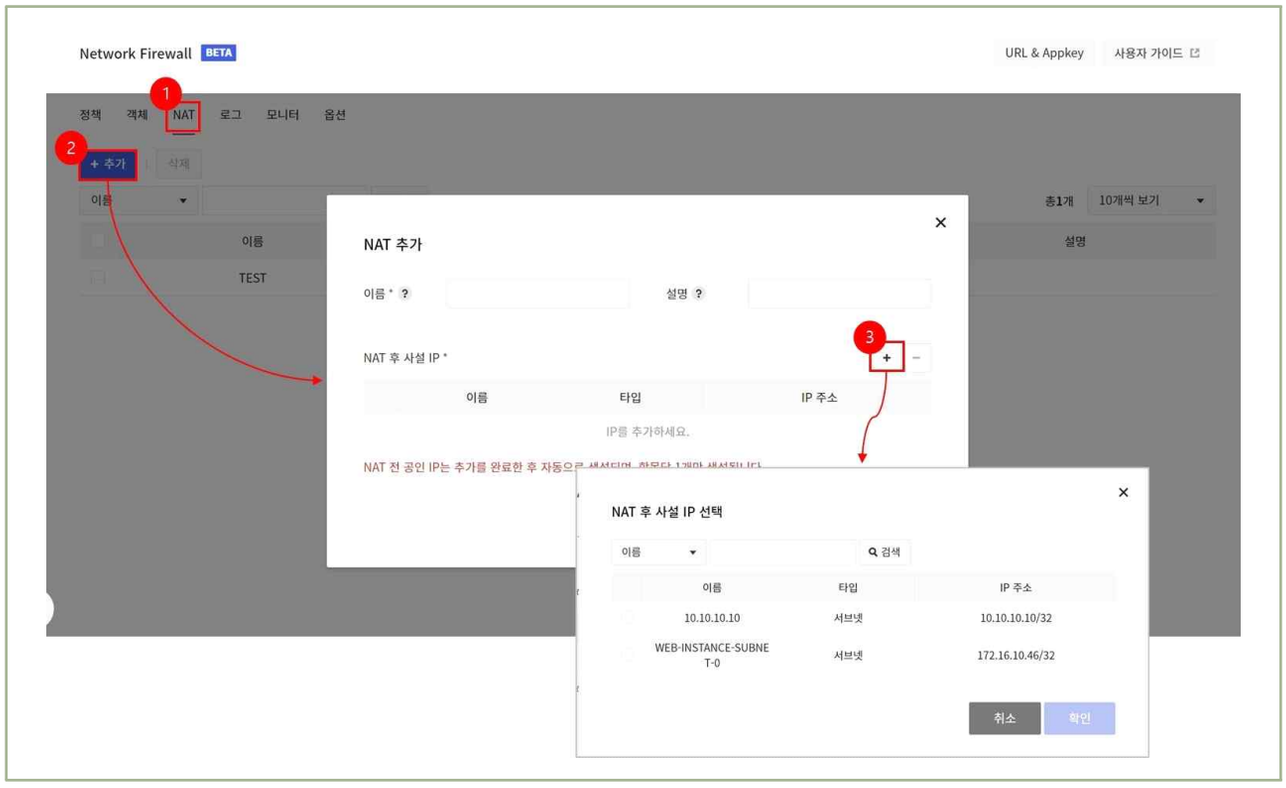
G. '그림 2-2-9 Network Firewall 경유 라우트 설정'에서와 같이 Hub VPC에 Network Firewall을 게이트웨이로 지정하는 라우트를 생성하면, Spoke VPC에 있는 인스턴스가 공인 통신을 하는 경우 Network Firewall을 경유하게 됩니다.

가) 공인 통신 필요 시 [Security 〉〉 Network Firewall] NAT 탭에서 NAT 추가가 필요합니다.

③ NAT 설정하기

A. Network Firewall의 NAT는 외부에서 접속할 인스턴스를 지정하여 전용 공인 IP를 생성하는 기능으로, 1:1 방식만 제공하며, port 기반 NAT는 제공하지 않습니다.

B. [Security 〉〉 Network Firewall] NAT를 클릭하고, 추가를 클릭하여 NAT 설정을 진행합니다.



| 그림 2-2-10 | NAT 추가 설정

C. ‘NAT 후 사설 IP’를 선택하면 NAT가 설정된 공인 IP가 생성됩니다.

4 참고 사항

- Network Firewall의 다양한 구성 사례 및 로그 연동 구성 등은 「NHN Cloud 네트워크 아키텍처 보안가이드」에 작성되어 있습니다.
- 마켓플레이스 내 3rd-party 「방화벽 솔루션」을 사용하면 네트워크간 송·수신 등의 통제 정책 적용이 가능합니다.
- NHN Cloud 마켓플레이스

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

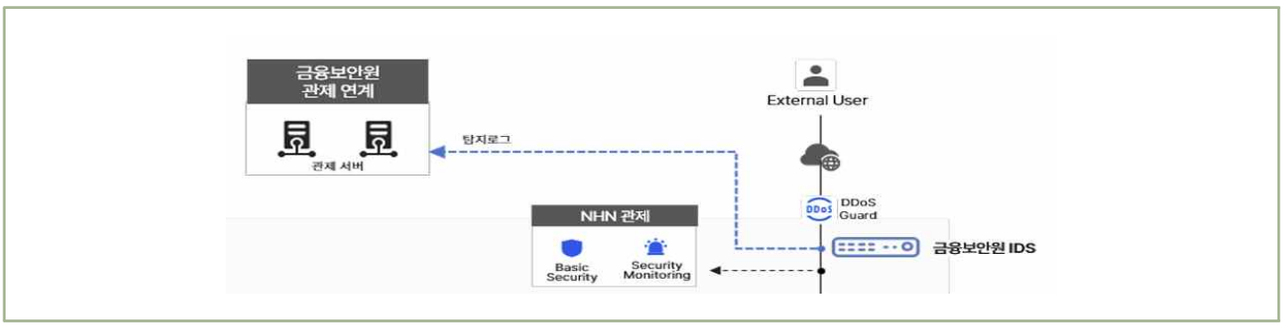
3 우수 사례

- **(가상자원관리시스템)**

  ① 금융보안원 통합보안관제 서비스 이용하기

  A. NHN Cloud의 국내 리전을 이용하는 경우 금융보안원의 통합보안관제를 신청하고 서비스를 제공받을 수 있습니다.

  B. 서비스는 FIP를 기준으로 제공되며, 금융보안원에 서비스를 신청하면, 해당되는 FIP 트래픽을 금융보안원 보안관제 장비로 전송합니다.



| 그림 2-3-1 | NHN Cloud 관제서비스 구성

C. '그림 2-3-1 NHN Cloud 관제서비스 구성'은 관제 서비스를 위한 NHN Cloud의 구성을 보여주고 있습니다.

D. 금융보안원의 IDS가 NHN Cloud의 트래픽 인입로에 위치해 있고, 해당 IDS에서 탐지한 이벤트로그를 통합보안관제센터에 전송하여 금융보안원의 관제 서비스를 제공받을 수 있습니다.

다만 공인 IP 변경 시 별도 안내가 반드시 필요합니다. 공인 IP 변경 미 통보 시 관제 누락 등에 대한 책임은 지지 않습니다.

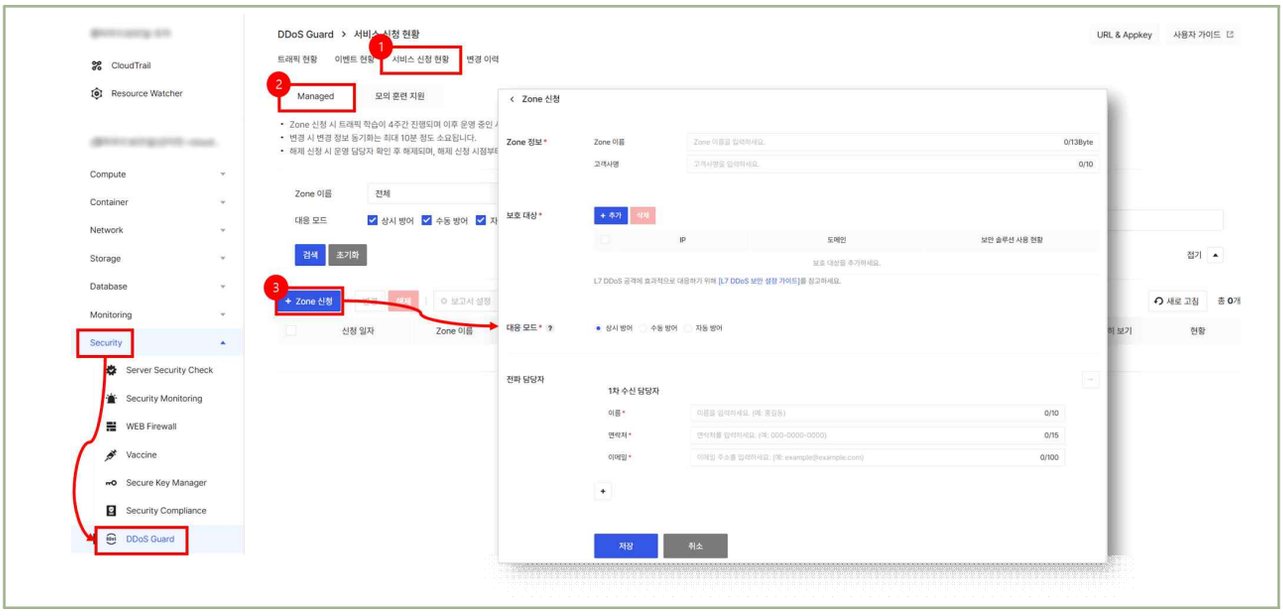
※ 서비스 신청 및 기타 문의는 금융보안원의 금융분야 정보공유분석센터 (금융 ISAC)로 문의하여 확인

E. 금보원의 보안관제 데이터 전송 방식은 물리 방식과 가상 방식으로 구분할 수 있습니다. 위에서 설명드린 방식은 물리 방식으로 만약 가상 방식으로 관제 데이터를 전송하고자 하는 경우 사업담당자를 통해 별도 협의 요청 부탁드립니다.

② NHN Cloud 서비스(DDoS GUARD) 이용하기

A. NHN Cloud의 서비스를 이용하여 DDoS 공격을 방어하고, 그 리포트를 제공받을 수 있습니다.

B. DDoS GUARD Basic 서비스는 무료로 제공되며, Managed 서비스의 경우에는 [프로젝트 〉〉 Security 〉〉 DDoS Guard 〉〉 서비스 신청 현황] 탭에서 서비스 신청이 가능합니다.



| 그림 2-3-2 | DDoS Guard Managed 서비스 신청

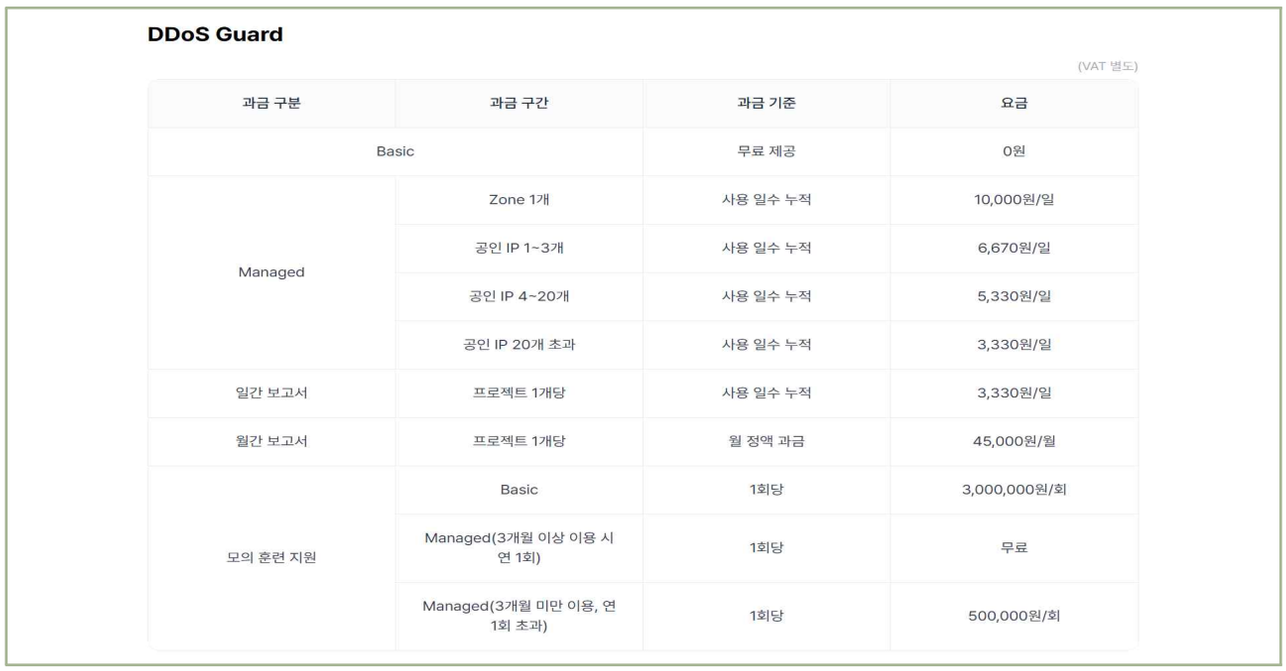
ㄱ. Zone 내에 여러 개의 보호대상(도메인)을 입력할 수 있으며, Zone을 여러 개 생성하여 Zone별로 임계치 등을 상이하게 적용할 수도 있습니다.

ㄴ. 추가로 L7 DDoS 공격에 효과적으로 대응하기 위해 Load Balancer, Nginx, Apache에

보안 설정을 고려할 수 있습니다. 설정 방법은 L7 DDoS 보안 설정 가이드를 참고하여 설정합니다.

ㄷ. 대응 모드에는 항상 DDoS 필터링을 적용하는 '상시 방어', NHN Cloud의 관제센터 담당자가 확인 후 수동으로 방어 모드 적용하는 '수동 방어', 관제시스템에서 자동 대응 후 담당자 전파를 수행하는 '자동 방어' 세가지 모드 중 선택하여 운영할 수 있습니다.

C. Managed 서비스의 경우 트래픽 학습 기반 임계치 설정 등 맞춤형 DDoS 정책 설정/관리가 가능하며, DDoS 상세 공격 정보 전파, 보고서 제공 등의 서비스를 제공합니다.



DDoS Guard

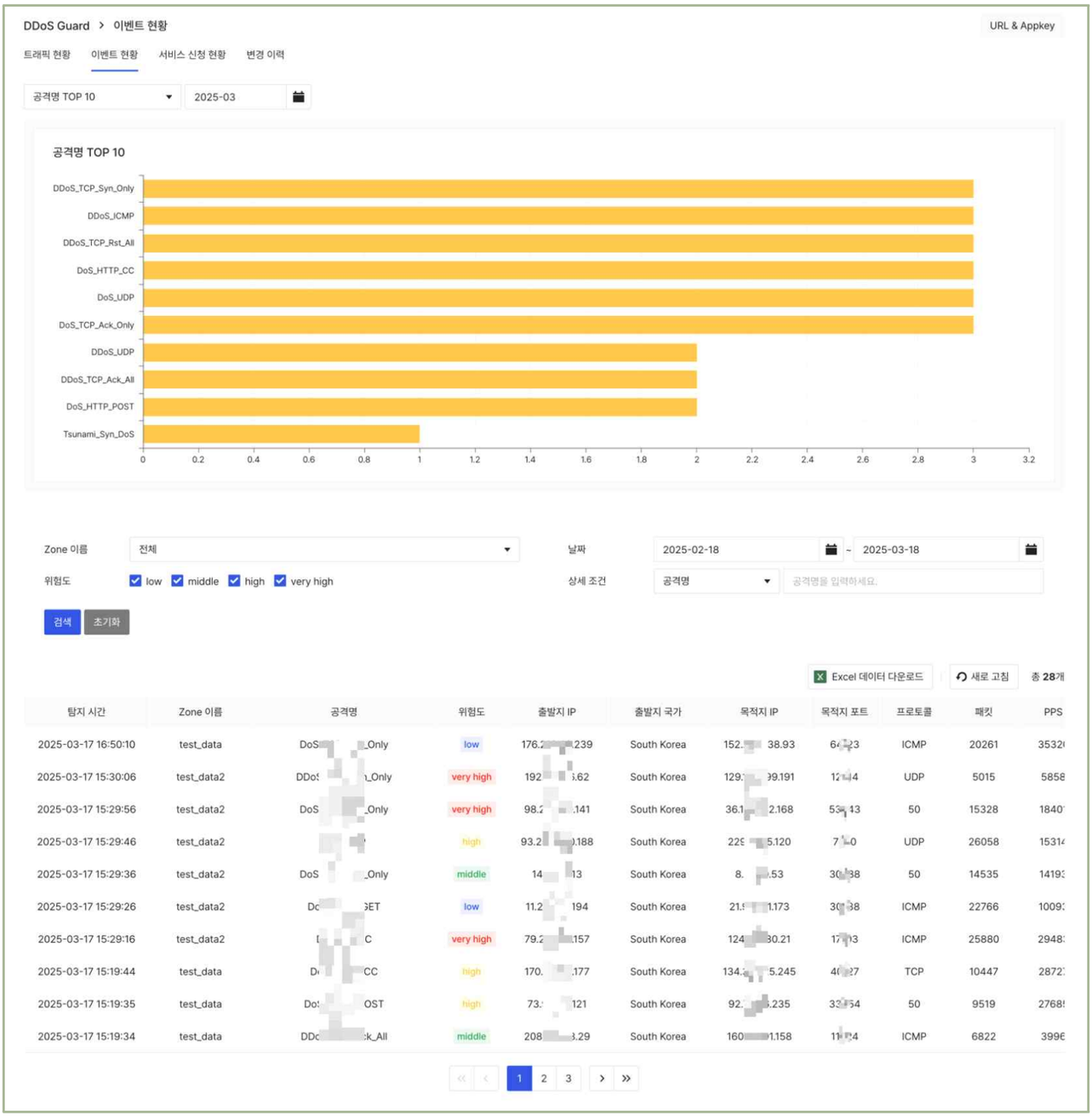
(VAT 별도)

과금 구분	과금 구간	과금 기준	요금
Basic		무료 제공	0원
Managed	Zone 1개	사용 일수 누적	10,000원/일
	공인 IP 1~3개	사용 일수 누적	6,670원/일
	공인 IP 4~20개	사용 일수 누적	5,330원/일
	공인 IP 20개 초과	사용 일수 누적	3,330원/일
일간 보고서	프로젝트 1개당	사용 일수 누적	3,330원/일
월간 보고서	프로젝트 1개당	월 정액 과금	45,000원/월
모의 훈련 지원	Basic	1회당	3,000,000원/회
	Managed(3개월 이상 이용 시 연 1회)	1회당	무료
	Managed(3개월 미만 이용, 연 1회 초과)	1회당	500,000원/회

| 그림 2-3-3 | DDoS GUARD 제공 서비스별 요금 체계

D. 신청 등록 완료 후 별도 학습 과정을 거치게 되며, 수일 내 서비스 안내 메일이 발송됩니다. 메일에는 적용할 정책이 표기되며, 고객과 협의하에 정책을 적용합니다.

E. DDoS Guard 서비스를 이용하면 콘솔에서 트래픽 현황 및 이벤트 현황을 확인할 수 있습니다.

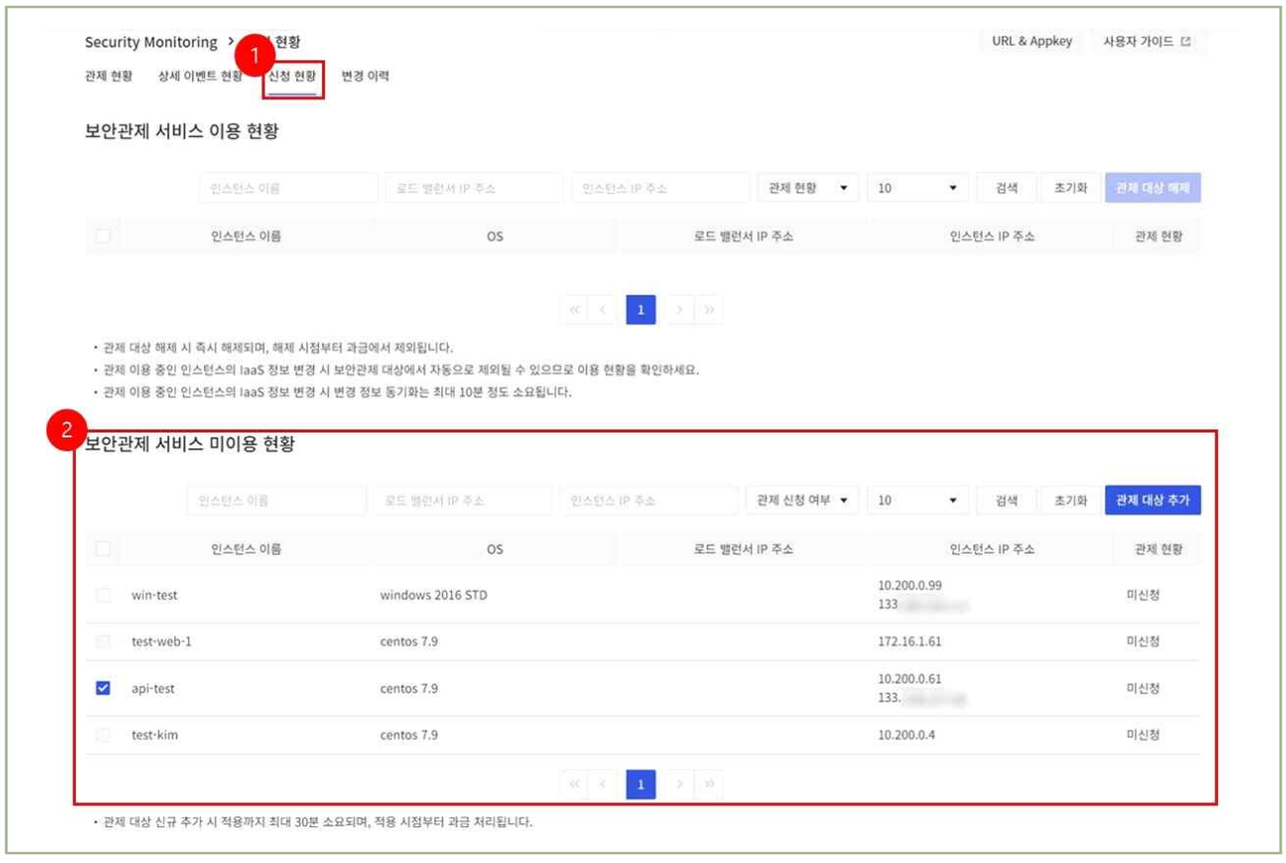


| 그림 2-3-4 | DDoS GUARD 이벤트 현황 제공 화면

③ NHN Cloud 서비스(Security Monitoring) 이용하기

A. NHN Cloud에서는 네트워크 트래픽 보안관제를 위한 IDS 서비스를 제공하고 있습니다.

B. [Security 〉〉 Security Monitoring]으로 이동하여 '신청 현황' 탭을 클릭하면, 보안관제 서비스 이용이 가능한 Instance 목록이 나타납니다.



| 그림 2-3-5 | Security Monitoring 서비스 신청 화면

가) FIP를 가지고 있는 Instance만 security monitoring 신청 및 서비스 이용이 가능합니다.

나) Load Balancer로 분산 구성한 경우 '동일 로드 밸런서 IP 주소'를 가지고 있는 자원은 같은 그룹으로 취급됩니다. 인스턴스 하나를 선택해도 동일한 로드 밸런서 IP 주소를 가진 자원은 같이 신청됩니다.

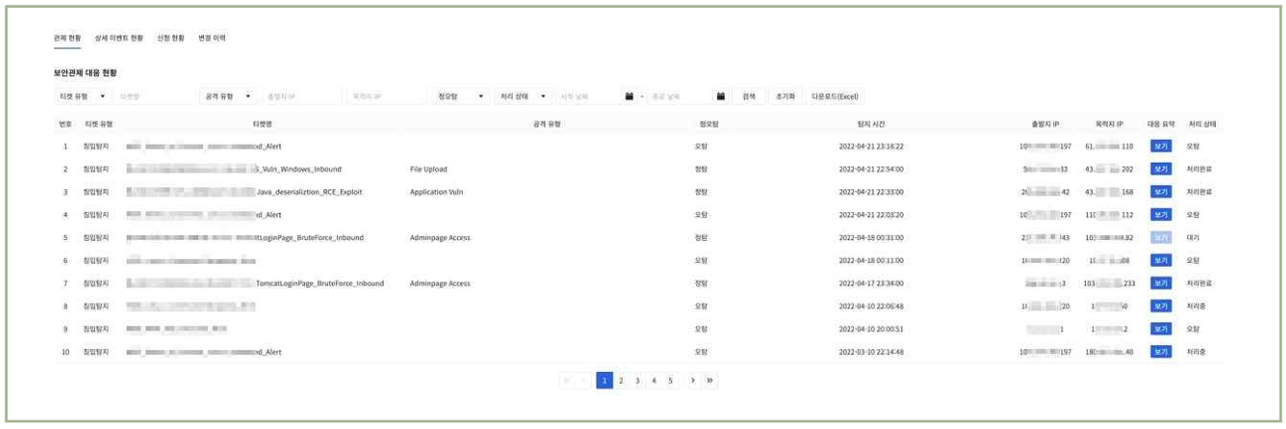
C. '관제 대상 추가'를 클릭하면 1시간 내 관제 서비스가 제공되며, 관제 대상 해제를 클릭하면 1시간 내 관제 서비스가 종료됩니다.

D. ‘신청 현황’ 탭에서 ‘보안관제 업무 수신 설정’을 할 수 있습니다.

전화번호를 입력하여 긴급 건 발생 시 유선 연락을 받거나, 메일 주소를 입력하여 업무 처리 내역에 대한 결과를 메일로 전달받을 수 있습니다.

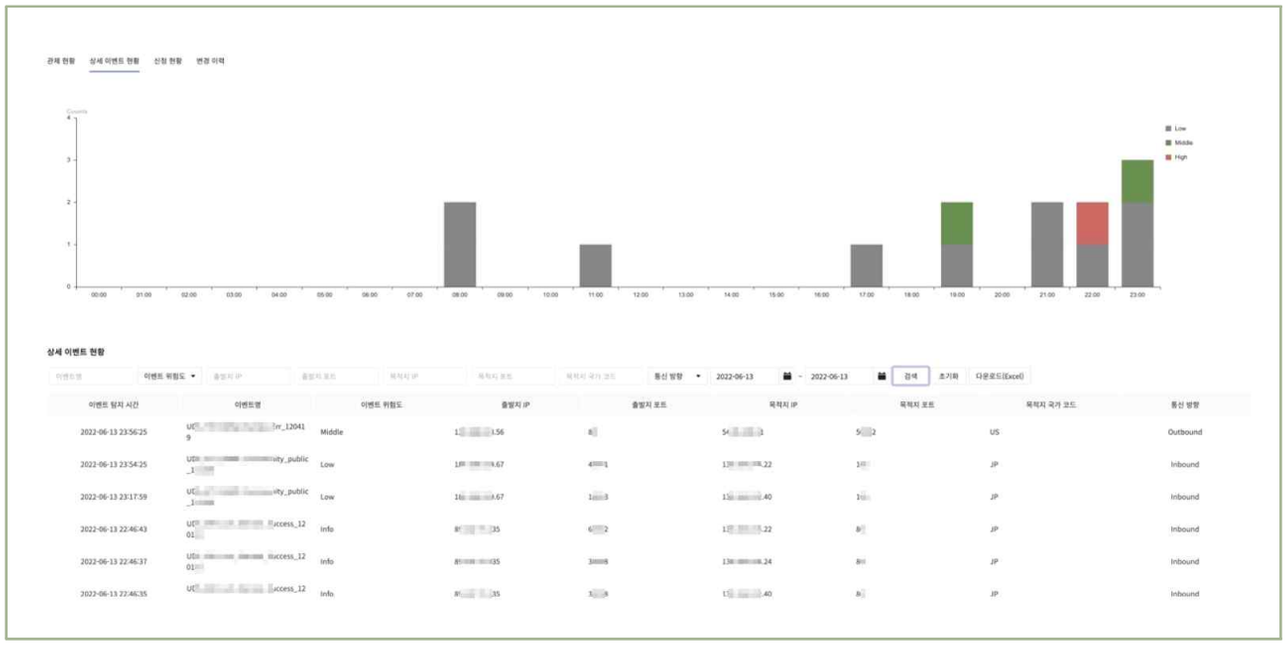
| 그림 2-3-6 | 보안관제 업무 수신 설정

E. ‘관제 현황’ 탭에서 최대 1년 내 보안관제 대응 현황을 확인할 수 있습니다.



| 그림 2-3-7 | 보안관제 대응 현황

F. ‘상세 이벤트 현황’ 탭에서 최대 3개월 내 상세한 이벤트 현황을 확인할 수 있습니다.



| 그림 2-3-8 | 상세 이벤트 현황

④ WAF 서비스 이용하기

A. NHN Cloud에서는 Web 공격에 대한 대응을 위해 WAF(Web Application Firewall) 서비스를 제공하고 있습니다.

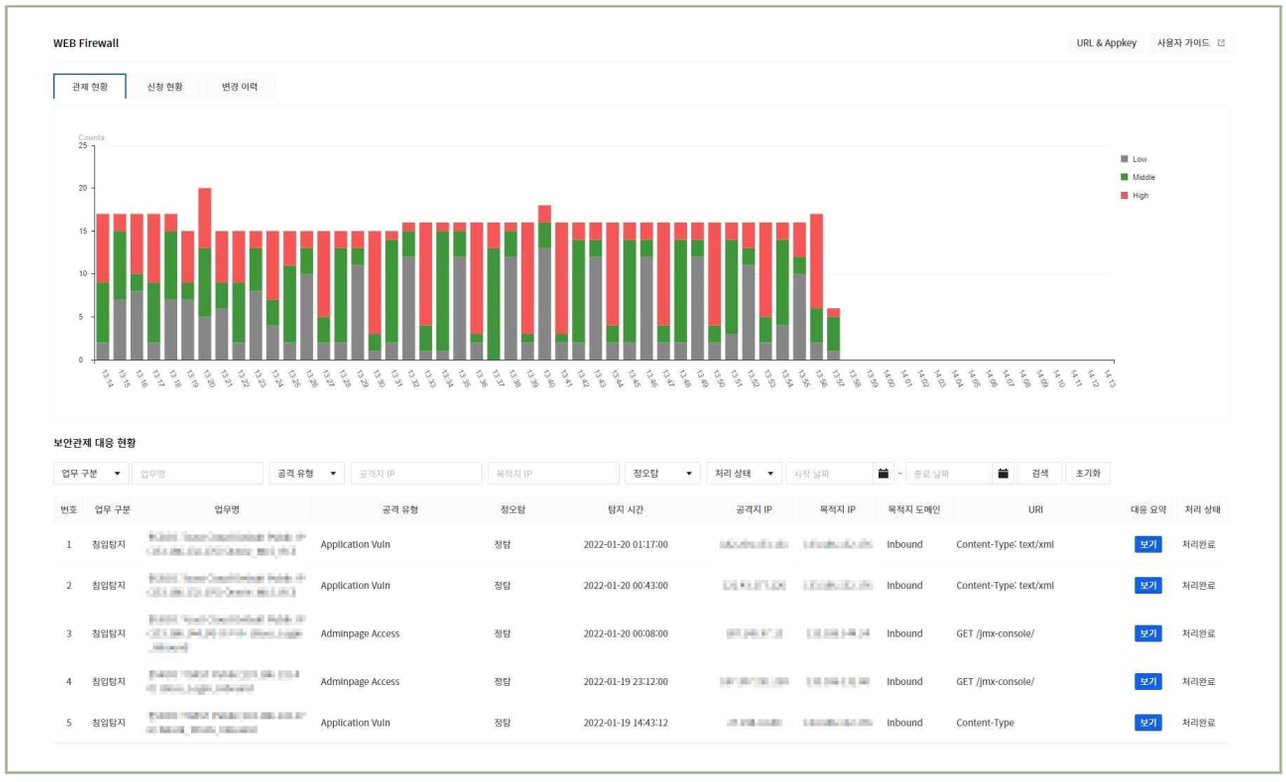
B. WAF 이용은 Self/Managed 두가지 형태를 지원하고 있습니다.

가) Self와 Managed의 차이

Self는 고객이 직접 WAF를 설치/운영하는 형태이고, Managed는 담당 엔지니어가 연락하여, 설치 및 운영을 지원하는 형태입니다.

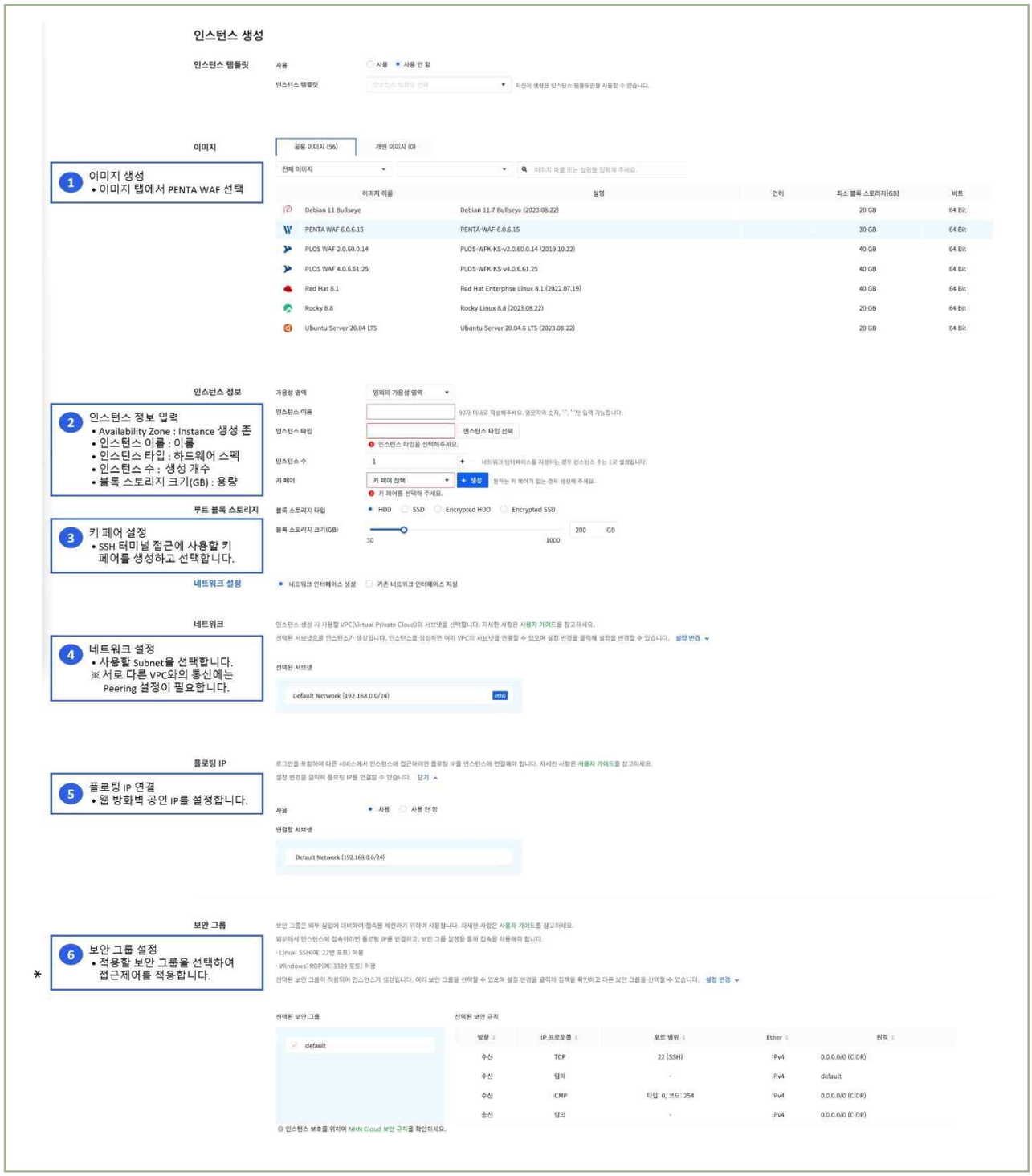
또한 Managed를 이용하는 경우 NHN Cloud console 및 제조사 GUI에서 관제 현황을 모니터링 할 수 있고, Self는 제조사에서 제공하는 GUI를 통해서만 모니터링 할 수 있습니다.

그리고 Managed를 이용할 경우 과학기술정보통신부 지정 보안관제 전문기업의 24시간 보안 관제 서비스를 제공받을 수 있습니다.



| 그림 2-3-9 | WAF 관제 현황 모니터링(Managed)

C. Self로 이용하는 경우 직접 Instance를 설치하고, 제조사의 사용자 가이드를 통해 초기 설정을 진행할 수 있습니다.



| 그림 2-3-10 | WAF Instance 설치(Self)

D. WAF 초기 설정 및 GUI 구성, 운영을 위한 가이드가 제공되고 있으니, Self로 이용하는 고객은 해당 가이드를 참고하여 구성합니다.

(WEBFRONT-KS WAF 설정 가이드, WAPPLES SA WAF 설정 가이드)

E. WAF의 다양한 구성 방식에 대한 예제 내용은 「NHN Cloud 네트워크 아키텍처 보안가이드」에서 다루고 있습니다. 다양한 구성 예제를 확인하려는 경우 해당 가이드를 참조하시기 바랍니다.

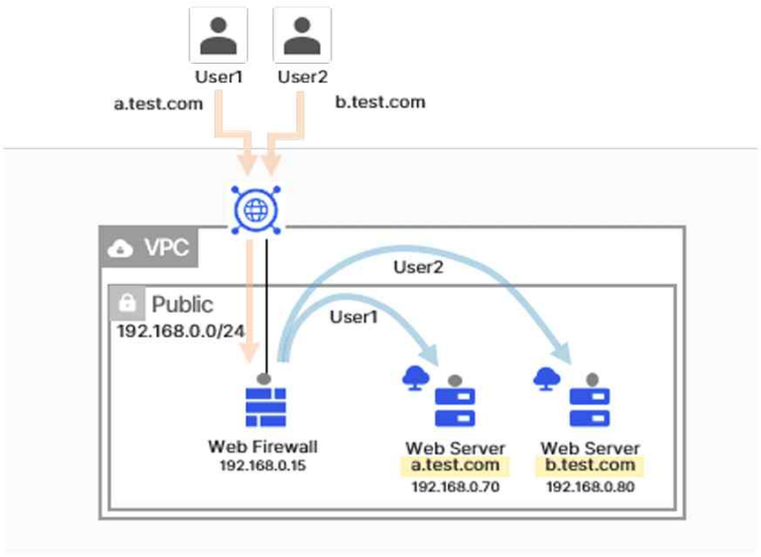


그림 2-35 서로 다른 도메인을 가진 2대의 웹 서버 구성(Proxy 방식의 WEB Firewall)

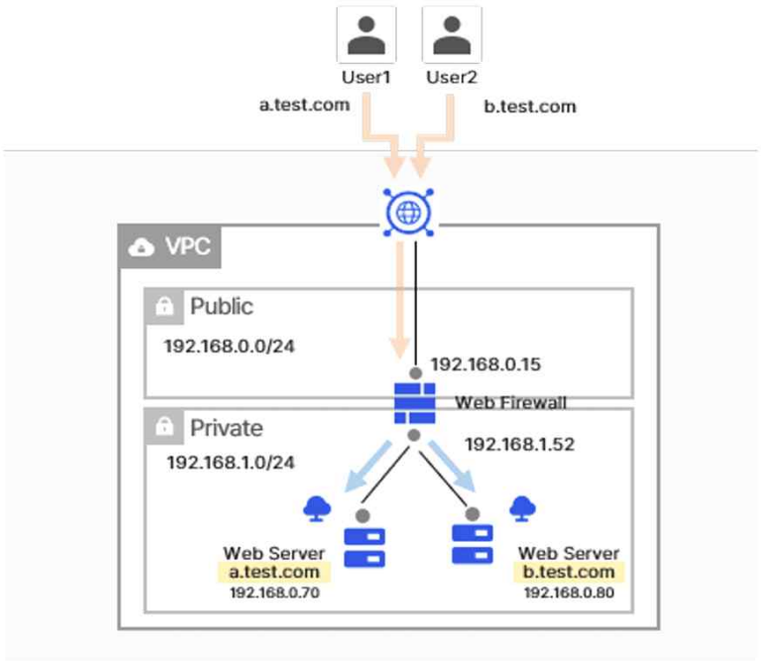


그림 2-36 서로 다른 도메인을 가진 2대의 웹 서버 구성(In-Line 방식의 WEB Firewall)

| 그림 2-3-11 | 네트워크 아키텍처 보안가이드 내 WAF 구성 예제

(API)

- API를 이용하여 Security monitoring 관제를 신청할 수 있습니다.

① 관제 미신청 목록 조회하기

A. '사용자가이드(security monitoring API)'에서 관제 미신청 목록 조회 API를 확인합니다.

관제 미신청 목록 조회

요청

[URI]

메서드	URI
GET	/v1.0/appkeys/{appKey}/not-applied-vms

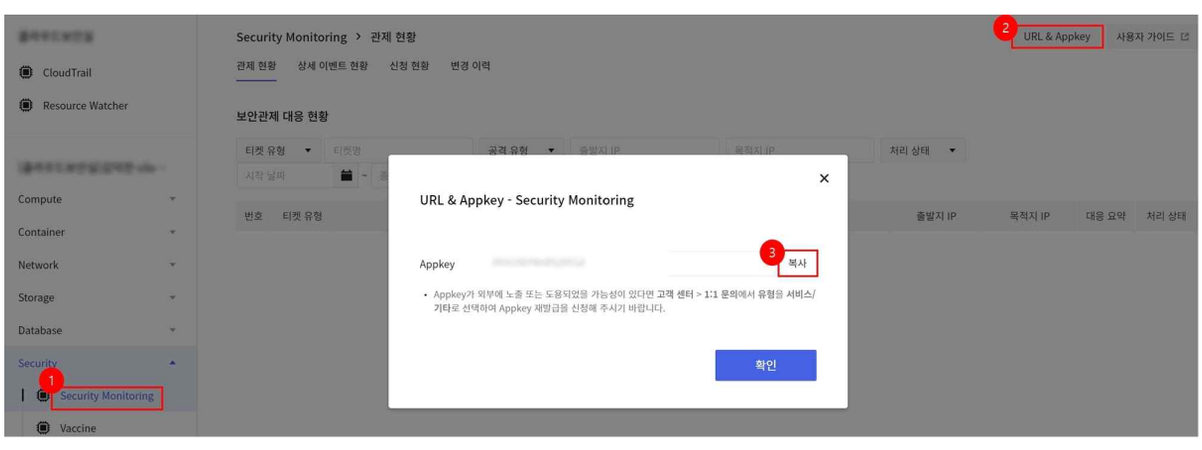
[예]

```
curl -X GET "https://kr1-secmon.api.nhncloudservice.com/v1.0/appkeys/{appKey}/not-applied-vms" \
 -H "Content-Type: application/json"
```

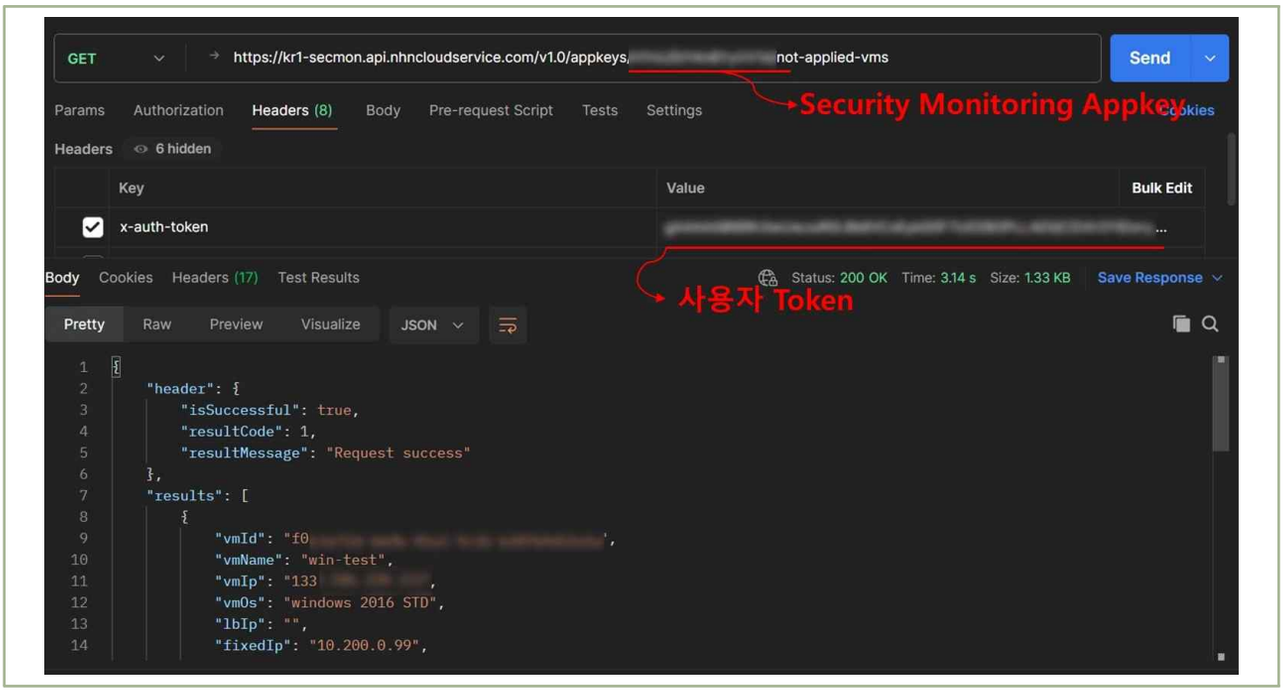
| 그림 2-3-12 | 관제 미신청 목록 조회 예시 API

B. 해당 예시를 바탕으로 API를 작성합니다.

※ URI의 appkey는 security monitoring의 appkey를 작성하여야 하며, [Security 〉〉 Security Monitoring]으로 이동 후 화면 상단의 URL & Appkey를 클릭하시면 확인할 수 있습니다.



| 그림 2-3-13 | Security Monitoring Appkey 확인

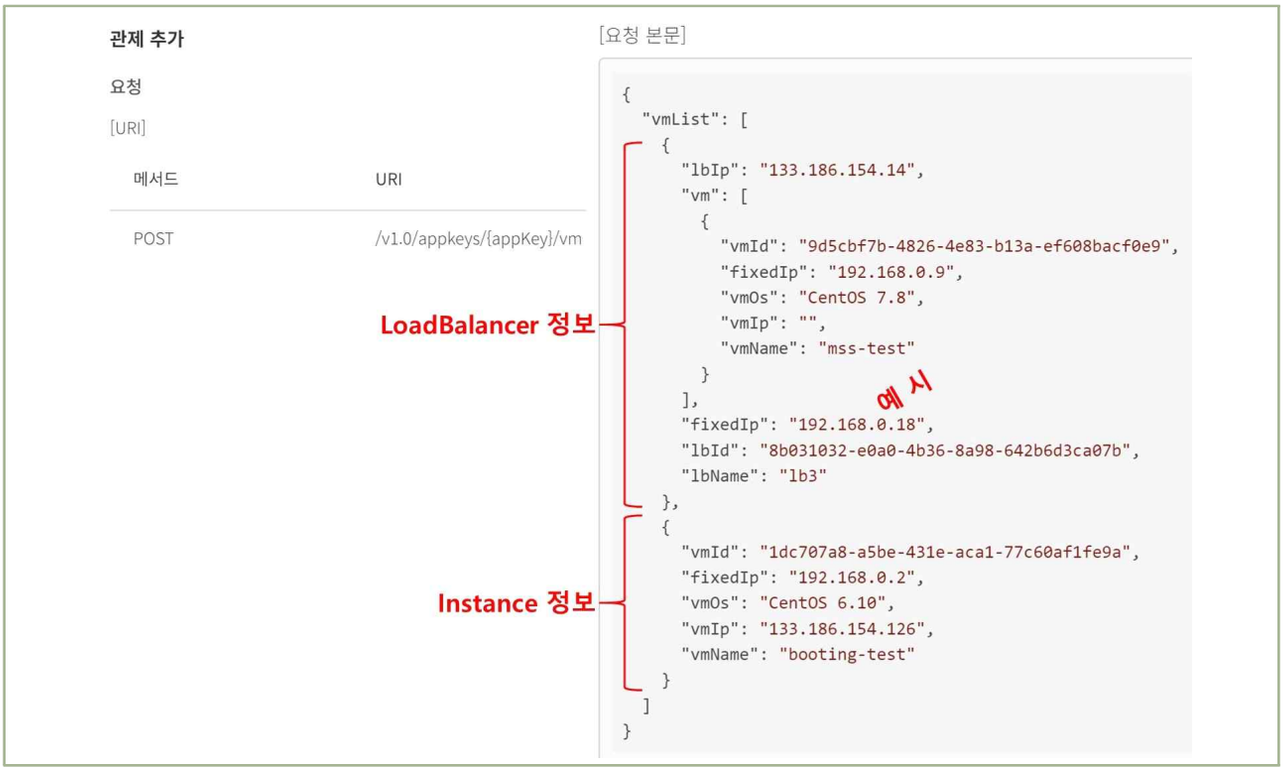


| 그림 2-3-14 | 관제 미신청 목록 조회 API 및 결과

C. 결과를 확인하여 관제 신청할 Instance를 확인합니다.

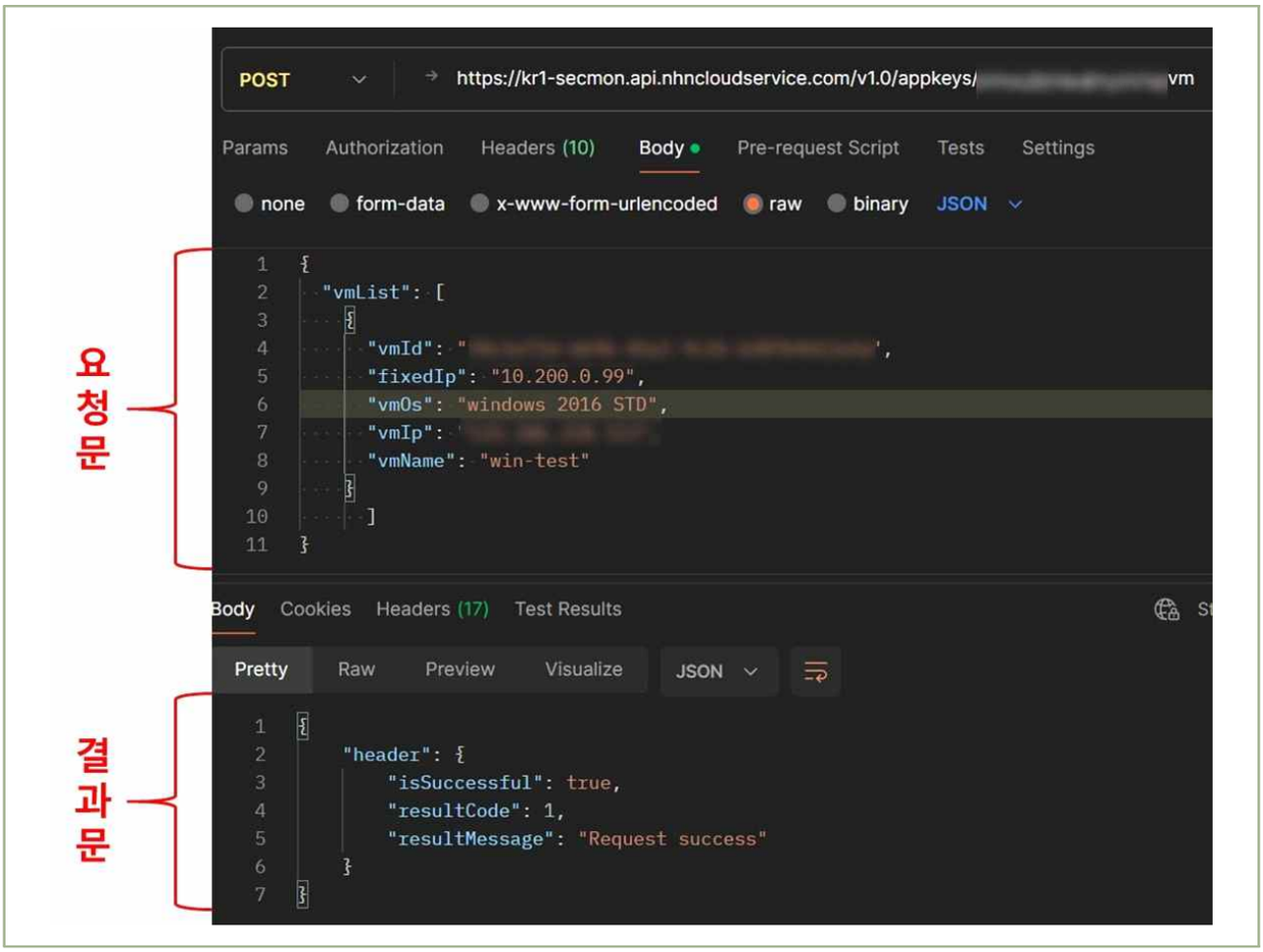
② Instance 관제 추가하기

A. 사용자가이드에서 관제 추가 API를 확인합니다.



| 그림 2-3-15 | 관제 추가 예시 API

B. '그림 2-3-15 관제 추가 예시 API'를 참고하여 Instance 관제 추가 API를 작성하고 결과를 확인합니다.



| 그림 2-3-16 | 관제 추가 API 및 결과

1 기준

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

2 설명

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

  - 예시

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

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

3 우수 사례

- **(가상자원관리시스템)**

  - '2.1 업무 목적에 따른 네트워크 구성', '2.2 내부망 네트워크 보안 통제'에서 내부 네트워크를 분리하고, 각 네트워크별 송·수신을 통제하는 방법(Security Groups, Network ACL, Network Firewall)에 대해 안내하였습니다.

  - 분리된 VPC/subnet 네트워크 중 인터넷 서비스 제공을 위해 웹서버를 구성하려면 인터넷 라우트를 설정하고 Floating IP를 설정하여야 합니다. 정보시스템의 안전한 환경 구성을 위해 해당 정보시스템 외 인터넷 통신이 불필요한 정보시스템은 인터넷 라우트 설정을 배제한 VPC/subnet에 구성하여 운영할 수 있습니다.

    VPC 생성, Subnet 생성, 라우팅 테이블 생성, 라우트 생성의 방법은 '2.1 업무 목적에 따른 네트워크 구성'을 참고하시기 바랍니다.

  - 해당 챕터에서는 추가로 안전하게 웹서버에 접속하는 방법에 대해 설명 드리겠습니다.

- FIP가 설정된 DMZ 내 Instance는 공인 IP를 통해 OS에 직접 접근할 수 있습니다.

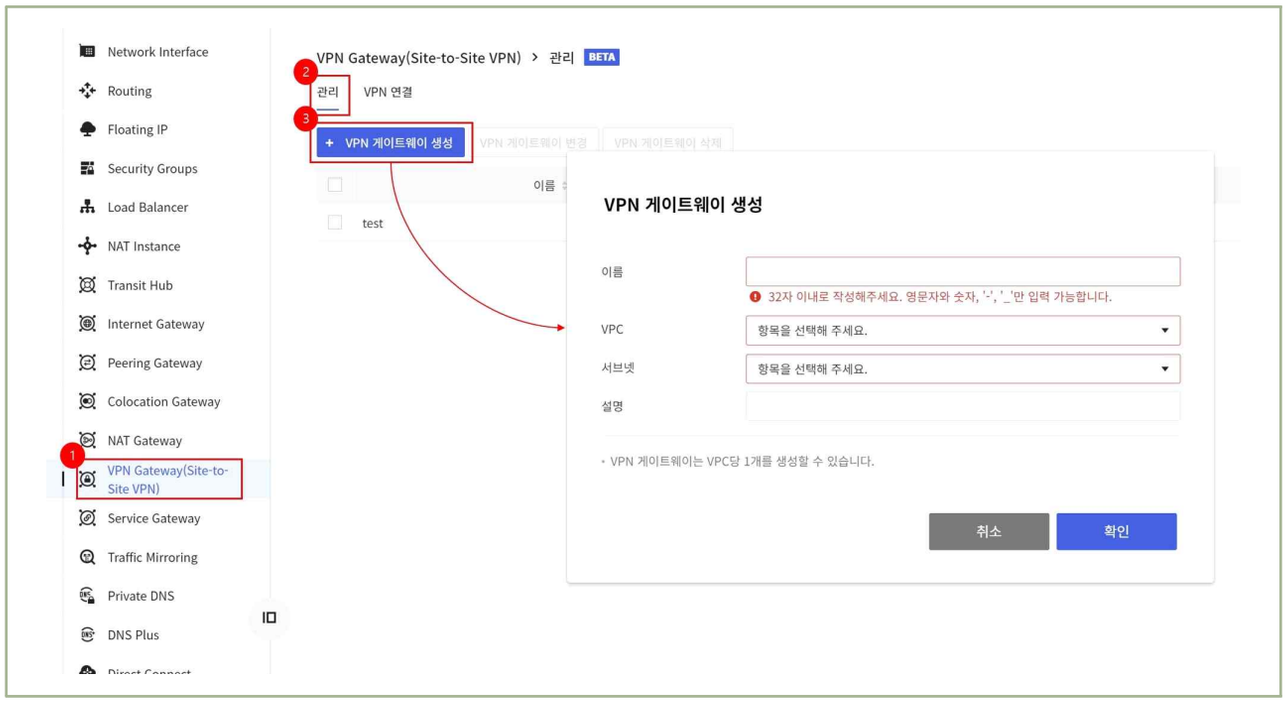
  하지만 공인 IP를 통해 접근이 가능하도록 설정하게 되면, 해커의 공격 대상이 될 수 있어 공인 IP를 통한 접근은 지양하여야 합니다.

- VPN 및 Bastion Host를 구성하여 안전하게 접속하는 방법을 안내 드리오니, 참고하시어 내부 상황에 맞게 적용합니다.

① VPN을 통한 사설 네트워크 구성하기

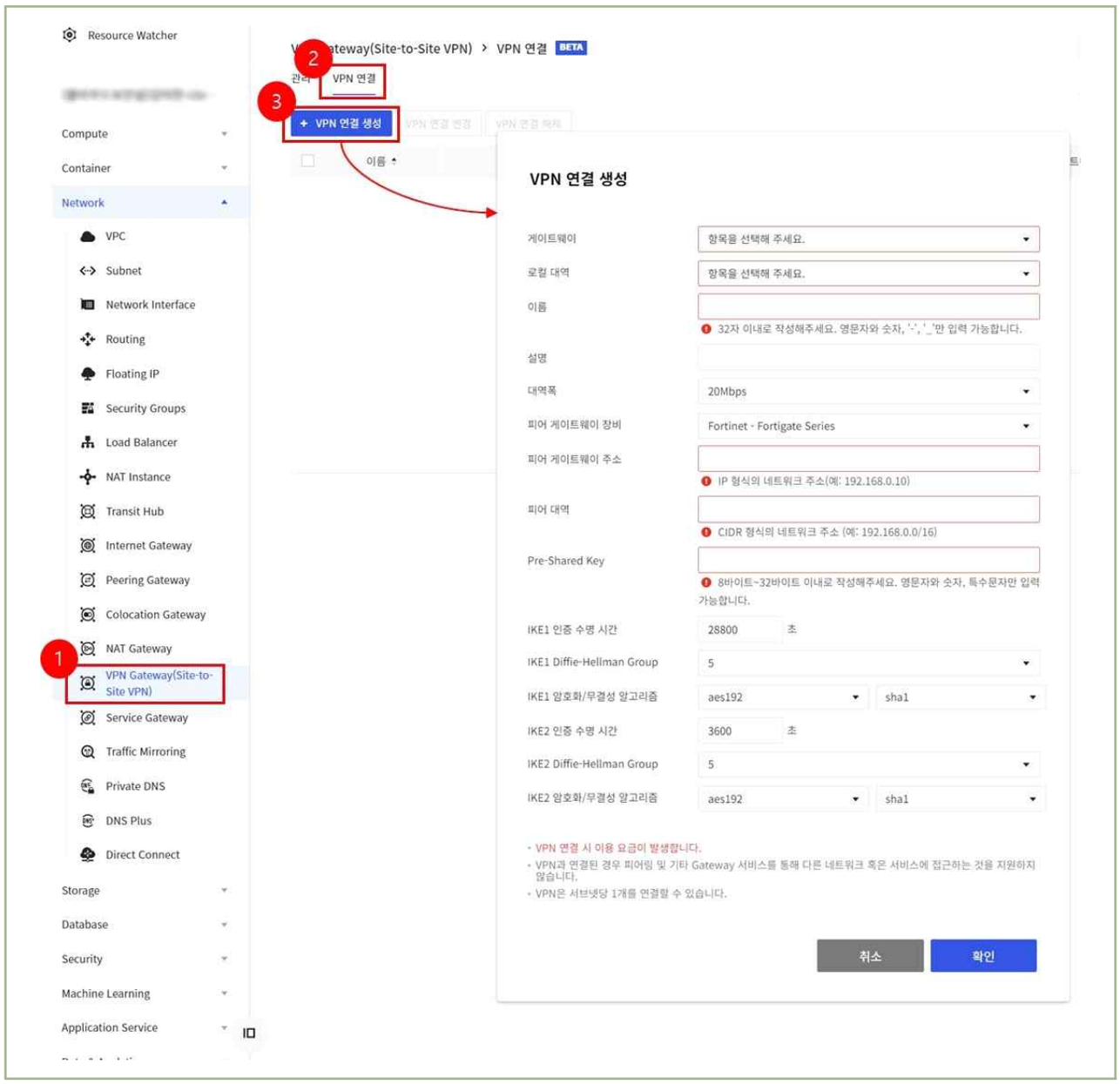
A. [Network 〉〉 VPN Gateway] 서비스를 이용하여 on-premise와의 네트워크 터널링을 구성하여 사설통신망을 구성, 폐쇄된 중요 단말망에서 cloud 네트워크에 접근할 수 있도록 설정하는 방법이 고려될 수 있습니다.

B. VPN Gateway(Site-to-Site VPN) 서비스의 관리 탭을 클릭하고, VPN 게이트웨이 생성을 클릭하여 관련 정보를 입력합니다.



| 그림 2-4-1 | VPN Gateway 생성

C. VPN 연결 탭을 클릭하고, VPN 연결 생성을 클릭하여 VPN 연결을 위한 정보를 입력합니다.



| 그림 2-4-2 | VPN Gateway 연결 설정

D. VPN Gateway의 '사용자가이드(VPN Gateway)'를 참고하여 VPN 터널 옵션을 작성합니다.

E. VPN 연결을 생성한 후 on-premise의 VPN 장비에 관련 설정을 진행합니다.

② Network Firewall의 VPN 기능 사용하기

A. VPN의 경우 VPN Gateway를 통해서도 구성이 가능하지만, Network Firewall을 이용해서도 VPN 구성이 가능합니다.

B. [Network Firewall 〉〉 VPN 〉〉 게이트웨이] 메뉴에서 게이트웨이 생성을 클릭하면 VPN 연결을 위한 게이트웨이를 생성할 수 있습니다.

| 그림 2-4-3 | Network Firewall의 VPN 게이트웨이 생성

C. 게이트웨이를 생성한 이후 게이트웨이를 외부에 연결하기 위한 플로팅 IP를 연결하여야 합니다.

| 그림 2-4-4 | Network Firewall의 VPN 게이트웨이 플로팅 IP 연결

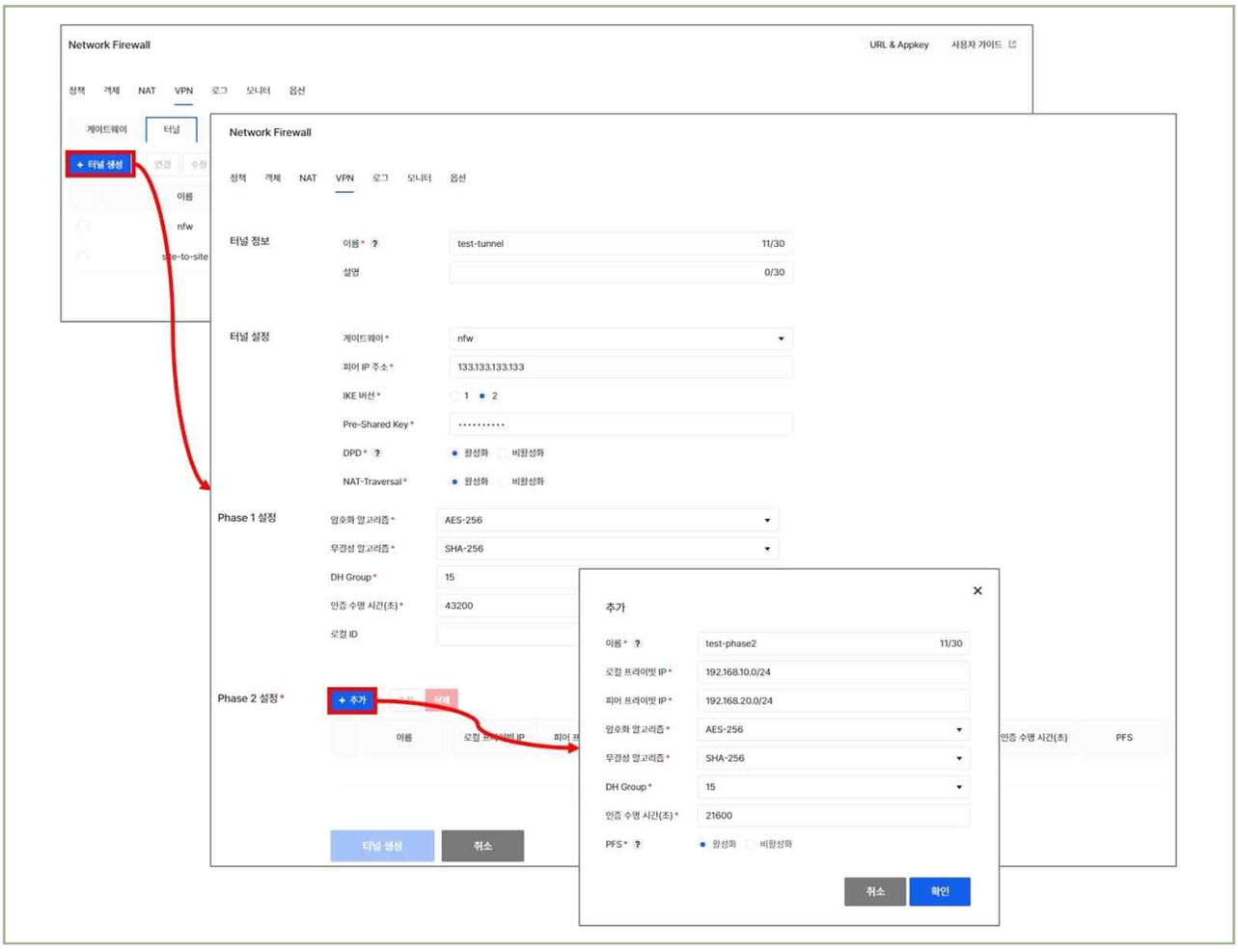
D. 플로팅 IP는 미사용 중인 플로팅 IP가 보여지며, 미사용 중인 플로팅 IP가 없는 경우 플로팅 IP의 추가 생성이 필요합니다.

E. 게이트웨이에 대한 설정이 완료되었다면 '터널' 메뉴에서 피어 장비와 연결할 터널을 생성합니다.

F. 터널 생성 시에는 '터널 정보, 터널 설정, Phase 1 설정, Phase 2 설정'을 입력하여야 하며, Phase 2 설정의 경우 최대 3개까지 생성이 가능합니다. 아래의 주의 사항을 참고하여 정보를 입력합니다.

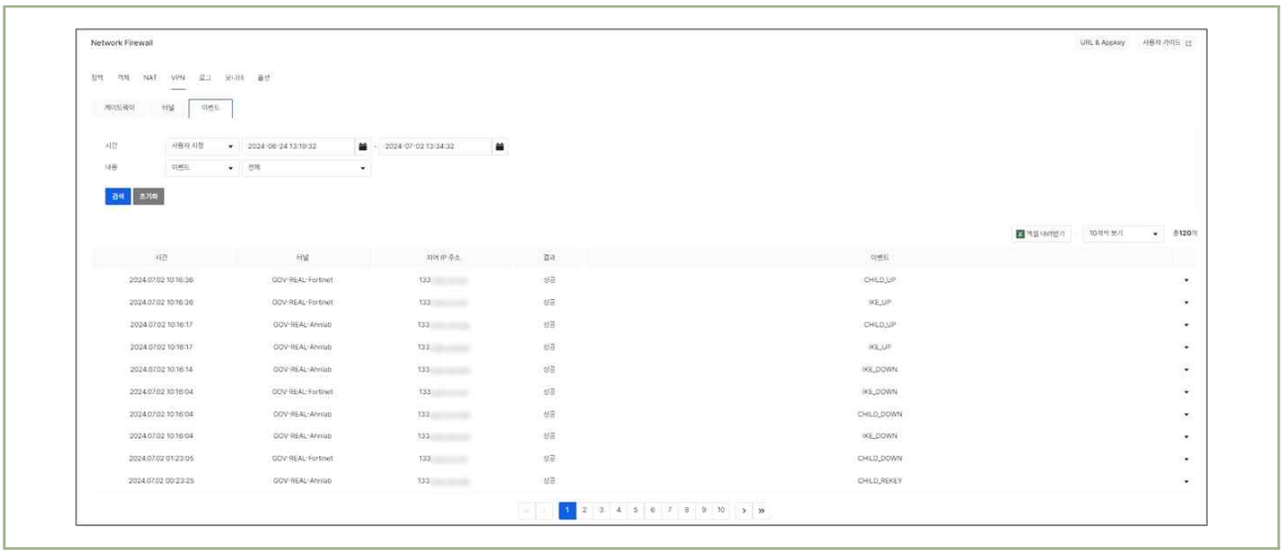
※ 주의 사항

- *모든 설정은 피어 VPN 장비와 동일하게 설정합니다.*
- *로컬 ID는 피어 VPN 장비의 설정 방식에 따라 선택적으로 설정합니다.*
- *Phase 2의 프라이빗 IP는 /24비트 이하로 설정합니다. /24비트 이상의 값을 설정해야 할 경우 서브넷 범위를 사전에 확인하여 서브넷의 시작 IP로 입력합니다. (예시 : 172.16.30.0/21 (X) → 172.16.24.0/21 (O))*
- *로컬 프라이빗 IP와 피어 프라이빗 IP는 서로 중복되지 않아야 합니다.*



| 그림 2-4-5 | Network Firewall 터널 생성

G. 위 설정을 완료하면 IPsec을 통한 터널통신을 진행할 수 있으며, '이벤트' 메뉴에서 VPN의 사용 내역을 확인할 수 있습니다.

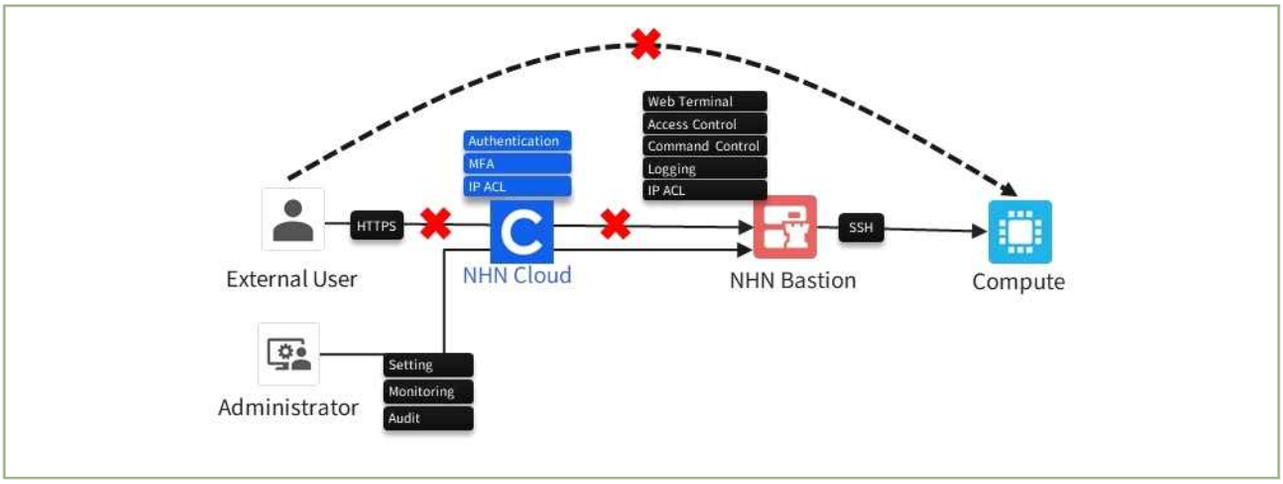


| 그림 2-4-6 | Network Firewall VPN 이벤트 조회

③ NHN Bastion 구성을 통해 연결하기

A. NHN Bastion는 외부 네트워크와 내부 네트워크 사이에 위치하며, 외부에서의 내부자원 직접 접근을 제한하고 내부 네트워크에 대한 보호를 제공합니다.

B. 서비스용 웹서버에 직접 접근하는 대신 보안 설정이 적용된 NHN Bastion을 경유하여 웹서버로 접근하면 해커의 웹서버 직접 접근을 차단할 수 있습니다.



| 그림 2-4-7 | NHN Bastion Host 구성도 예시

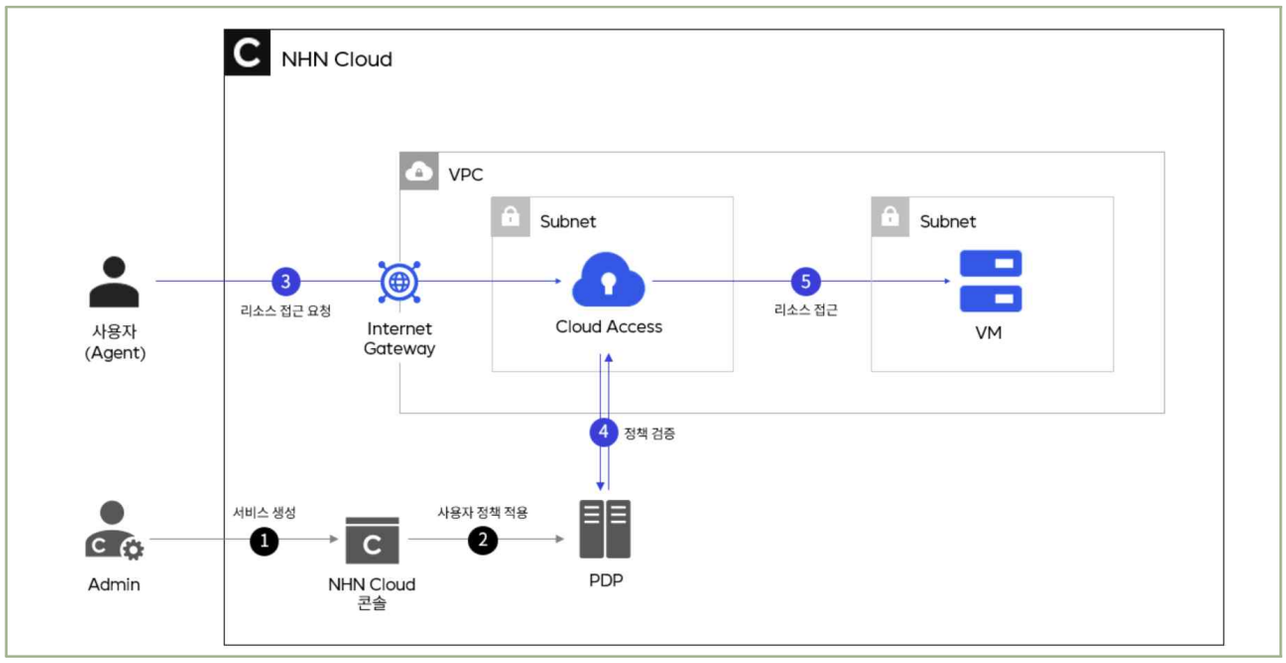
C. NHN Bastion 구성 시 IP ACL을 설정하거나, 접속 포트를 제외한 모든 포트를 차단하는 등의 접근제한 조치가 필요합니다.

D. NHN Bastion의 정책 설정을 통해 명령어 사용 통제, 모니터링도 가능합니다. (1.5 참조)

④ Cloud Access로 안전한 접속 수단 구현하기

A. Cloud Access는 제로 트러스트 보안 모델을 기반으로 NHN Cloud 리소스에 안전하게 접속할 수 있도록 지원하는 서비스입니다.

B. 관리자는 NHN Cloud 콘솔에서 사용자의 지속 인증, 실시간 로깅 및 모니터링 기능을 활용하여 효율적으로 서비스를 운용할 수 있습니다.



| 그림 2-4-8 | Cloud Access의 동작 방식

C. 그림 2-4-8의 구성에서 '정책 결정 지점'(Policy Decision Point, PDP)의 정책은 콘솔을 통해 설정할 수 있으며, 설정된 정책은 '정책 시행 지점'(Policy Enforcement Point, PEP)인 Cloud Access 서비스에서 수행됩니다.

D. 콘솔에서는 Cloud Access에서 VM간의 ACL 정책부터, 접속 시 복수 인증, 엔드포인트 설정(인터넷 차단, 필수 소프트웨어 설치 검사, 차단 소프트웨어 검사, 백신 검사 등)을 추가로 지정하여 안전한 단말환경을 지속적으로 검사하게 설정할 수 있습니다.

4 참고 사항

- 마켓플레이스 내 3rd-party 「서버접근제어 솔루션」을 사용하면 서버에 직접 접근하는 단말을 제어하는 것이 가능합니다.
- NHN Cloud 마켓플레이스

1 기준

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

2 설명

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

  - 예시

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

    2) 사설 IP 할당 현황에 대한 주기적 검토 수행

3 우수 사례

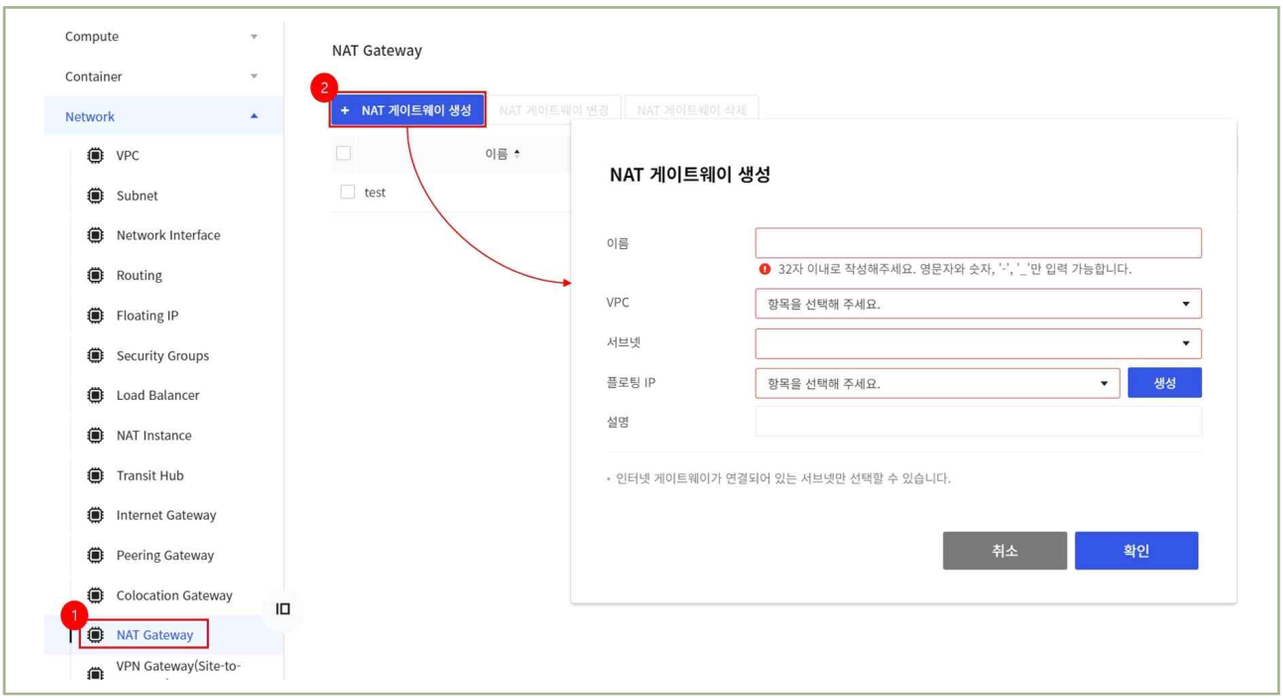
- **(가상자원관리시스템)**

  - NHN Cloud의 VPC, Subnet 등의 기능을 통해 사설 네트워크 대역 분리, Internet Gateway 생성, Floating IP 생성 방법 등의 경우 앞의 챕터에서 가이드 하였습니다.
  - 인터넷 통신을 위해 Instance에 Floating IP를 직접 부여하는 방법 외 NAT Gateway, NAT Instance를 통해 인터넷 통신을 구성하는 방법에 대해 가이드 하겠습니다.
  - NAT Gateway는 완전 관리형 서비스로 인터넷 게이트웨이가 연결되지 않은 Instance들이 인터넷에 엑세스 할 수 있도록 지원합니다. 다만 인터넷에서 이 Instance들로 연결을 시작할 수는 없습니다.

    NAT Instance는 Instance를 고객이 직접 관리하는 서비스로 OS 관리, 패치 등을 직접 관리해야 하며, NAT Gateway와 마찬가지로 인터넷에서 이 Instance들로 연결을 시작할 수 없습니다.

① NAT Gateway 생성하기

A. [Network 〉〉 NAT Gateway]로 이동하여 NAT 게이트웨이 생성을 클릭합니다.



| 그림 2-5-1 | NAT Gateway 생성

B. NAT Gateway는 Internet Gateway가 연결된 subnet에서만 생성이 가능합니다.

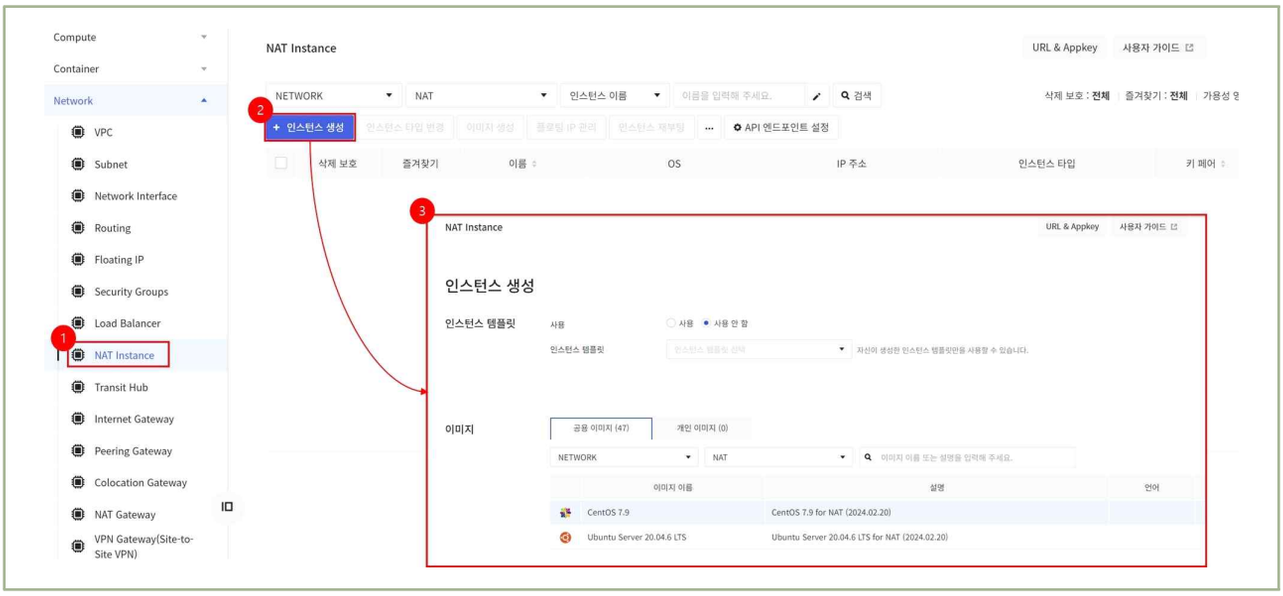
C. [Network 〉〉 Routing]으로 이동하여 NAT Gateway 연결이 필요한 라우팅 테이블을 클릭한 후 라우팅을 설정합니다.

| 그림 2-5-2 | NAT Gateway 라우트 생성

D. 라우팅을 설정하면 VPC 내 특정 CIDR을 대상으로 인터넷 통신 시 NAT Gateway를 통해 통신하게 됩니다.

② NAT Instance 생성하기

A. [Network 〉〉 NAT Instance]로 이동하여 인스턴스 생성을 클릭합니다.

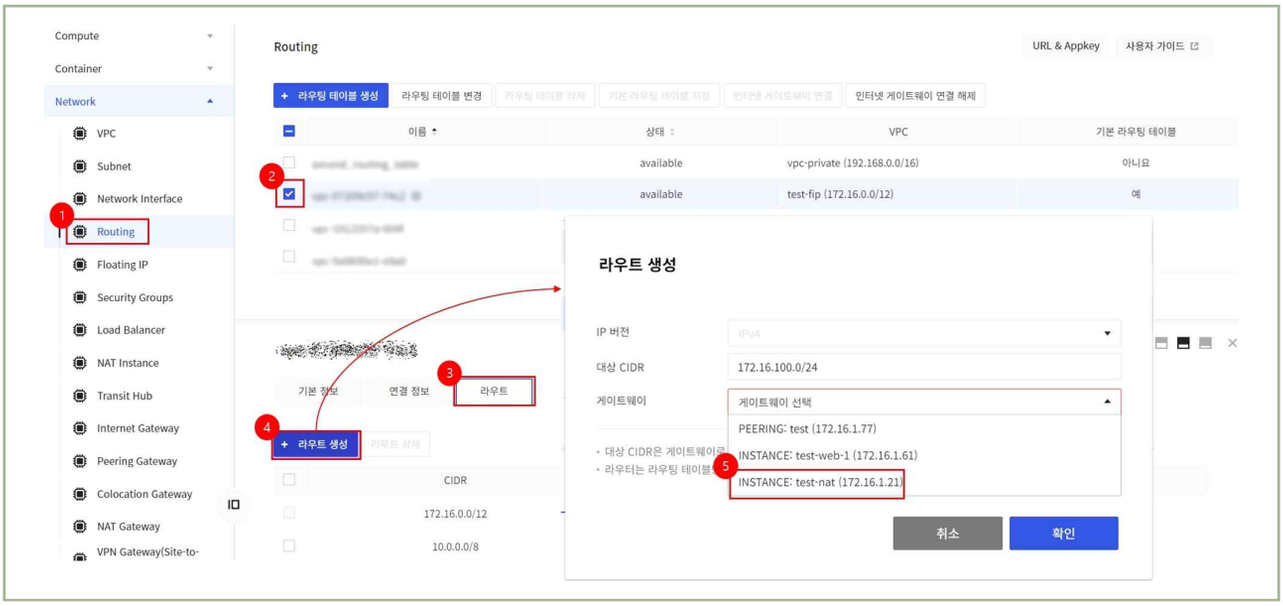


| 그림 2-5-3 | NAT Instance 생성

B. 인스턴스 생성을 클릭하면 Instance 생성 화면과 동일한 창으로 이동되며, Instance 이미지가 NAT 용으로 제공되는 이미지만 보이게 됩니다.

C. 위의 이미지를 이용하여 해당 서비스가 필요한 subnet에 Instance를 생성합니다.

D. [Network 〉〉 Routing]으로 이동하여 NAT 설정이 필요한 VPC를 선택하고, 라우트 탭에서 라우트 생성을 클릭, NAT Instance를 게이트웨이로 하는 Route를 생성합니다.



| 그림 2-5-4 | NAT Instance 라우트 생성

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

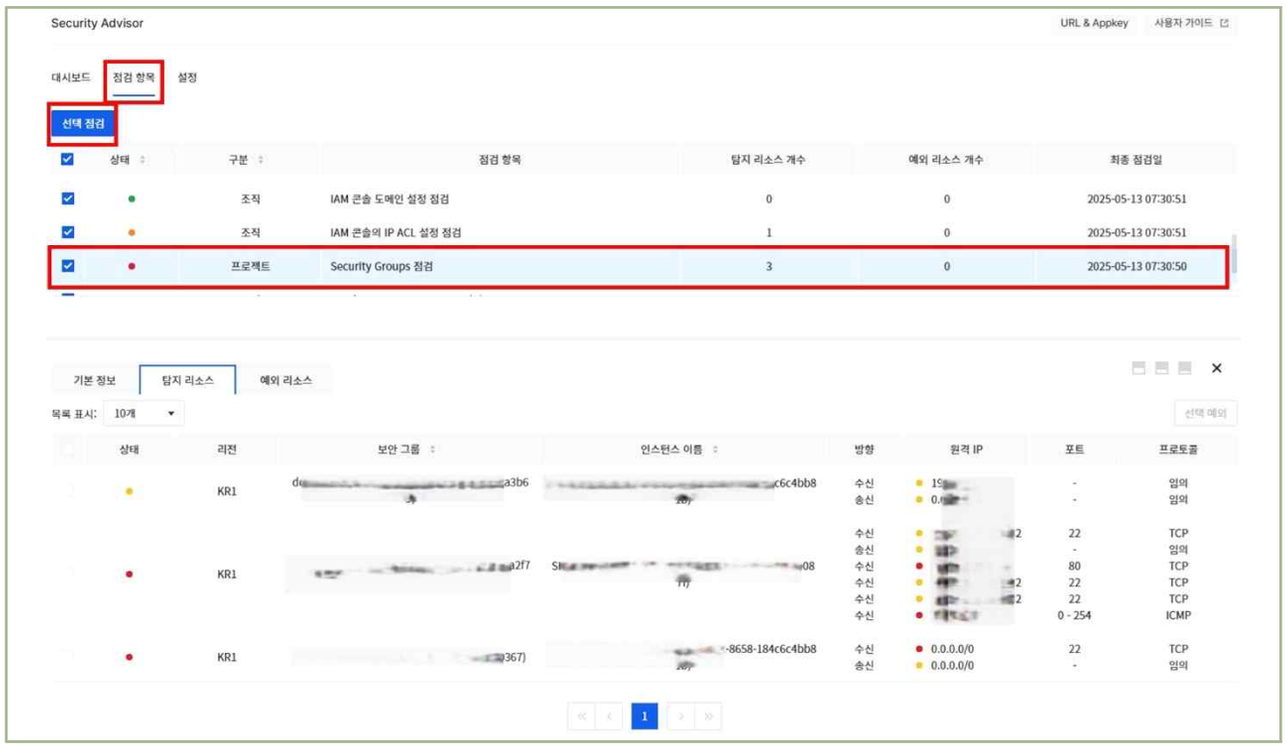
    1) 방화벽 정책에 관한 주기적 검토 수행
    2) ACL 정책에 관한 주기적 검토 수행
    3) 보안그룹에 관한 주기적 검토 수행

3 우수 사례

- **(가상자원관리시스템)**

  ① Security Advisor 서비스를 이용하여 Security Groups 점검

  - Security Advisor의 점검 항목 중 “Security Groups 점검”을 이용하여 인스턴스에 적용된 Security Groups의 Rule을 Security Advisor의 기준으로 점검할 수 있습니다

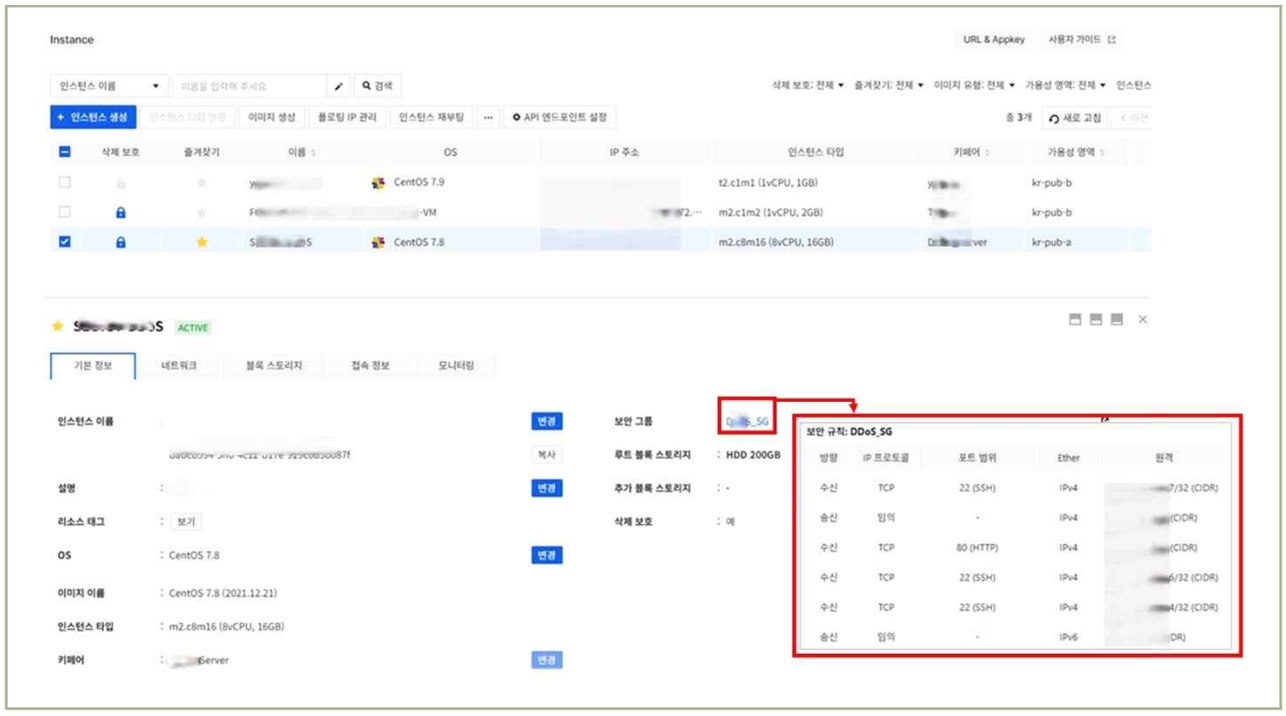


| 그림 2-6-1 | Security Groups 점검

- Security Advisor의 자동 점검 기능[Security Advisor 〉〉 설정 〉〉 점검 설정]을 활용하여 주기적인 점검할 수 있습니다.

| 그림 2-6-2 | 자동 점검 설정

② 모든 Security Groups 룰을 확인하기 위해서는 [Compute 〉〉 Instance] 화면으로 이동하여 개별 확인할 수 있습니다.



| 그림 2-6-3 | Instance Security Groups 적용 확인

③ Network Firewall 서비스를 사용하는 경우, Hit Count 또는 Last Hit Time을 활용하여 정책 사용 여부를 확인할 수 있습니다.

| 그림 2-6-4 | Network Firewall Hit Count 확인

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, MFA등 추가 인증 방식을 구현하고 접속 IP를 제한하는 등 강화된 보안환경 구성

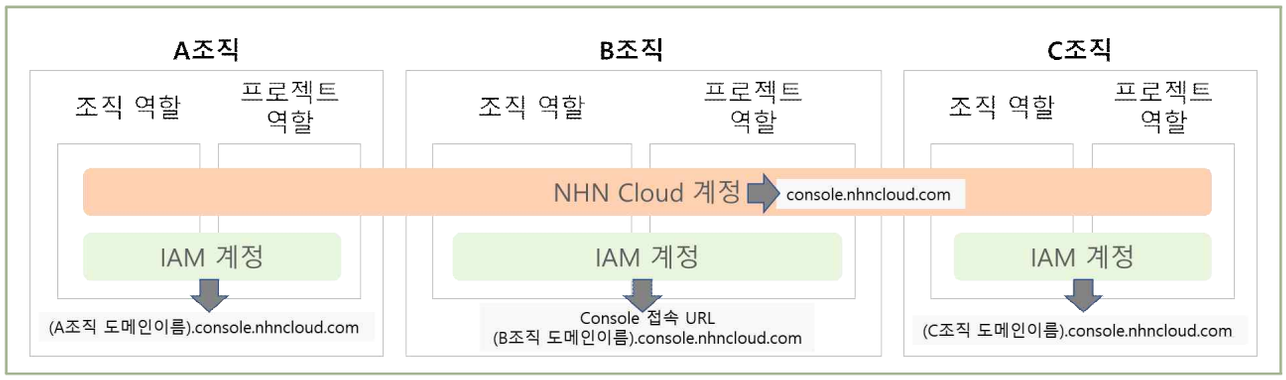
3 우수 사례

- **(가상자원관리시스템)**

  ① 업무별 역할 분리하기

  - NHN Cloud 에서의 이용자 계정은 NHN Cloud 계정과 IAM 계정으로 구분되어 있으며, 역할 권한은 조직 관리 역할 및 조직 서비스 이용 역할, 프로젝트 관리 역할 및 프로젝트 서비스 이용 역할로 구분되어 있습니다.

- 계정 및 역할 권한의 차이를 잘 숙지하여 권한을 부여합니다.



| 그림 3-1-1 | NHN Cloud의 계정 체계와 조직/프로젝트 역할 관계

A. 조직 역할

가) 조직 관리 및 조직 서비스 이용 역할을 부여합니다.

나) 조직 관리 역할의 경우 OWNER, ADMIN, MEMBER, Billing Viewer, Budget Admin, Budget viewer, Log Viewer, ORG Dashboard Viewer, NONE으로 구분되며, NHN Cloud 계정, IAM 계정에 권한 부여가 가능합니다.

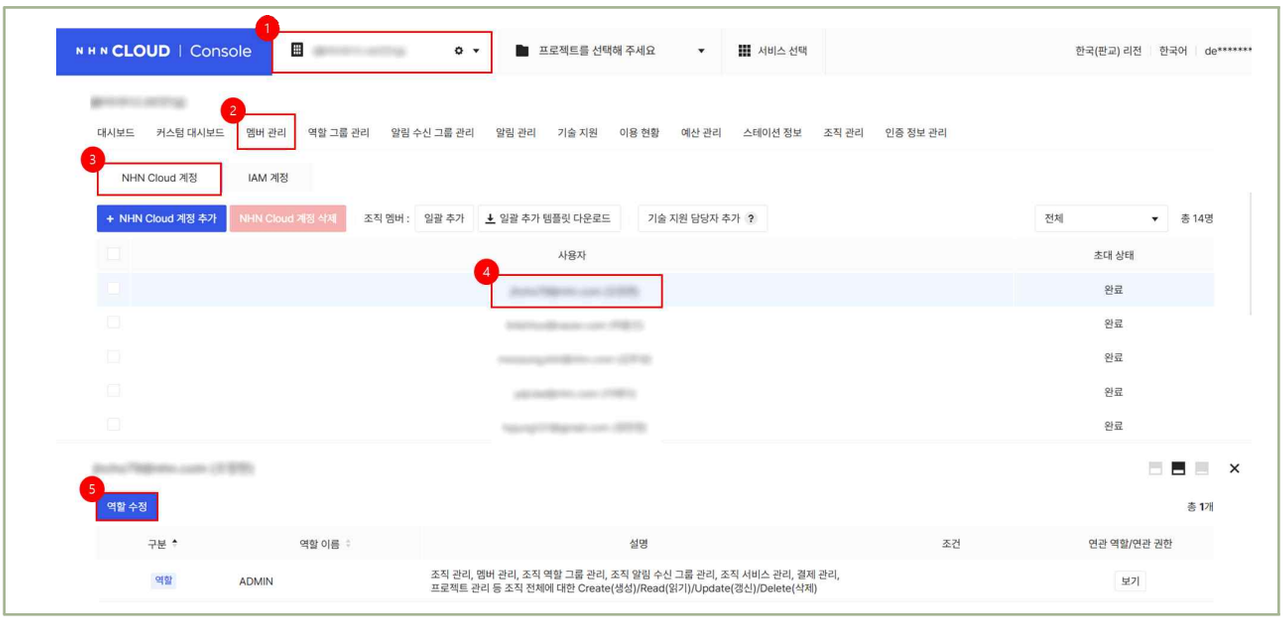
조직 관리 역할

역할	설명
OWNER	조직 생성, 조직 관리, 멤버 관리, 조직 서비스 관리, 결제 관리, 프로젝트 관리 등 조직 전체에 대한 Create(생성)/Read(읽기)/Update(갱신)/Delete(삭제)
ADMIN	조직 관리, 멤버 관리, 조직 서비스 관리, 결제 관리, 프로젝트 관리 등 조직 전체에 대한 Create(생성)/Read(읽기)/Update(갱신)/Delete(삭제)
MEMBER	프로젝트 Create(생성), 조직 대시보드 Read(읽기), 프로젝트에 대한 Read(읽기)
BILLING_VIEWER	결제 관리 이용현황 Read(읽기), 예산 관리에 대한 Read(읽기)
BUDGET_ADMIN	예산 관리에 대한 Create(생성)/Read(읽기)/Update(갱신)/Delete(삭제)
BUDGET_VIEWER	예산 관리에 대한 Read(읽기)
LOG_VIEWER	사용자 Action 로그 관리 Read(읽기), 리소스 관리 Create(생성)/Read(읽기)/Update(갱신)/Delete(삭제)
ORG_DASHBOARD_VIEWER	조직 대시보드 Read(읽기)
NONE	조직 대시보드 Read(읽기), 조직 기본 설정 Read(읽기)

| 그림 3-1-2 | 조직 관리 역할 종류

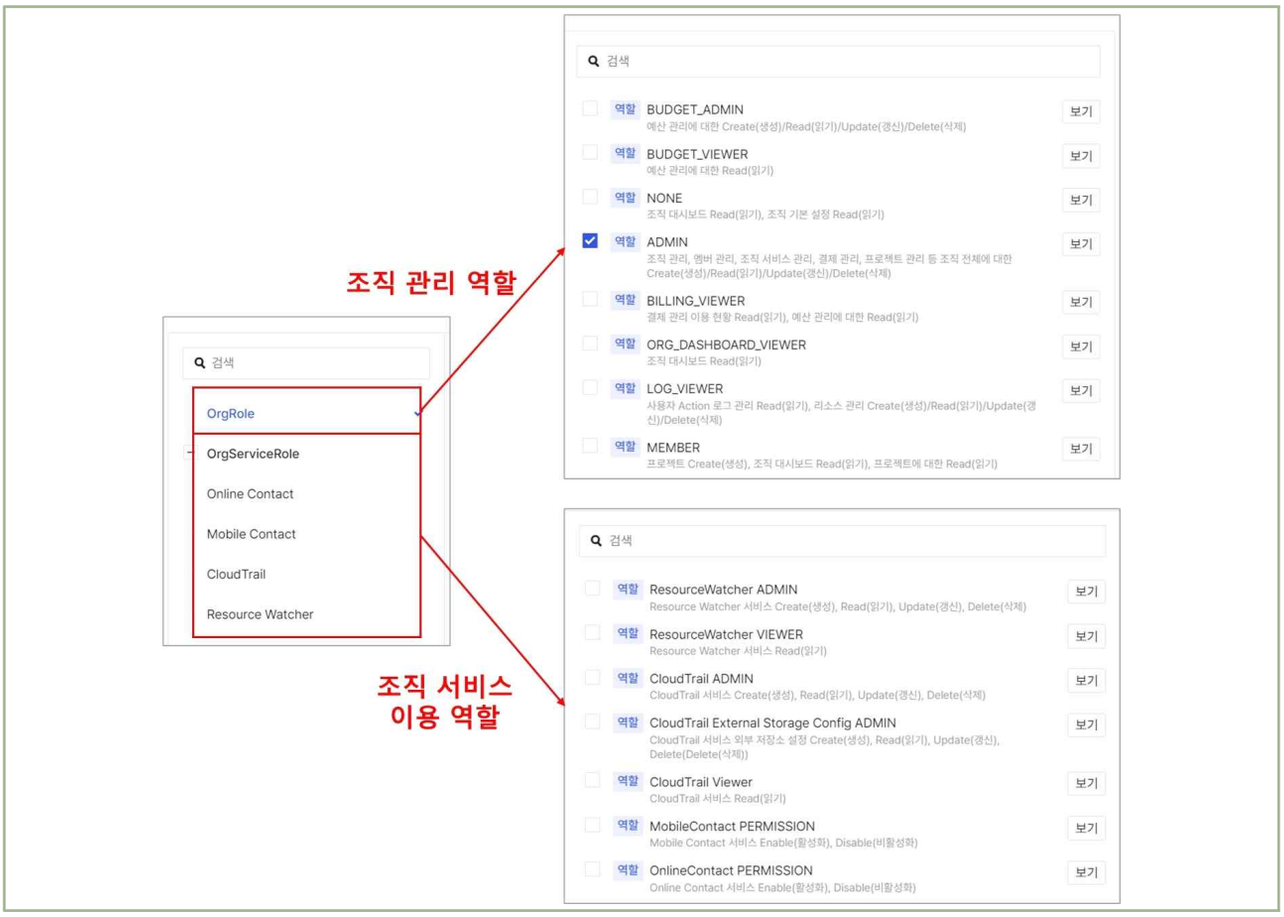
다) 조직 서비스 이용 역할의 경우 CloudTrail과 Resource Watcher, Moblie Contact, Online Contact 서비스에 대한 역할 권한을 설정할 수 있습니다.

라) 조직 역할 설정은 조직의 멤버 관리 탭에서 진행됩니다. [조직 〉〉 멤버 관리 〉〉 NHN Cloud 계정/IAM 계정]에서 설정하고자 하는 계정의 '역할 수정'을 클릭하여 역할을 지정합니다.



| 그림 3-1-3 | NHN Cloud 계정의 조직 역할 설정

마) 역할 수정 메뉴에서 ‘OrgRole(조직 관리 역할)’과 ‘OrgServiceRole(조직 서비스 이용 역할)’을 설정할 수 있습니다.



| 그림 3-1-4 | 조직 관리 역할과 조직 서비스 이용 역할 설정

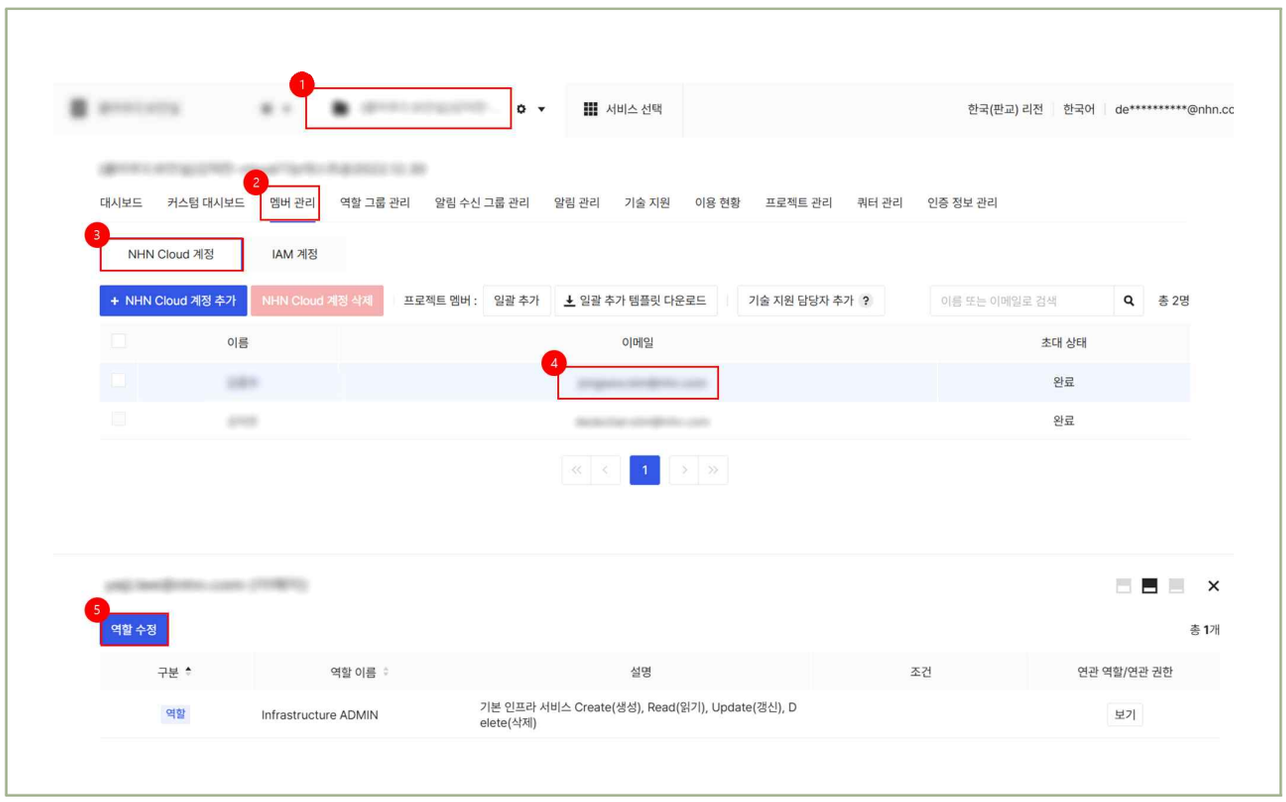
바) IAM 계정은 멤버 관리 탭에서 'IAM 계정'를 클릭한 후 권한을 변경하고자 하는 계정을 선택, '역할 수정'을 클릭하여 조직 권한을 수정할 수 있습니다.

B. 프로젝트 역할

가) 프로젝트 역할은 '프로젝트 관리 역할', '프로젝트 서비스 이용 역할'로 구분되며, 프로젝트 역할에 따라 적절할 권한을 부여하여야 합니다.

(NHN Cloud 사용자 가이드(프로젝트 역할))

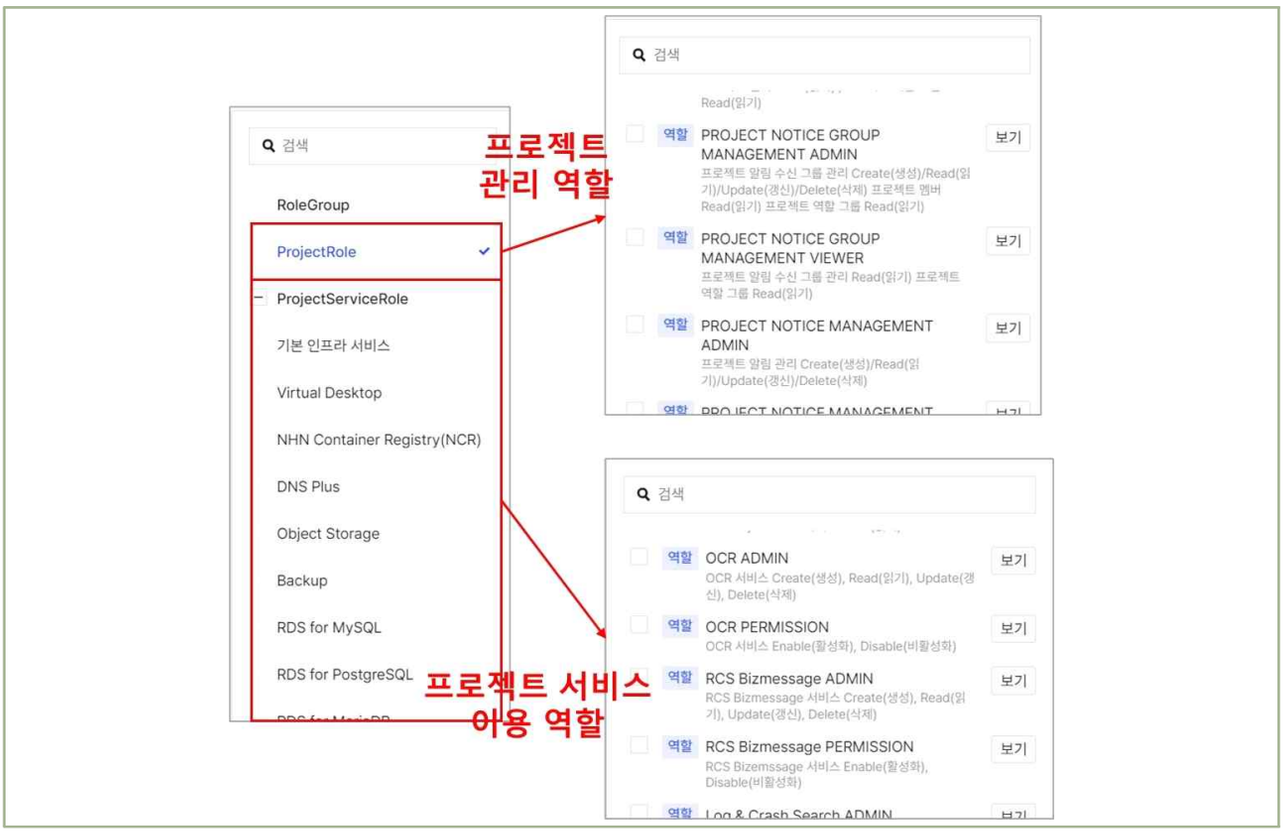
나) NHN Cloud 계정의 경우 [프로젝트 〉〉 멤버 관리 〉〉 NHN Cloud 계정]에서 역할을 변경할 계정을 클릭한 후 '역할 수정'을 클릭하여 역할을 변경합니다.



| 그림 3-1-5 | 프로젝트 역할 수정

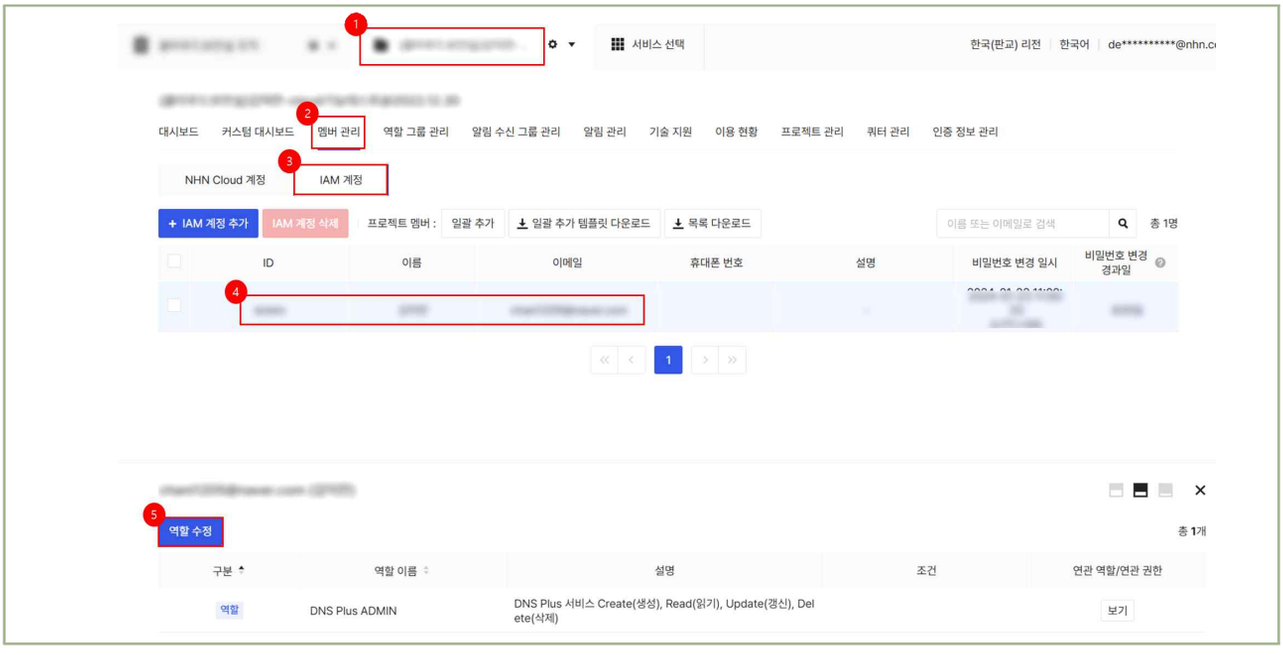
다) 프로젝트의 역할 수정 메뉴에서는 'ProjectRole(프로젝트 관리 역할)'과 'ProjectService Role(프로젝트 서비스 이용 역할)'을 설정할 수 있습니다.

'역할 그룹 관리' 메뉴에서 별도 설정한 역할 그룹이 존재하는 경우 'RoleGroup(역할 그룹)'으로 설정할 수도 있습니다. 'RoleGroup'을 설정하는 경우 개발팀/운영팀 또는 운영수탁사, 감사부서 등으로 Role name을 설정하여 기본 권한을 지정 운영할 수 있습니다.



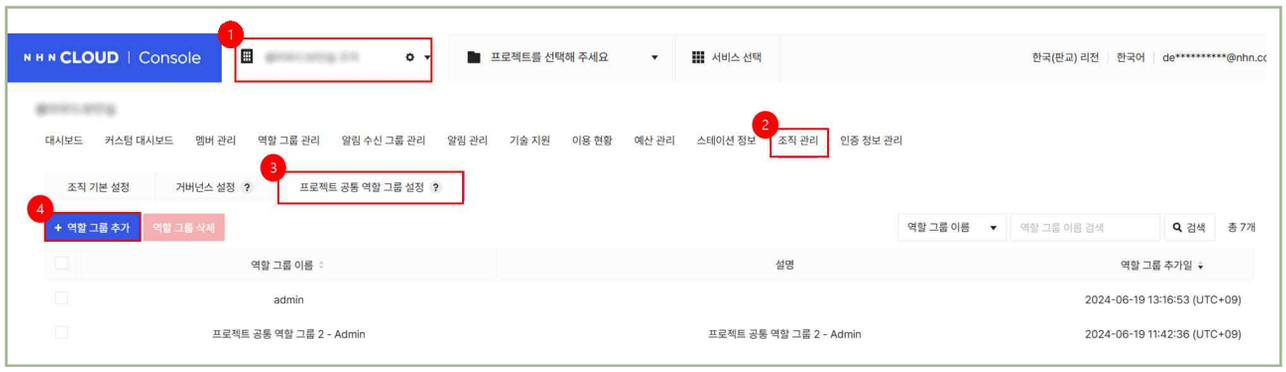
| 그림 3-1-6 | 프로젝트 역할 권한 설정

라) IAM 계정의 경우 [프로젝트 〉〉 멤버 관리 〉〉 IAM 계정]에서 역할을 변경할 계정을 클릭한 후 '역할 수정'을 클릭하여, NHN Cloud 계정과 동일한 방법으로 프로젝트 역할 권한을 수정합니다.



| 그림 3-1-7 | IAM 계정의 프로젝트 역할 수정

마) 만약 전체 조직 내 역할 그룹을 공통으로 적용하고자 하는 경우에는 [조직 〉〉 조직 관리 〉〉 프로젝트 공통 역할 그룹 설정] 탭에서 역할 그룹을 추가하면, 전체 프로젝트에 해당 역할 그룹이 추가됩니다.



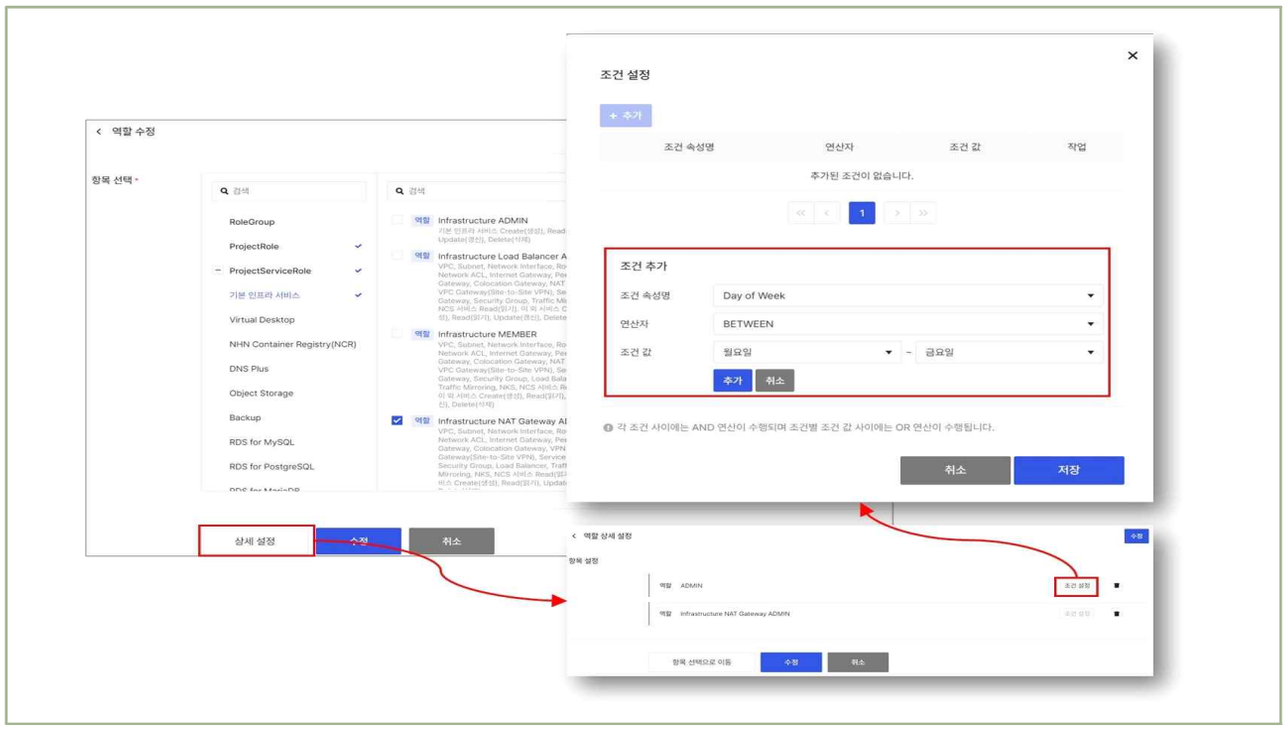
| 그림 3-1-8 | 프로젝트 공통 역할 그룹 설정

C. 역할에 조건 추가하기

가) 역할 권한을 부여할 때 역할별로 조건을 지정할 수 있습니다.

※ 현재는 일부 서비스 권한에만 조건 설정이 가능합니다. 모든 서비스 권한에 조건을 부여할 수 있도록 하기 위해 계속 개발 중이며, 지속 배포될 예정입니다.

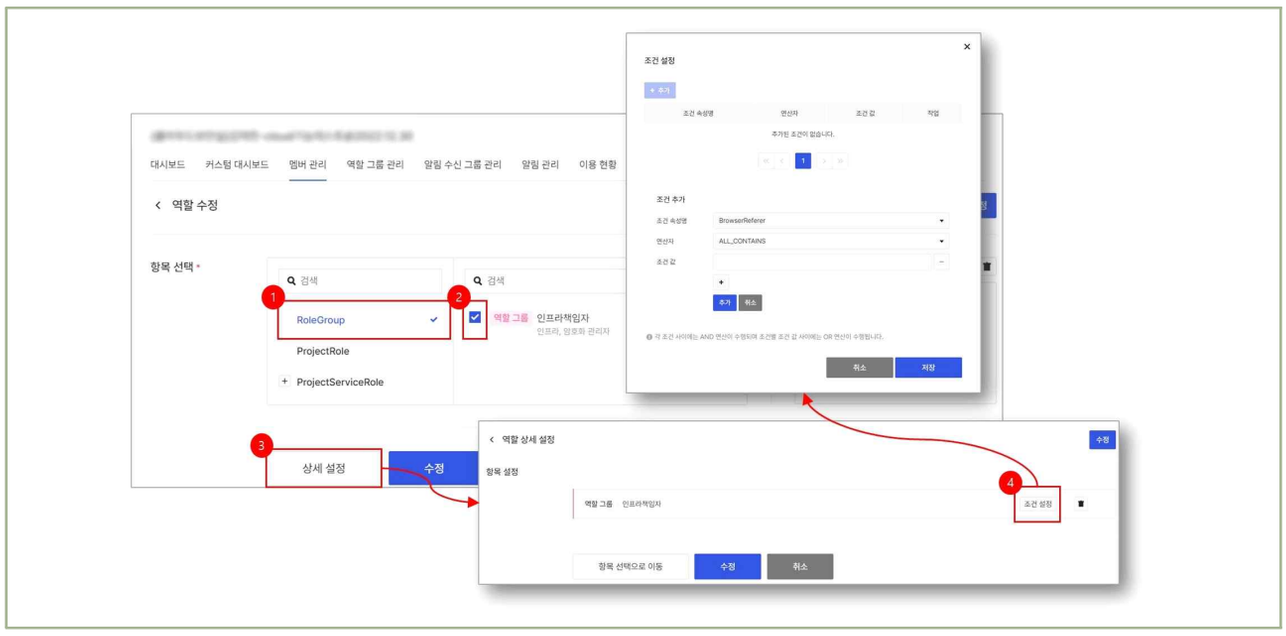
나) 조건 속성에는 'BrowserReferer', 'BrowserUserAgent', 'DateTime', 'Day of Week', 'IP Address', 'Time', 'CloudTrail 서비스의 프로젝트 ID 목록을 제약하는 속성' 값 중 선택할 수 있으며, 사용자의 상황에 맞게 연산자 및 조건 값을 지정할 수 있습니다.



| 그림 3-1-9 | 역할 조건 추가

다) 위 조건은 'ADMIN' 권한은 월요일부터 금요일까지만 유효한 권한으로 부여된다는 조건입니다.

라) 각 서비스별 조건을 지정하지 않고 '역할 그룹(RoleGroup)'에도 조건을 부여할 수 있습니다. 이 경우 '역할 그룹' 내 선택된 서비스는 전부 해당 조건을 적용받게 됩니다.



| 그림 3-1-10 | 역할 그룹에 조건 설정

② 조직 보안(IP ACL) 설정하기

A. NHN Cloud의 가상자원을 관리하는 console에 대해 IP ACL을 적용할 수 있습니다.

B. [조직 》 조직 관리 》 조직 거버넌스 설정 》 IP ACL 설정]에서 IP ACL을 설정할 수 있습니다.

| 그림 3-1-11 | Console에 대한 IP ACL 설정

C. IP ACL 입력 실수로 접속에 문제가 생긴 경우 고객센터로 문의하여 지원을 받으실 수 있습니다.

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

- **(가상자원관리시스템)**

  ① NHN Cloud 계정과 IAM 계정의 차이

  A. ‘그림 3-1-1 NHN Cloud 계정 체계와 조직/프로젝트 역할 관계’에서 NHN Cloud의 계정은 NHN Cloud 계정과 IAM 계정으로 구분되어 있음을 확인하였습니다.

  B. 조직 및 프로젝트에서 NHN Cloud 계정을 초대하거나, IAM 계정을 생성하여 이용자별 개별 계정으로 인증을 적용할 수 있습니다.

  C. 먼저 NHN Cloud 계정과 IAM 계정의 차이에 대해 이해하고 각 계정을 초대/생성하는 방법을 알아보겠습니다.

요건	NHN Cloud 계정	IAM 계정
생성 방법	NHN Cloud 포탈 회원 가입	조직 관리자가 IAM 계정 생성
로그인 보안 설정 • *2-factor 인증* • *실패 횟수에 따른 잠금 시간 설정* • *로그인 세션 설정*	계정 소유자가 직접 설정 (2-factor 인증만 설정 가능)	조직 관리자가 설정 가능 [조직 관리 >> 거버넌스 설정]에서 IAM 전체 관리 정책 수립
PW 복잡도 정책 설정	불가 (NHN Cloud 정책에 따라 운영됨)	조직 관리자가 설정 가능 [조직 관리 >> 거버넌스 설정]에서 IAM 전체 비밀번호 관리 정책 수립
접속 URL	Console.nhncloud.com	조직도메인.console.nhncloud.com
타 인증 서비스 연동 가능 여부	불가	가능

| 그림 3-2-1 | NHN Cloud 계정과 IAM 계정의 보안 설정 차이

D. '그림 3-2-1 NHN Cloud 계정과 IAM 계정의 보안 설정 차이'에서 NHN Cloud 계정과 IAM 계정의 주요한 차이에 대해 설명하였습니다.

NHN Cloud 계정은 조직에 묶여 있지 않고, NHN Cloud 서비스를 이용하는 계정입니다. 하나의 계정으로 여러 조직에 속하여 서비스를 이용할 수 있고, 조직이 삭제되어도 계정이 유지될 수 있습니다.

IAM 계정은 조직에 묶여 있는 계정으로, 조직 관리자가 자신의 조직 내에서만 사용할 계정을 만들어 운용합니다. 따라서 조직이 삭제되면 IAM 계정 또한 삭제됩니다.

E. 전부 NHN Cloud 계정으로 구성원을 구성할 수도 있고, 조직 OWNER 외 전부 IAM 계정으로 생성하여 관리할 수도 있습니다.

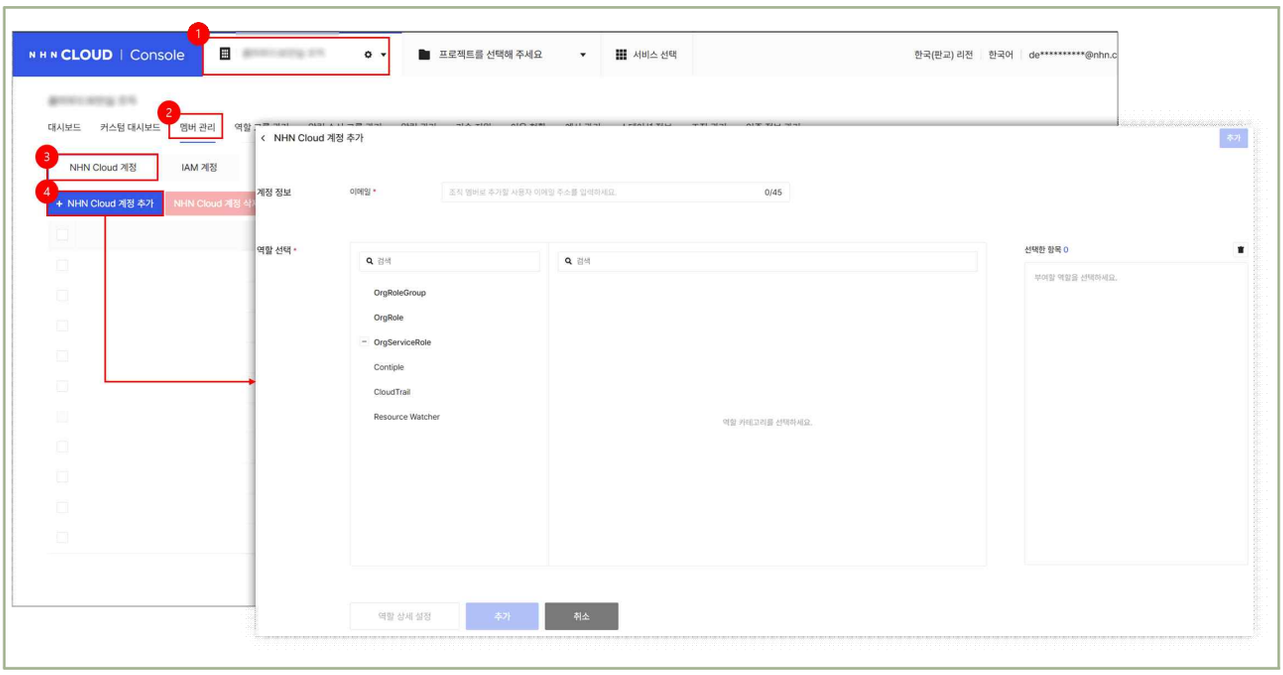
계정의 특성에 맞게 설정하여 운영하는 것이 중요한데, 보안을 고려하여 최소한의 관리자만 NHN Cloud 계정으로 초대하고, 나머지는 IAM 계정으로 사용자를 등록하여 보안 설정을 세세하게 적용하는 식으로 운용할 수 있습니다.

② NHN Cloud 계정 추가하기

A. 조직/프로젝트 대상에 맞게 NHN Cloud 계정을 추가할 수 있습니다.

B. [조직/프로젝트 〉〉 멤버관리 〉〉 NHN Cloud 계정 〉〉 NHN Cloud 계정 등록]으로 NHN Cloud 계정을 초대할 수 있습니다.

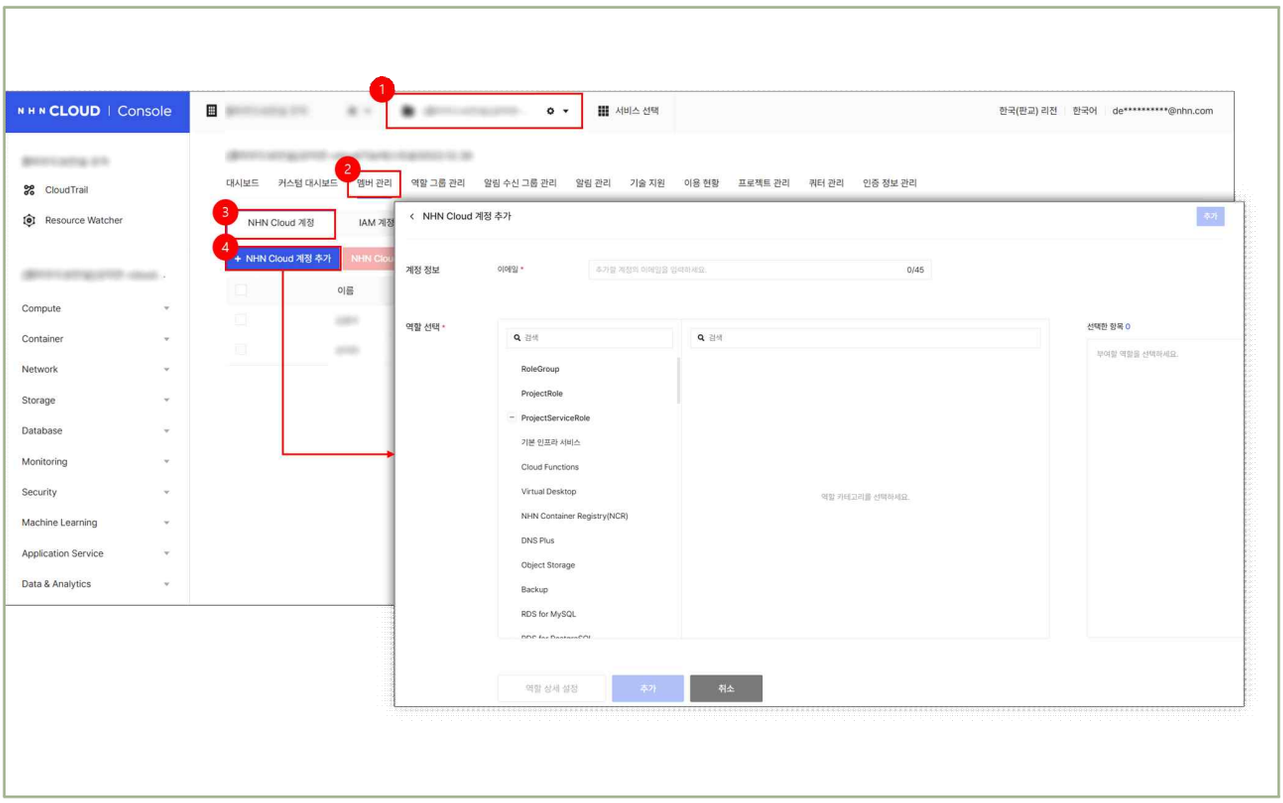
사용자 정보는 회원가입 시 기입했던 정보로 적용됩니다.



| 그림 3-2-2 | 조직 멤버로 NHN Cloud 계정 초대

C. [프로젝트 〉〉 멤버관리]에서 해당 프로젝트의 서비스별 권한을 부여/회수 할 수 있습니다.

※ compute, network 등의 IaaS 서비스는 '기본 인프라 서비스'로 통합 제공됩니다.



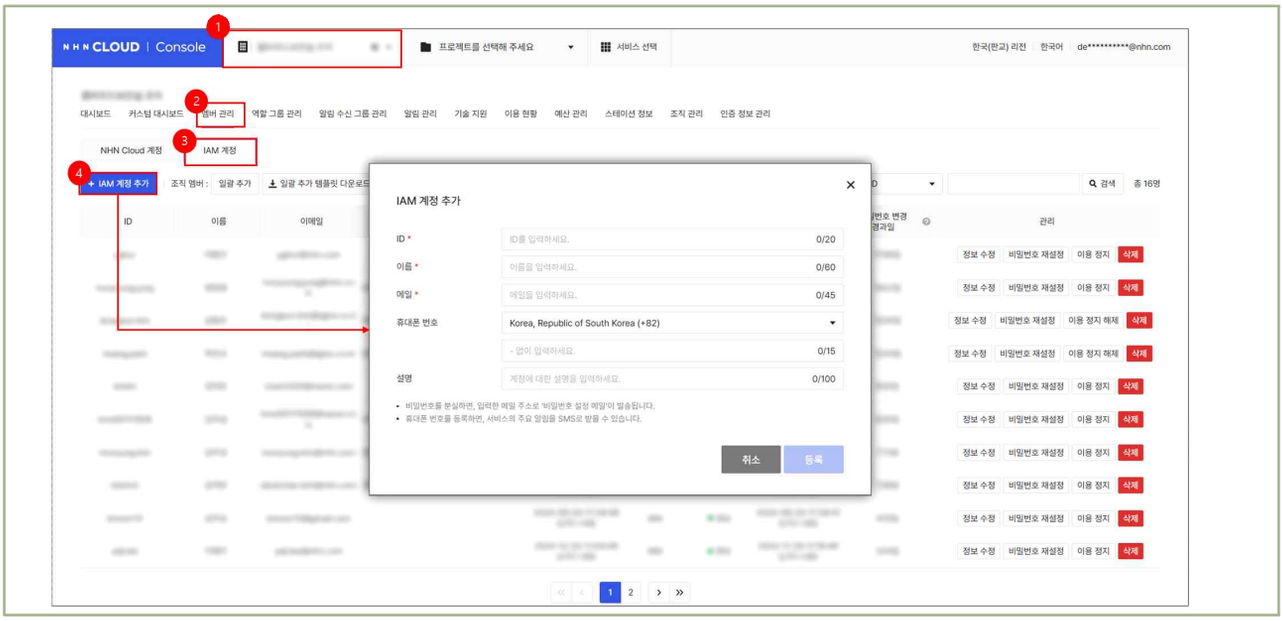
| 그림 3-2-3 | 프로젝트 멤버로 NHN Cloud 계정 초대

③ IAM 계정 추가하기

A. 조직/프로젝트 대상에 맞게 IAM 계정을 추가할 수 있습니다.

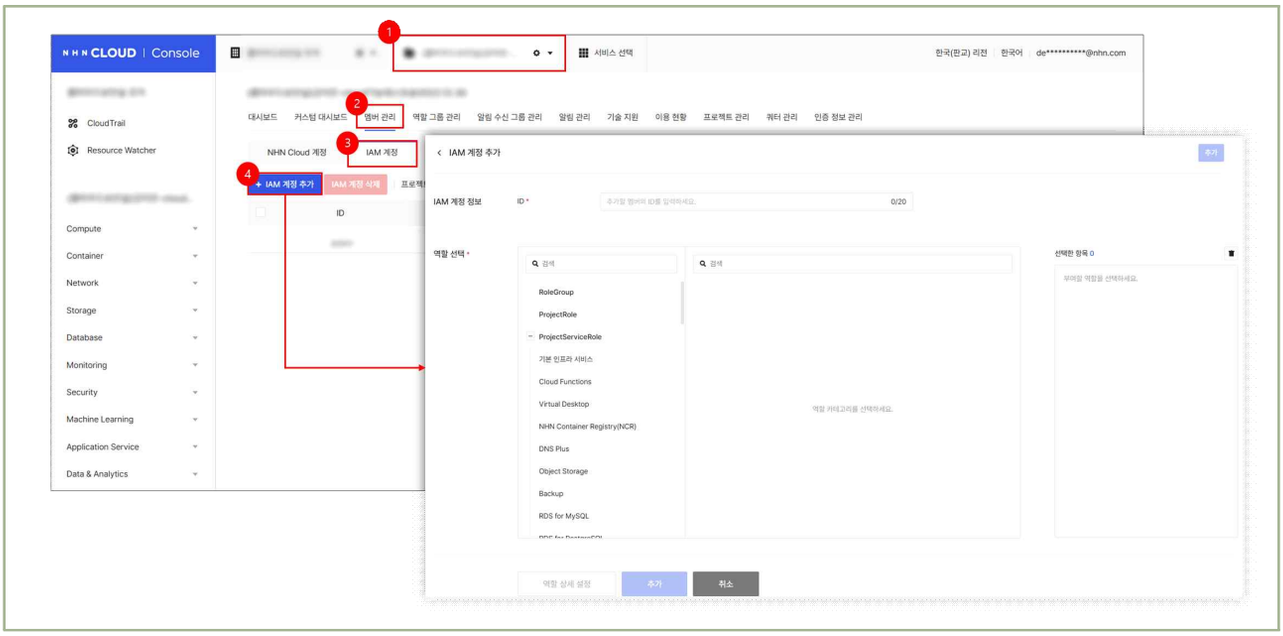
다만 프로젝트에 IAM 계정을 초대하기 위해서는 조직에 IAM 계정을 먼저 등록하여야 하며, 조직 역할은 '역할 없음'이 초기 셋팅으로 설정되어 있습니다.

B. 사용자 정보는 조직 관리자가 입력하는 정보(ID, 이름, 메일, 휴대폰 번호)로 적용됩니다.



| 그림 3-2-4 | 조직 멤버로 IAM 계정 등록

C. [프로젝트 〉〉 멤버관리]에서 해당 프로젝트의 서비스별 권한을 부여/회수 할 수 있습니다.



| 그림 3-2-5 | 프로젝트 멤버로 IAM 계정 등록

④ SSO 연동하기

A. NHN Cloud의 IAM 계정의 경우 SSO 연동하여 이용할 수 있습니다.

B. SAML 2.0, OIDC 등의 연동이 가능하며, 연동이 필요할 시 사업담당자 또는 고객센터를 통해 문의 부탁드립니다.

⑤ 계정 별 MFA 설정

A. NHN Cloud 계정의 경우 개별 설정이 필요하며, IAM 계정의 경우 조직 관리 메뉴에서 일괄 설정이 가능합니다.

B. NHN Cloud 계정 및 IAM 계정의 이메일, 휴대폰 또는 Google OTP 설정 방법과 관련해서는 '3.4클라우드 가상자원 관리 시스템 관리자 권한 추가인증 적용'을 참조하시기 바랍니다.

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

- **(가상자원관리시스템)**

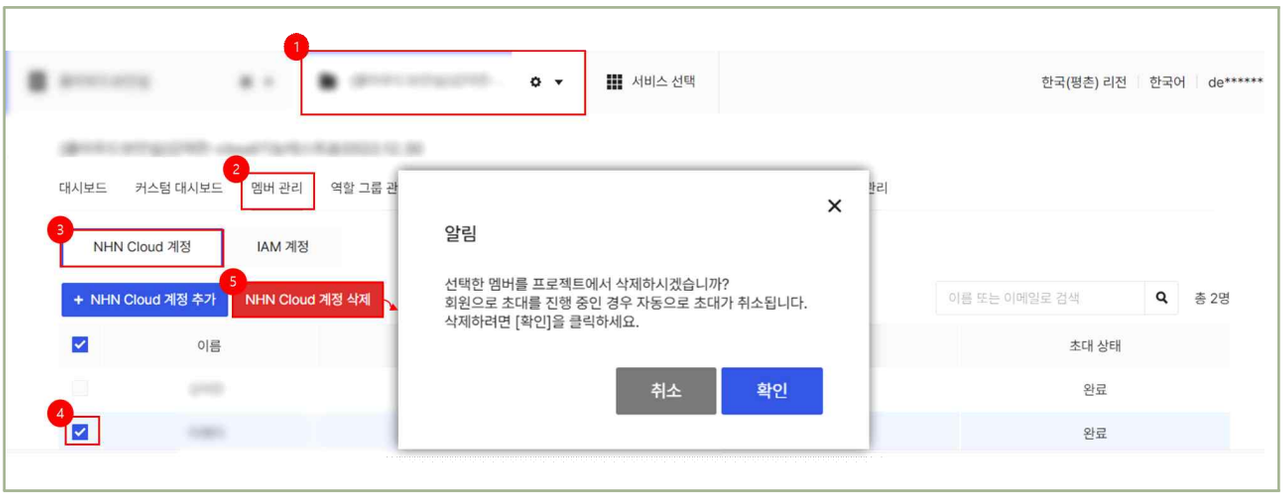
  - NHN Cloud 계정은 조직 또는 프로젝트와 상관없이 NHN Cloud의 서비스를 이용하는 계정이기에 조직 관리자가 계정을 삭제할 수는 없습니다.

    다만 조직 및 프로젝트에 더 이상 접속하지 못하도록 설정하는 것이 가능하며, IAM 계정은 조직 관리자가 계정을 정지 또는 삭제하는 것이 가능합니다.

① NHN Cloud 계정 삭제하기

A. 프로젝트에서 NHN Cloud 계정 삭제하기

가. [프로젝트 〉〉 멤버 관리 〉〉 NHN Cloud 계정]에서 삭제하고자 하는 NHN Cloud 계정을 선택하고, ‘NHN Cloud 계정 삭제’를 클릭하면 계정의 삭제가 가능합니다.

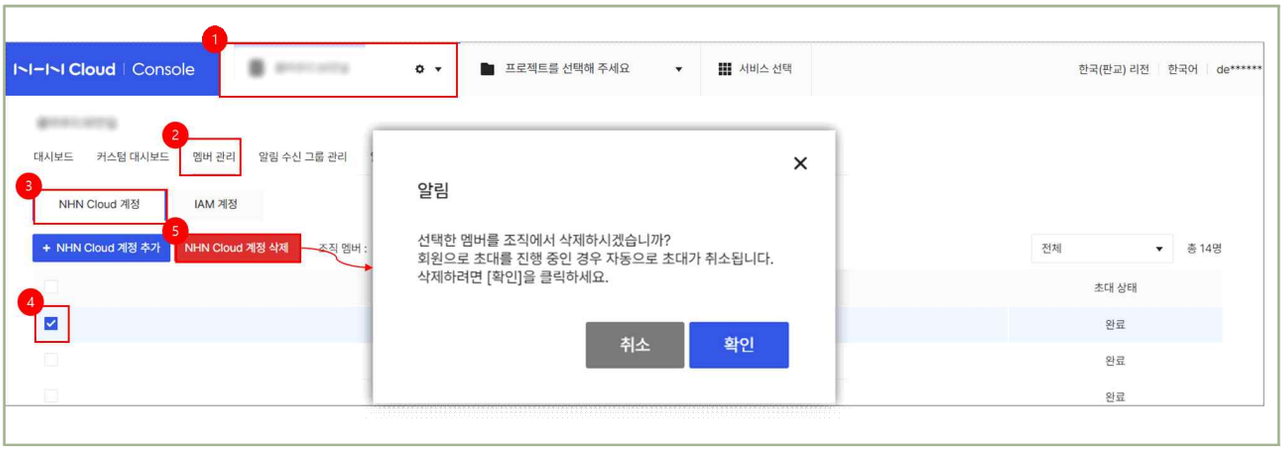


| 그림 3-3-1 | 프로젝트에서 NHN Cloud 계정 삭제하기

B. 조직에서 NHN Cloud 계정 삭제하기

가) [조직 〉〉 멤버 관리 〉〉 NHN Cloud 계정]에서 NHN Cloud 계정을 삭제할 수 있습니다.

나) 삭제 시 원복이 불가하며, 다시 초대하여 설정을 진행하여야 합니다.

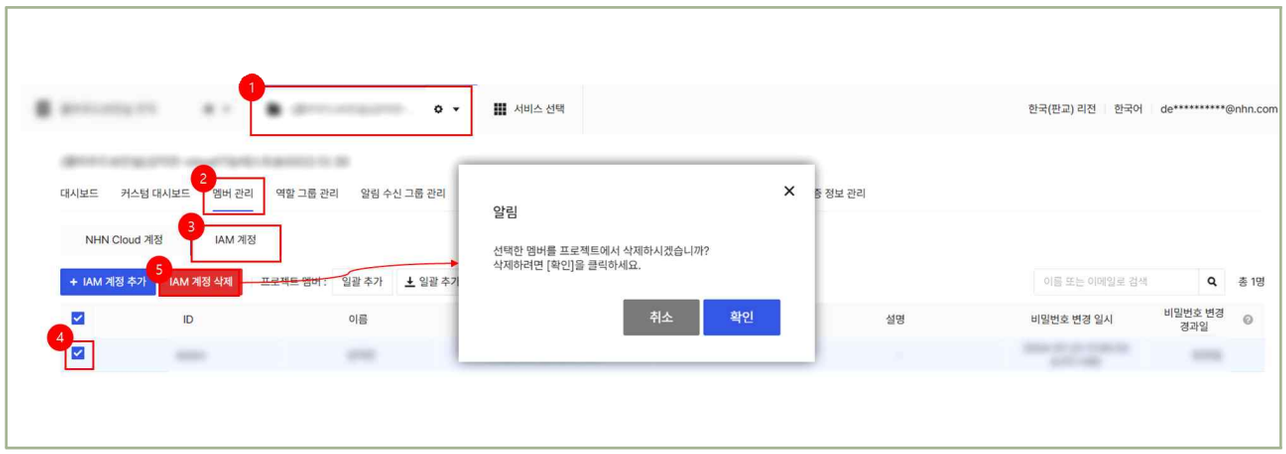


| 그림 3-3-2 | 조직에서 NHN Cloud 계정 삭제하기

② IAM 계정 삭제하기

A. 프로젝트에서 IAM 계정 삭제하기

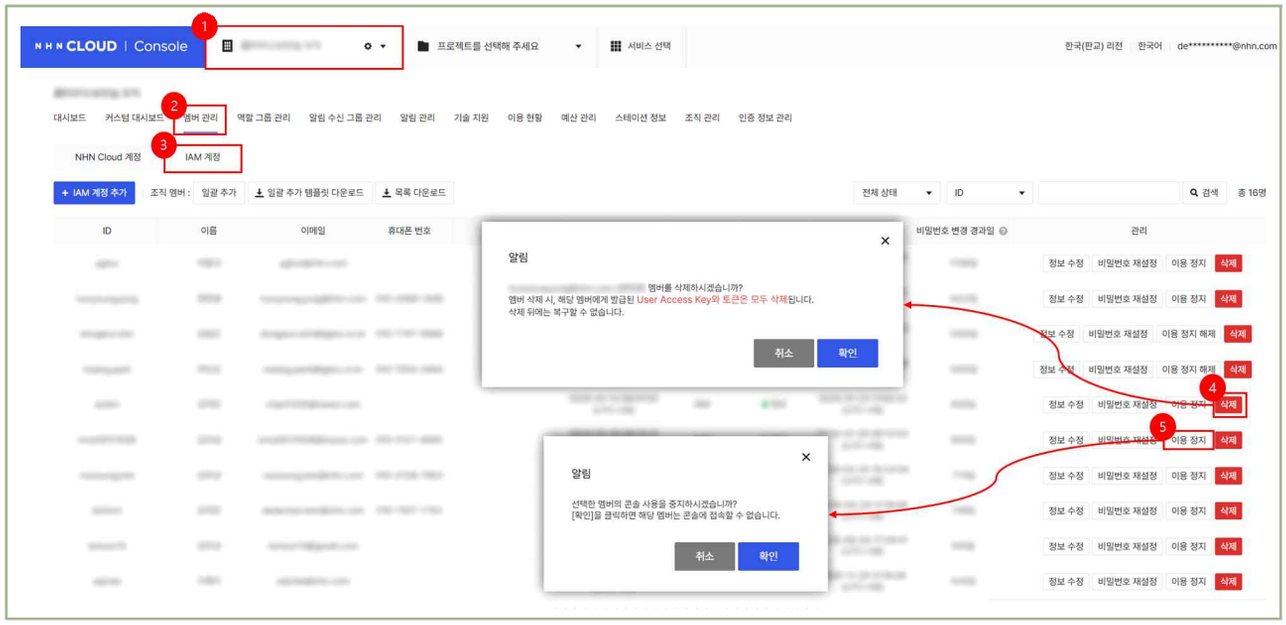
가) [프로젝트 〉〉 멤버 관리 〉〉 IAM 계정]에서 IAM 계정을 선택하여 삭제를 진행할 수 있습니다.



| 그림 3-3-3 | 프로젝트에서 IAM 계정 삭제하기

B. 조직에서 IAM 계정 정지/삭제하기

가) [조직 〉〉 멤버 관리 〉〉 IAM 계정]에서 IAM 계정을 이용 중지 또는 삭제할 수 있습니다.

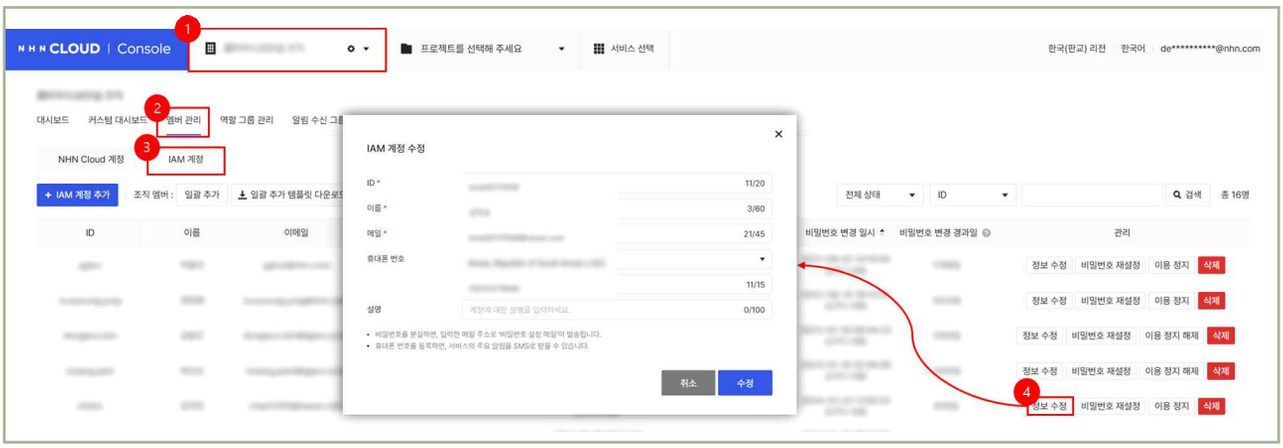


| 그림 3-3-4 | 조직에서 IAM 계정 정지/삭제하기

③ IAM 계정 비밀번호설정 메일링 보내기

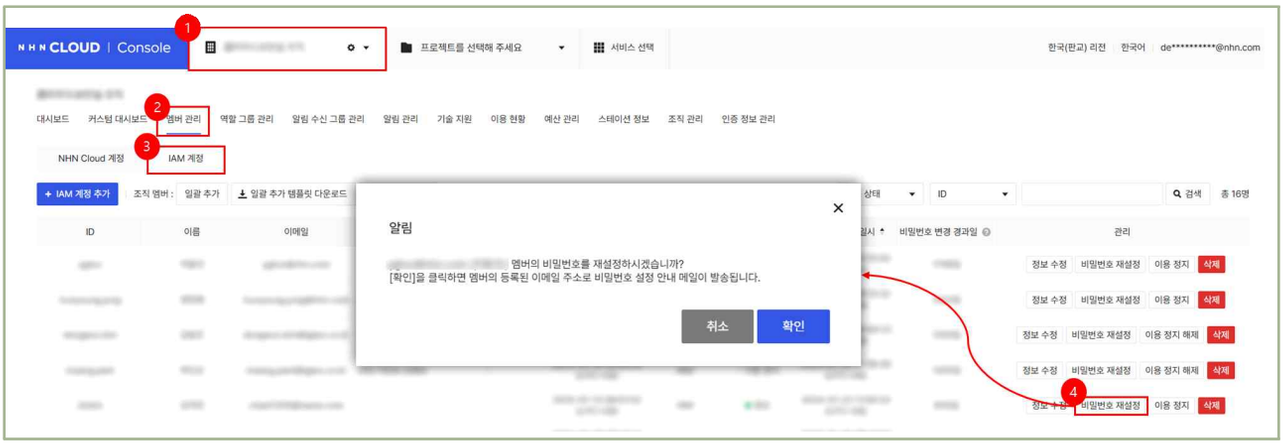
- 공용 계정 등의 용도로 사용하던 IAM 계정의 사용자가 변경되는 경우 정보를 변경하고 비밀번호 재설정 메일을 보낼 수 있습니다.

A. [조직 〉〉 멤버 관리 〉〉 IAM 계정]에서 정보 수정을 클릭하여 메일 주소, 휴대폰 번호 등의 2차 인증을 위한 정보를 수정할 수 있습니다.



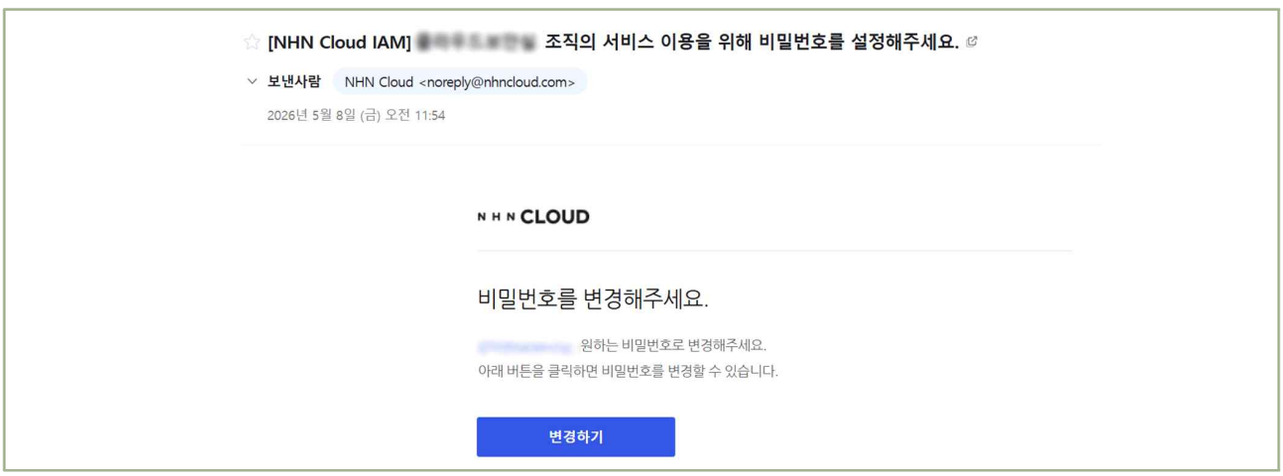
| 그림 3-3-5 | IAM 계정의 이용자 정보 수정

B. 이용자의 메일 주소를 변경한 후 '비밀번호설정 메일링'을 클릭하여 비밀번호 재설정 메일을 전송할 수 있습니다.



| 그림 3-3-6 | IAM 계정 비밀번호 재설정 메일 발송

C. 메일은 정보에 등록된 메일 주소로 발송되며, 메일 본문의 '변경하기'를 클릭하여 비밀번호를 변경할 수 있습니다.



| 그림 3-3-7 | IAM 계정 비밀번호 변경 안내 메일

1 기준

식별번호	기준	내용
3.4.	**클라우드 가상자원 관리 시스템 관리자 권한 추가 인증 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

- **(가상자원관리시스템)**

  ① NHN Cloud 계정 추가 인증수단 적용

  A. NHN Cloud 계정의 보안 설정 로그인 후 화면 오른쪽 위 접속 계정을 클릭한 후, 로그인 보안 설정을 클릭하여 보안 설정을 위한 페이지를 열람합니다.

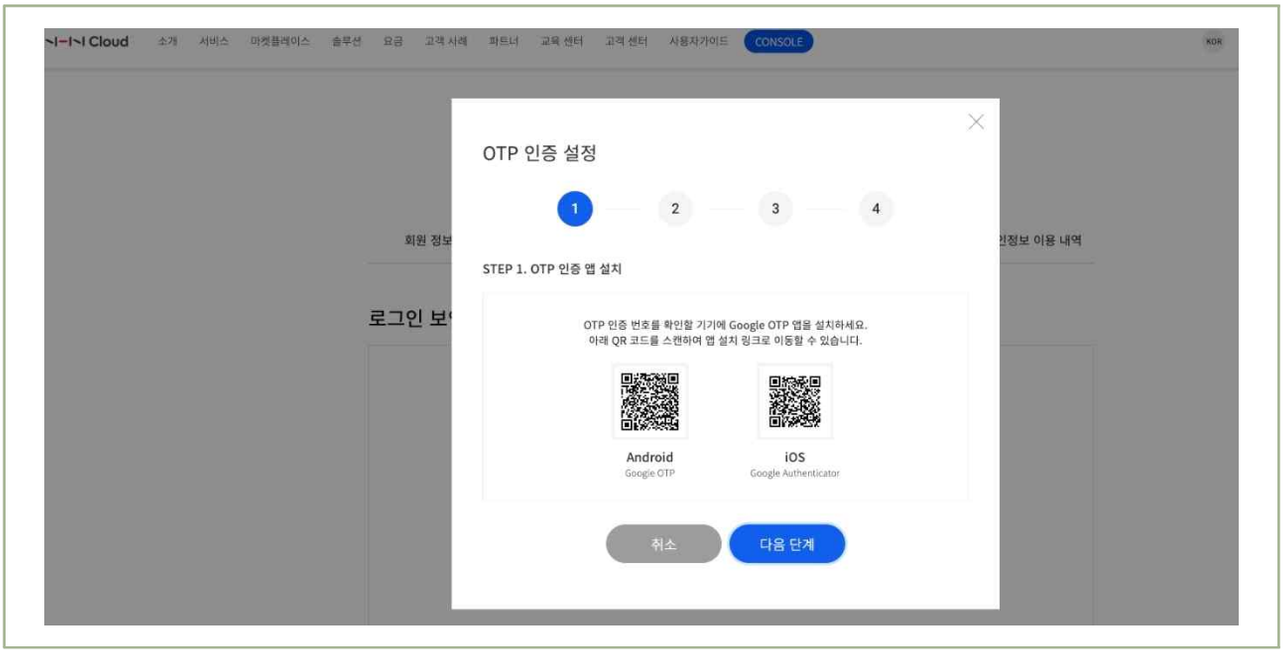
  열람 시 비밀번호 확인을 위해 다시 한번 비밀번호를 입력하도록 요청합니다.

| 그림 3-4-1 | NHN Cloud 계정 로그인 보안 설정

B. 변경 버튼을 눌러 '이메일 또는 휴대폰으로 인증 후 로그인', 'Google OTP 인증 후 로그인' 설정 중 원하는 보안 방법을 선택한 후 저장을 클릭합니다.

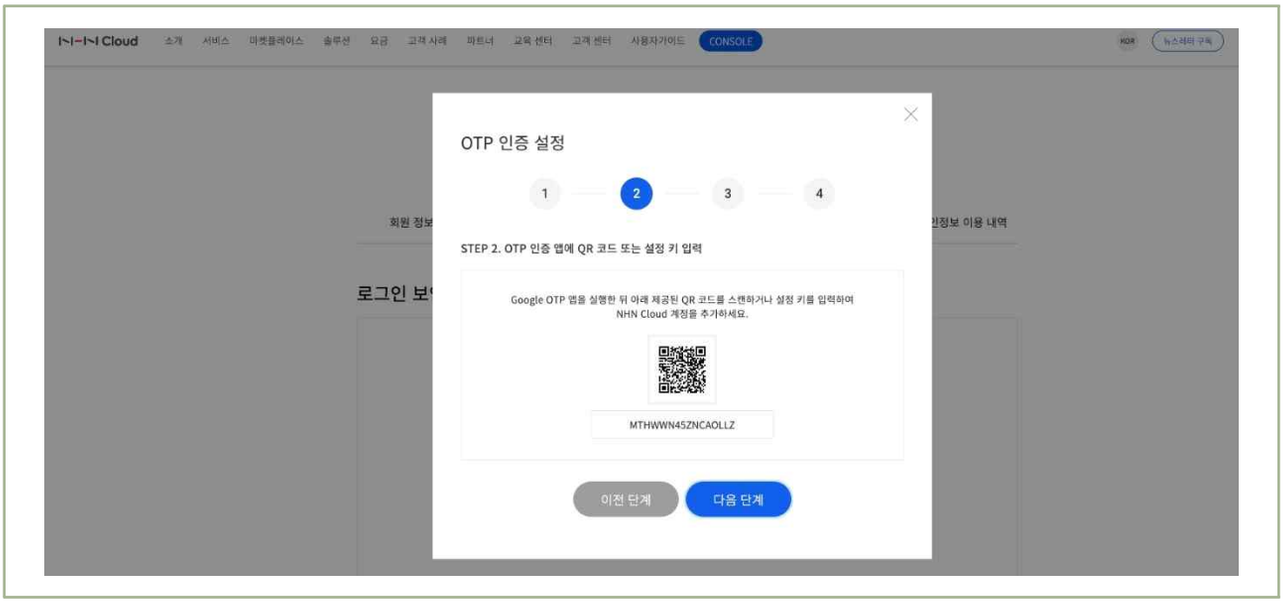
C. Google OTP를 선택한 경우 다음과 같은 절차로 등록을 진행합니다.

가) OTP 인증 앱을 설치합니다.



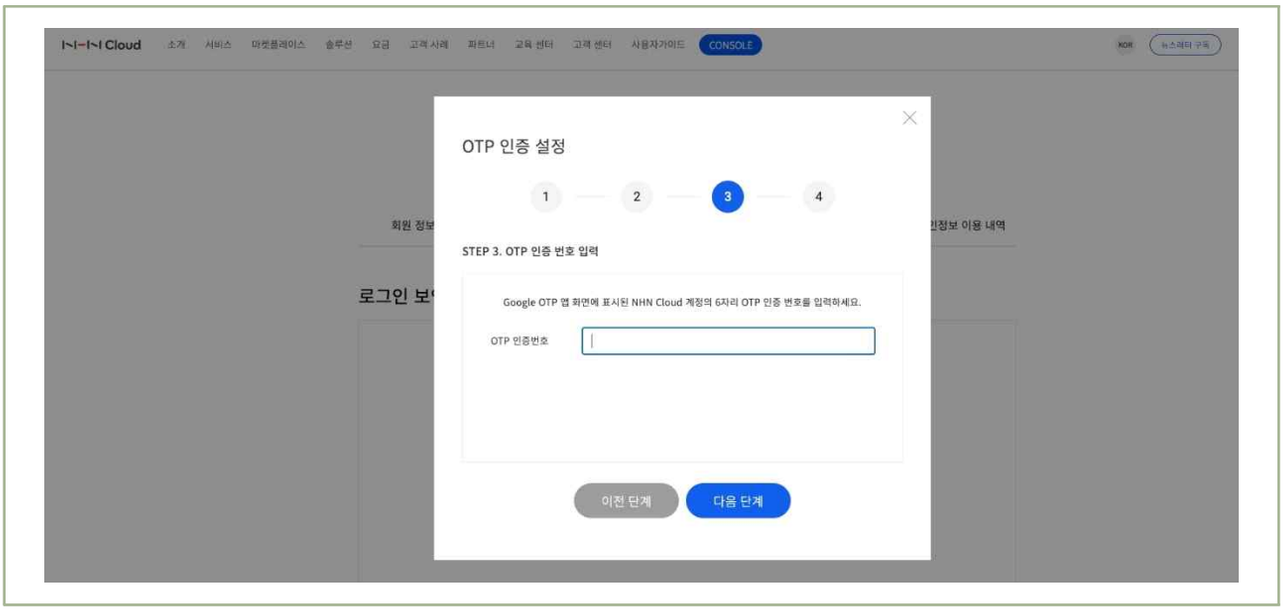
| 그림 3-4-2 | OTP 인증 앱 설치

나) OTP 인증 앱에 NHN Cloud 계정을 추가합니다.



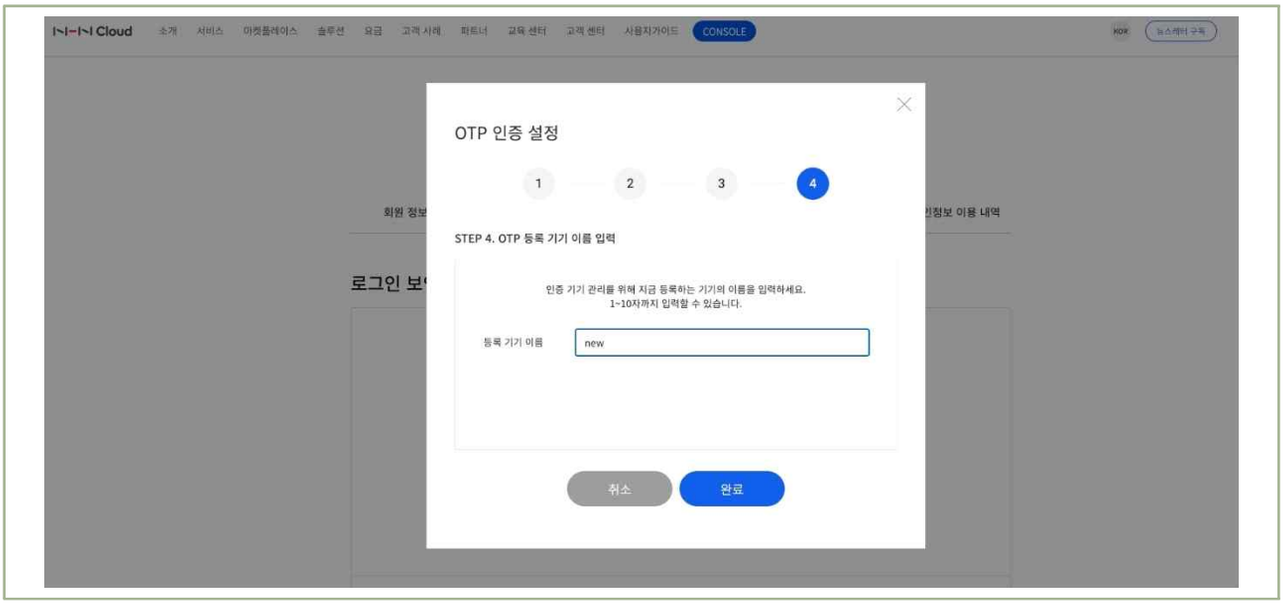
| 그림 3-4-3 | NHN Cloud 계정 추가

다) OTP 인증 앱 화면에 표시된 NHN Cloud 계정의 인증번호를 입력합니다.



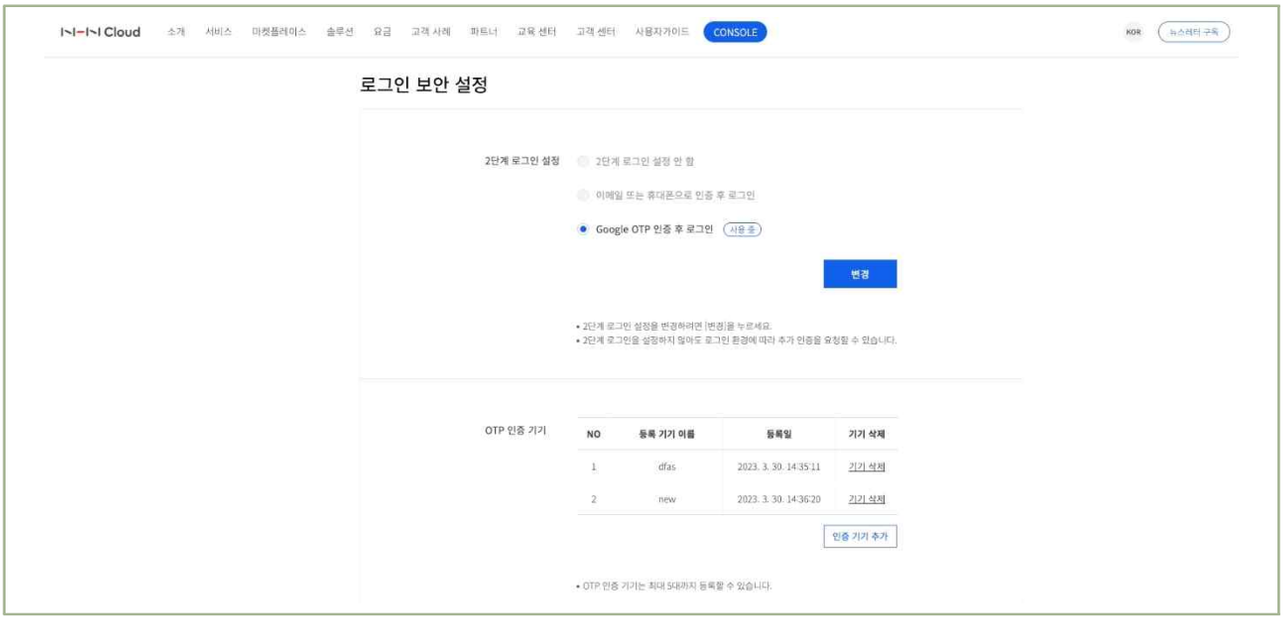
| 그림 3-4-4 | NHN Cloud 계정 인증번호 입력

라) OTP 등록 기기 명을 입력합니다.



| 그림 3-4-5 | OTP 등록 기기 명 입력

마) OTP 인증 설정이 완료되면 OTP 인증 기기 리스트에 등록된 기기가 표시됩니다.

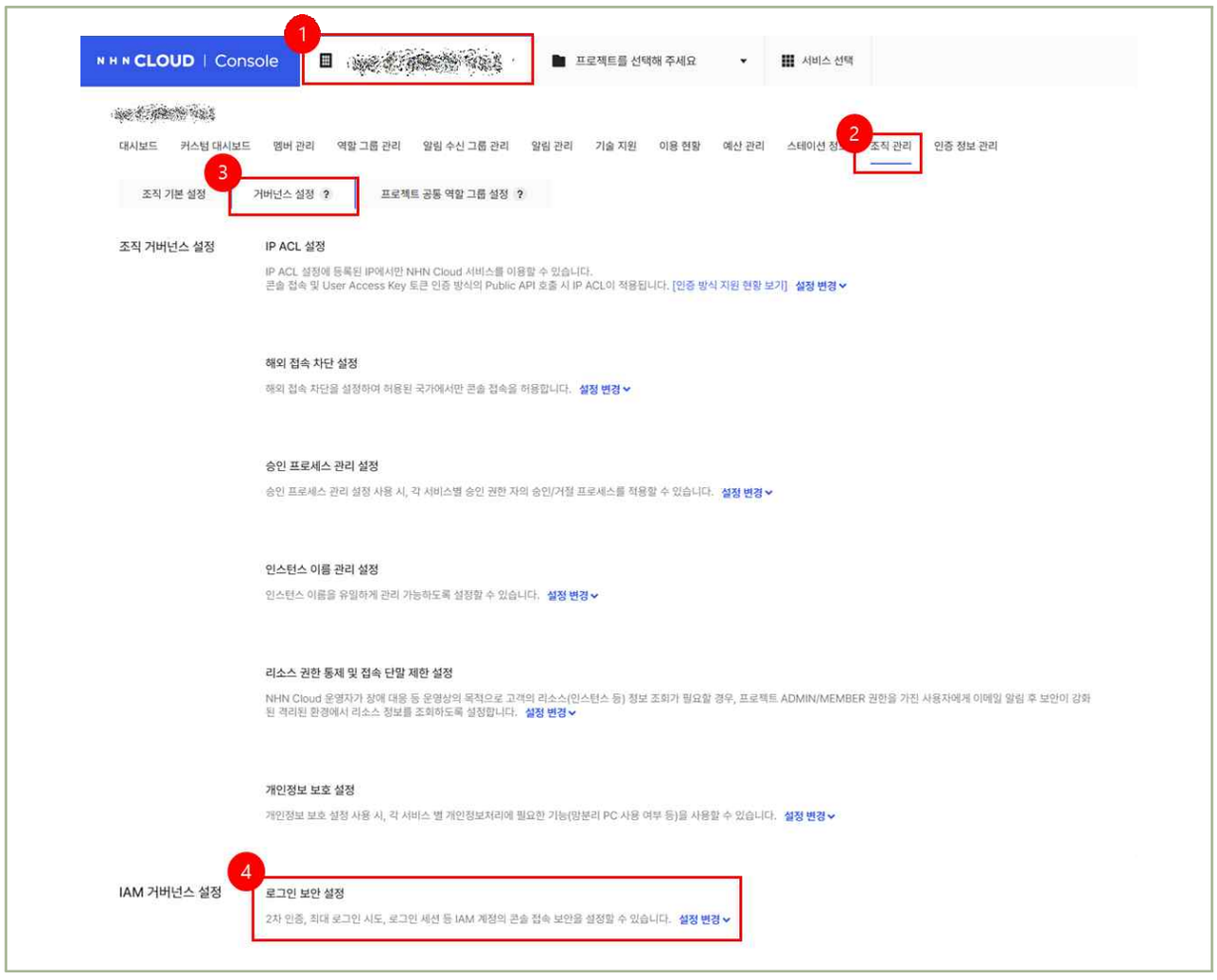


| 그림 3-4-6 | OTP 인증 기기 리스트 조회

② IAM 계정 추가인증 수단 적용

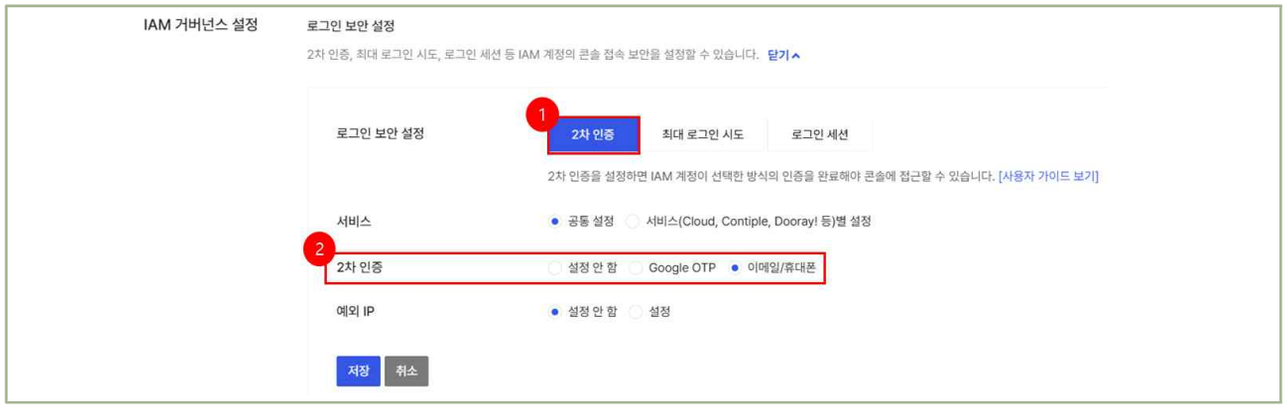
A. IAM 계정의 추가인증 수단 적용은 조직의 OWNER 또는 ADMIN 권한만 가능합니다.

B. [조직 〉〉 조직 관리 〉〉 거버넌스 설정 〉〉 IAM 거버넌스 설정]에서 '로그인 보안 설정'의 설정 변경을 클릭합니다.



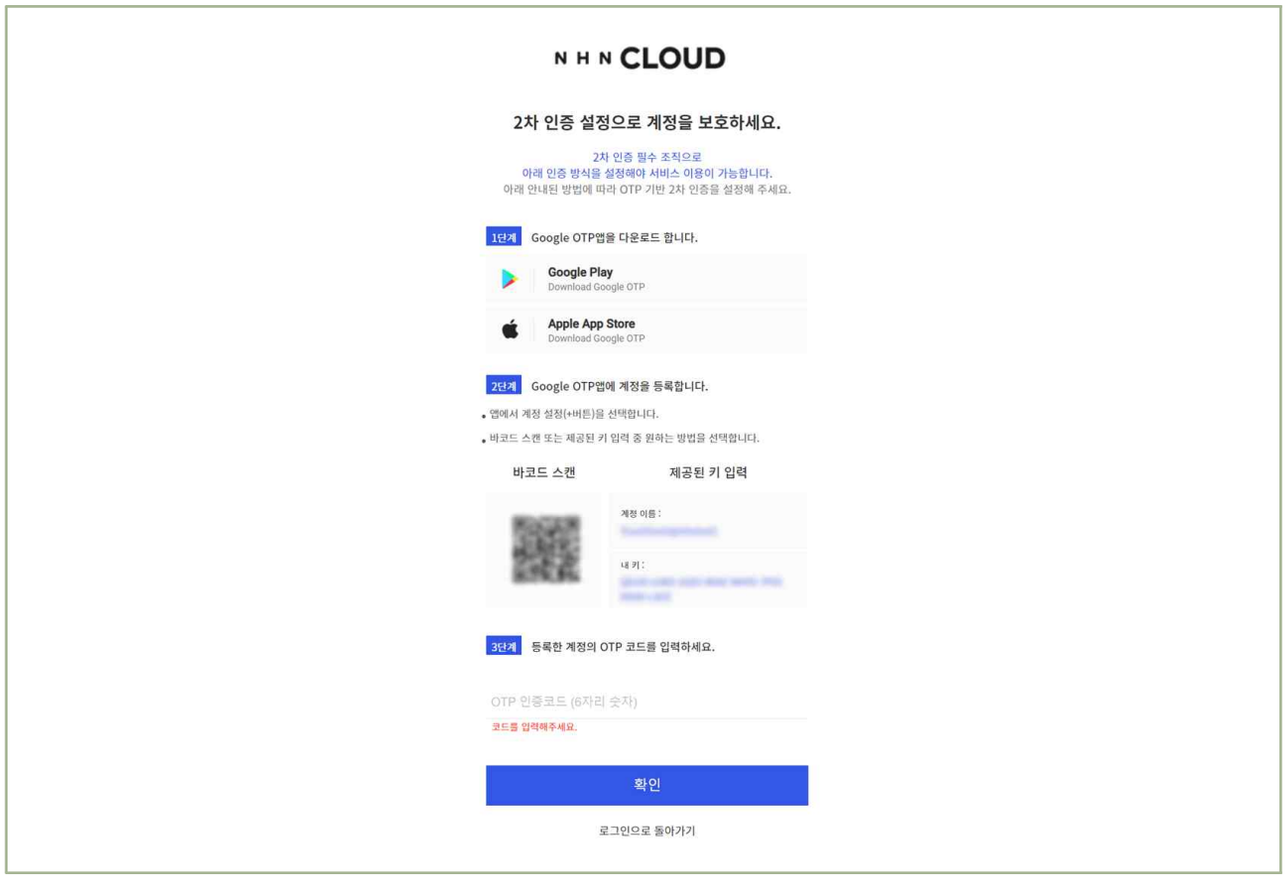
| 그림 3-4-7 | IAM 추가인증 수단 적용 메뉴

C. 로그인 보안 설정 메뉴 중 '2차 인증'을 클릭하여 2차 인증 수단을 설정합니다.



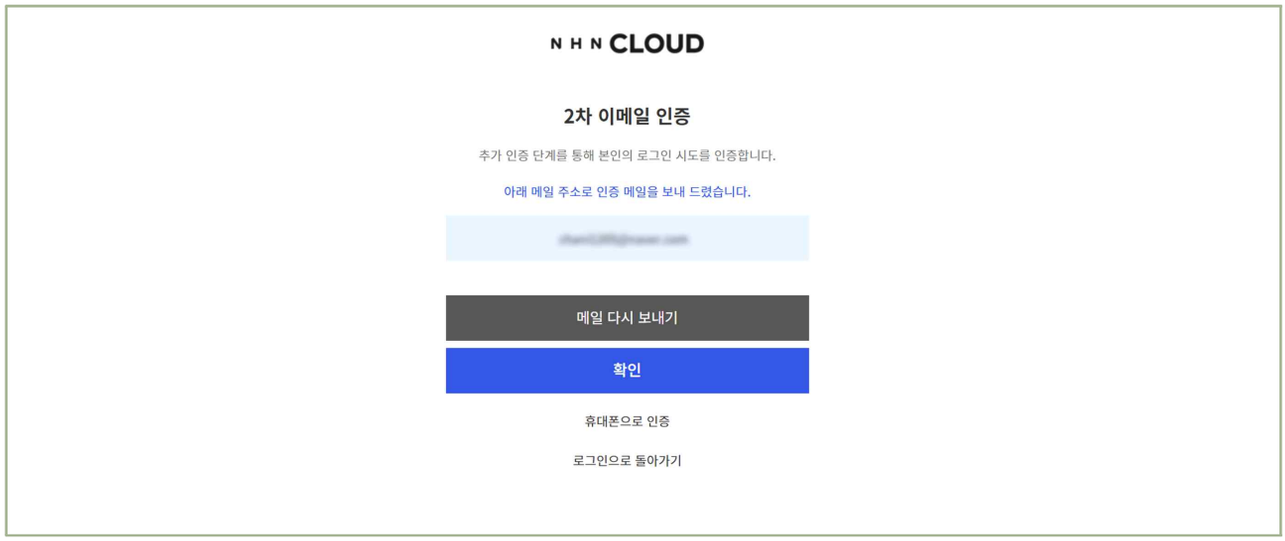
| 그림 3-4-8 | IAM 추가인증 수단 적용

D. Google OTP를 선택하게 되면 IAM 계정 로그인 후 Google OTP 설치 관련 안내창으로 이동합니다.



| 그림 3-4-9 | IAM 계정 Google OTP 설치 안내 페이지

E. 이메일/휴대폰을 선택한 경우 해당 매체의 인증을 요청합니다.



| 그림 3-4-10 | 이메일/휴대폰 인증 페이지

F. 해당 인증을 완료한 후 IAM 계정으로 접속할 수 있습니다.

1 기준

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

2 설명

- 클라우드 가상자원 관리시스템 계정에 대한 로그인 규칙을 수립하여야 한다.

  - 예시

    1) 로그인 오류에 따른 보안통제 방안 수립(5회이상 로그인 실패 시 계정 잠김 등)

3 우수 사례

- **(가상자원관리시스템)**

  ① NHN Cloud 계정 로그인 보안 설정

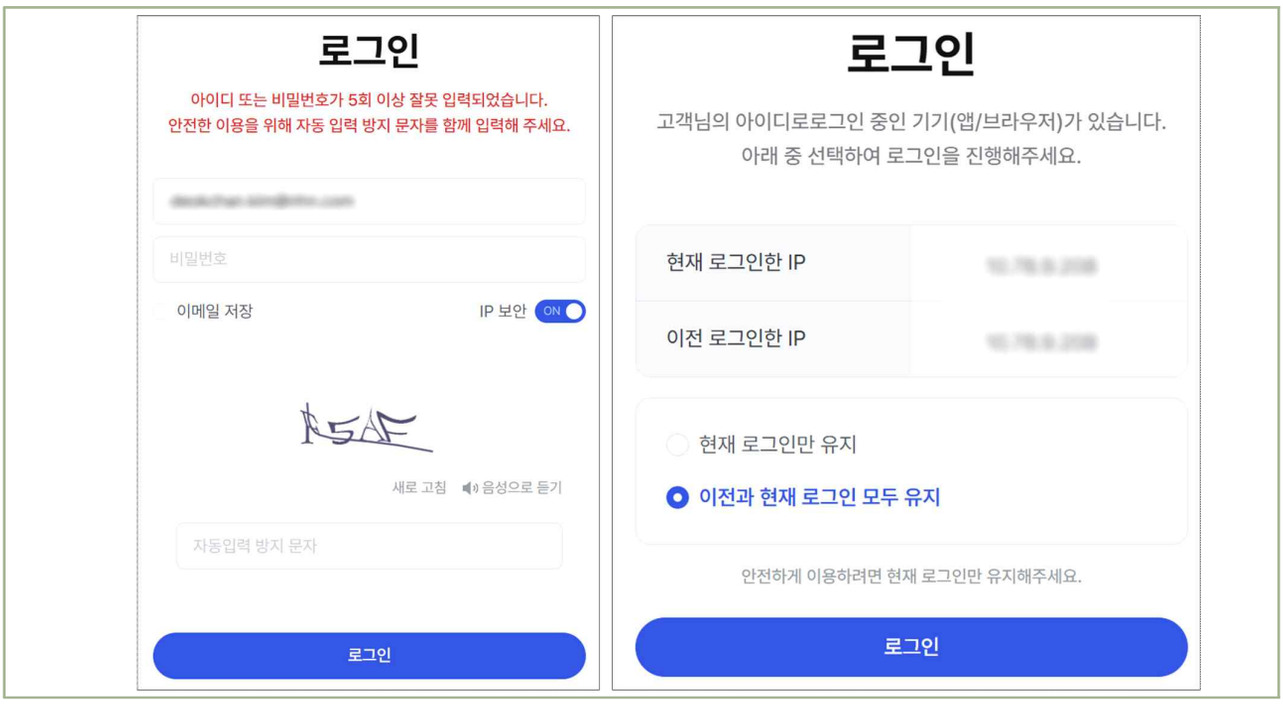
  - NHN Cloud 계정의 경우 2차인증 외 로그인 설정을 변경할 수 없으며, NHN Cloud의 포탈 정책에 따라 운영됩니다.

  ※ NHN Cloud 포탈 로그인 정책

  ㄱ. 로그인 실패 정책 : 5회 실패 시 captcha 입력 추가

  ㄴ. 세션 유지 시간 : 6시간

  ㄷ. 중복 로그인 : 허용(신규 로그인 창에서 기존 로그인 유지할 것인지 선택)



| 그림 3-5-1 | NHN Cloud 계정의 콘솔 로그인 정책

② IAM 계정 로그인 보안 설정

A. IAM 계정의 경우 [조직 〉〉 조직 관리 〉〉 거버넌스 설정 〉〉 IAM 거버넌스 설정]에서 로그인 보안 정책을 설정할 수 있습니다.

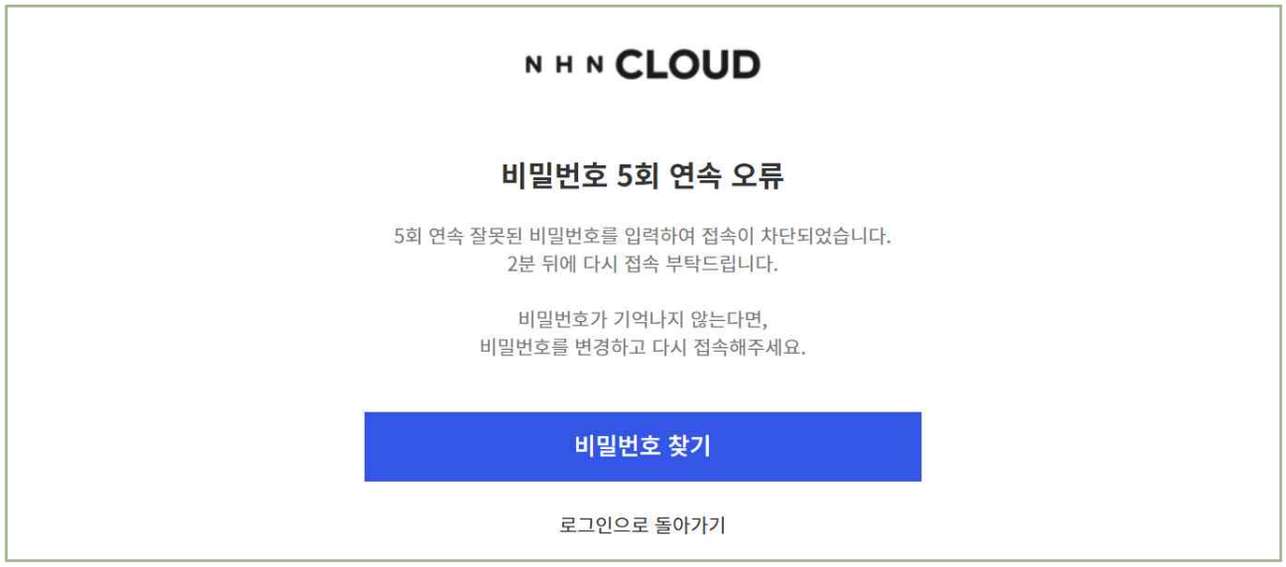
B. 로그인 보안 설정은 '2차 인증', '최대 로그인 시도', '로그인 세션' 3가지를 설정할 수 있습니다.

C. 회사의 컴플라이언스 및 보안 수준에 따라 적용 수치는 달라질 수 있으나, 2차 인증은 '설정', 최대 로그인 시도는 '설정 – 5회/10분', 로그인 세션은 '로그인 세션 수 1개, 로그인 세션 유지시간 10~60분'을 권고 드립니다.

| 그림 3-5-2 | IAM 로그인 보안 설정, 2차 인증 설정

| 그림 3-5-3 | IAM 로그인 보안 설정, 최대 로그인 시도 설정

| 그림 3-5-4 | IAM 로그인 보안 설정, 로그인 세션 설정



| 그림 3-5-5 | IAM 계정 로그인 실패 화면

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

- **(가상자원관리시스템)**

  ① NHN Cloud 계정 비밀번호 규칙

  - NHN Cloud 계정의 경우 비밀번호 규칙을 변경할 수 없으며, NHN Cloud의 포탈 정책에 따라 운영됩니다

  ※ NHN Cloud 포탈 비밀번호 정책

  ㄱ. 영문, 숫자, 특수문자 3조합

  ㄴ. 최소 8자리 이상

  ㄷ. 4자리 이상의 동일한 숫자 금지

  ② IAM 계정 비밀번호 규칙

  A. [조직 〉〉 조직 관리 〉〉 거버넌스 설정 〉〉 IAM 거버넌스 설정]에서 IAM 계정의 비밀번호 정책을 설정할 수 있습니다.

  B. 기본 비밀번호 정책을 그대로 사용할 수 있고, 세부 설정을 변경 적용할 수 있는 '사용자 비밀번호 정책'으로 선택하여 사용할 수 있습니다.

C. 별도의 사내 보안 정책이 없다면 기본 비밀번호 정책으로, 사내 보안 정책과 기본 비밀번호 정책이 상이하다면 사용자 비밀번호 정책으로 설정하여 기준을 강화합니다.

| 그림 3-6-1 | IAM 계정 기본 비밀번호 정책

| 그림 3-6-2 | IAM 계정 사용자 비밀번호 정책

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

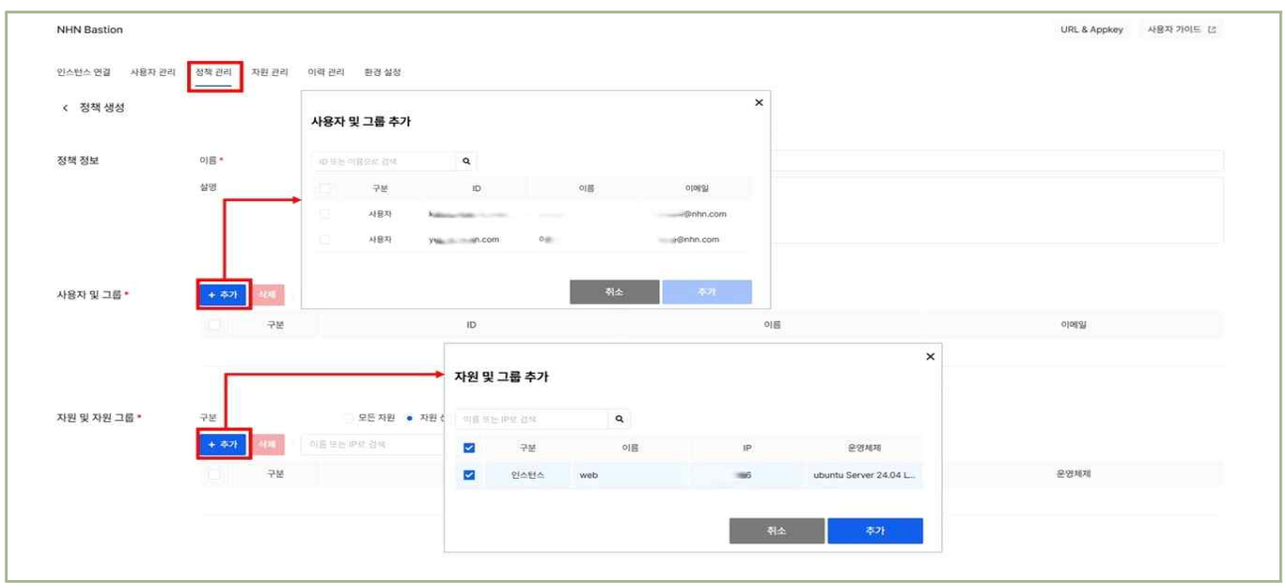
    2) 공개용 웹서버에 접근 가능한 계정으로 로그인 시 추가인증 수단 적용 등

3 우수 사례

- **(가상자원관리시스템)**

  ① NHN Bastion 서비스 활용

  - NHN Bastion 서비스를 활용하여 공개용 웹서버에 접근하는 계정을 제한하고 명령어 통제 정책 등을 적용할 수 있습니다. 인스턴스에 접근할 수 있는 계정을 정책에 추가하여 공개된 웹서버 등에 관리자 또는 운영자만 접근 가능하도록 설정할 수 있습니다.



| 그림 3-7-1 | NHN Bastion을 통한 인스턴스 접근 계정 추가

| 그림 3-7-2 | 인스턴스 접근 통제 정책

4 참고 사항

- 마켓플레이스 내 3rd-party 「서버접근제어 솔루션」을 사용하면 서버 접근 시 OTP 등의 추가 인증을 적용하는 것이 가능합니다.
- NHN Cloud 마켓플레이스

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

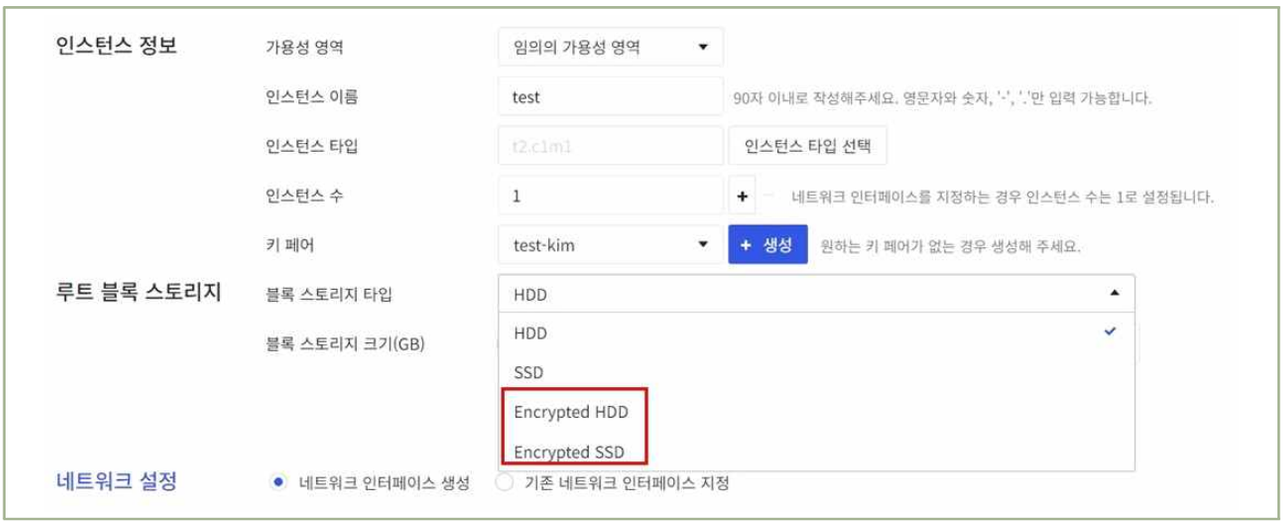
3 우수 사례

- **(가상자원관리시스템)**

  ① Block storage 암호화

  A. Instance 생성 시 루트 블록 스토리지에 대한 스토리지 타입을 설정할 수 있으며, 암호화 타입을 선택하여 볼륨에 대한 암호화를 설정할 수 있습니다.

  B. Instance 생성 메뉴에서 '루트 블록 스토리지'의 블록 스토리지 타입에서 암호화 타입을 선택할 수 있습니다.



| 그림 4-1-1 | Instance 생성 시 루트 블록 스토리지 암호화 타입 선택

C. 'Encrypted HDD/SSD' type 생성 시 NHN Cloud의 SKM 서비스로 생성한 대칭키 ID를 입력합니다.

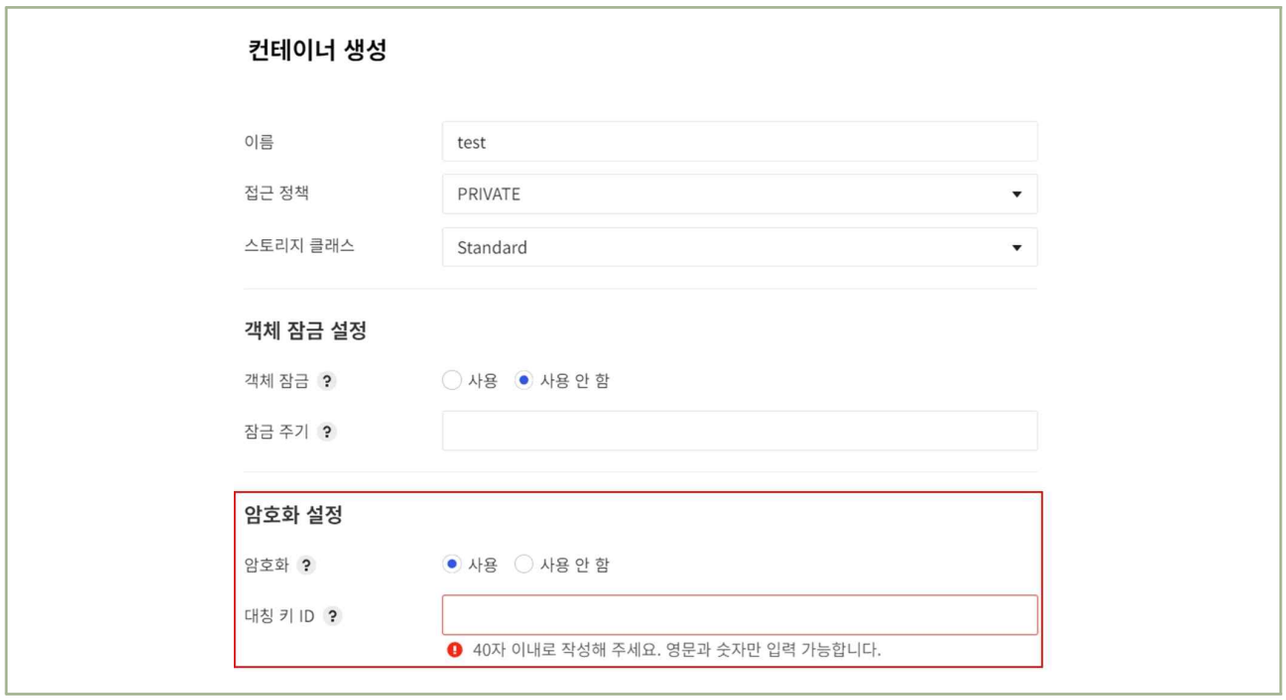
| 그림 4-1-2 | Secure Key Manager(SKM) 서비스에서 대칭키 ID 확인

| 그림 4-1-3 | 암호화 블록 스토리지 생성 시 대칭 키 ID 입력

D. 암호화 블록 스토리지 생성에 사용한 '대칭키'를 삭제하는 경우, 해당 블록 스토리지를 복호화 할 수 없으니 이용에 주의합니다.

② Object storage 암호화

A. Object storage 컨테이너 생성 시 SKM 서비스의 대칭키를 이용하여 암호화 설정을 할 수 있습니다.

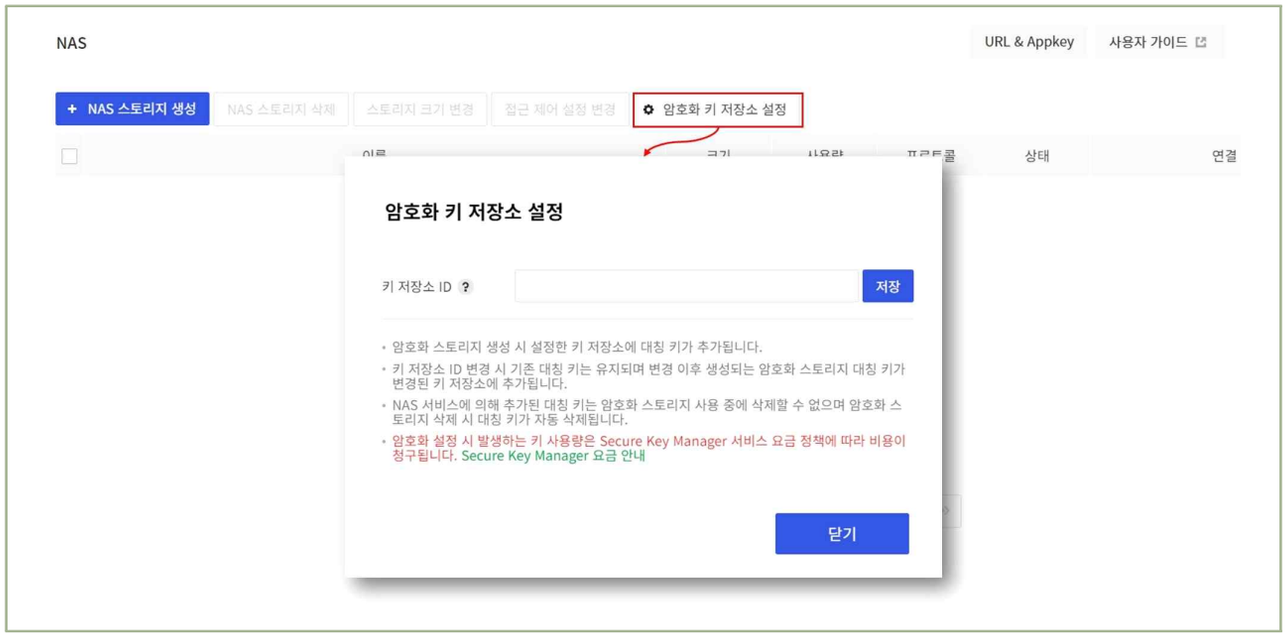


| 그림 4-1-4 | Object storage 암호화 설정

B. 컨테이너 암호화 설정으로 생성한 경우 해당 설정을 중간에 해제할 수 없으며, 암호화 키를 삭제한 경우 더 이상 해당 컨테이너에 객체를 업로드 하거나 다운로드 할 수 없습니다.

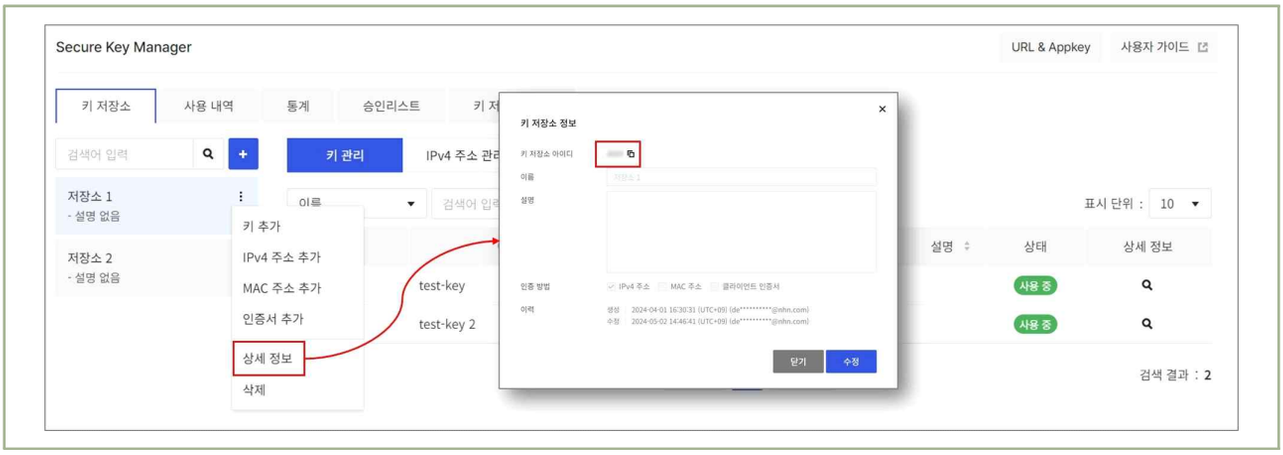
③ NAS 암호화

A. NAS 생성 시 암호화 저장하기 위해서는 '암호화 키 저장소 설정'을 하여야 합니다.



| 그림 4-1-5 | NAS 암호화 키 저장소 설정

B. SKM의 키 저장소 ID는 키 저장소의 '상세 정보'를 클릭하여 확인할 수 있습니다.



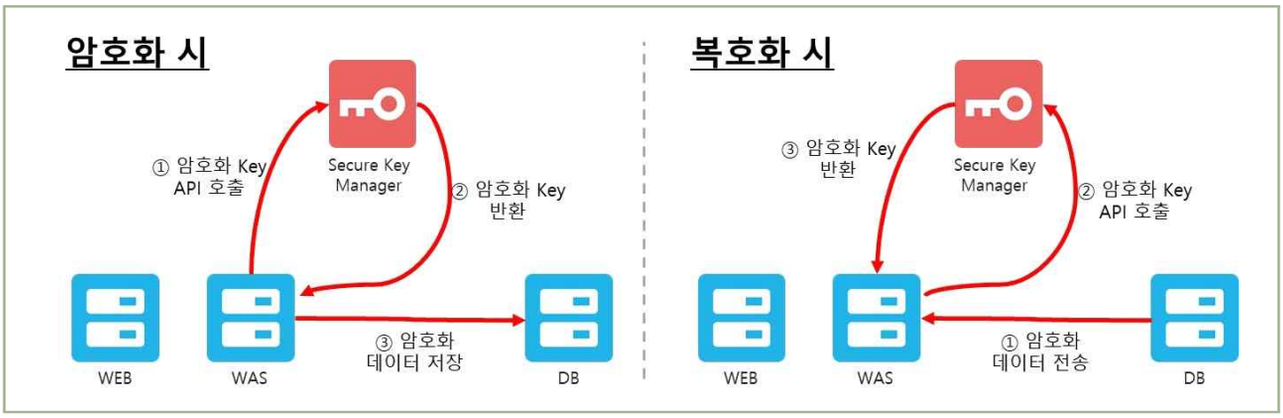
| 그림 4-1-6 | 키 저장소 ID 확인

C. '암호화 키 저장소' 설정을 완료하면 NAS 생성 시 추가 설정을 통해 암호화를 적용할 수 있습니다.

| 그림 4-1-7 | NAS 암호화 설정

④ DB 암호화

A. DB에 저장되는 데이터를 암호화 할 시 SKM 서비스를 이용할 수 있습니다.



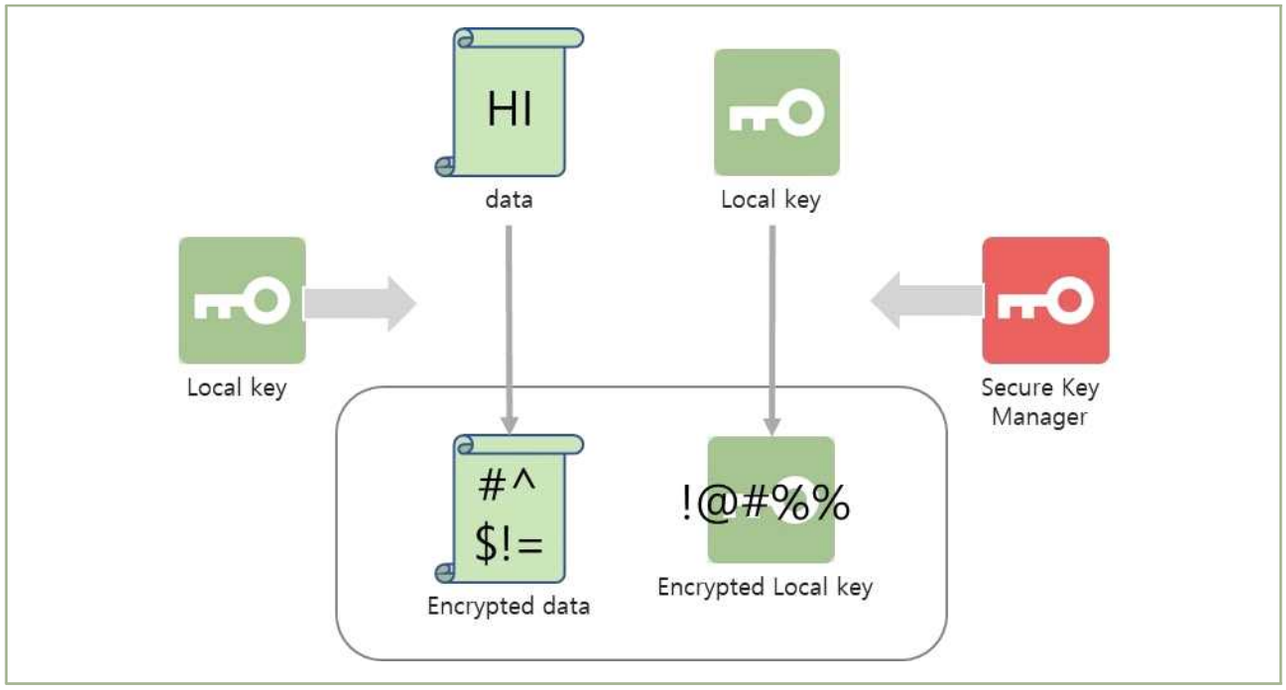
| 그림 4-1-8 | SKM 이용 방식

B. Secure Key Manager에 저장된 암호화 키를 호출하여 WAS에서 암호화 처리 후 DB에 저장되도록 구현하는 것이 가능합니다.

※ API endpoint 및 인증(IPv4, MAC, 인증서)을 이용하여 암호화 키 호출을 제한할 수 있습니다.

| 그림 4-1-9 | SKM IPv4 인증 추가

C. 빈번한 API 암/복호화 시 성능 및 비용 문제가 발생할 수 있으며, 이 경우 봉투 암호화(envelope encryption) 기법을 이용할 수도 있습니다.



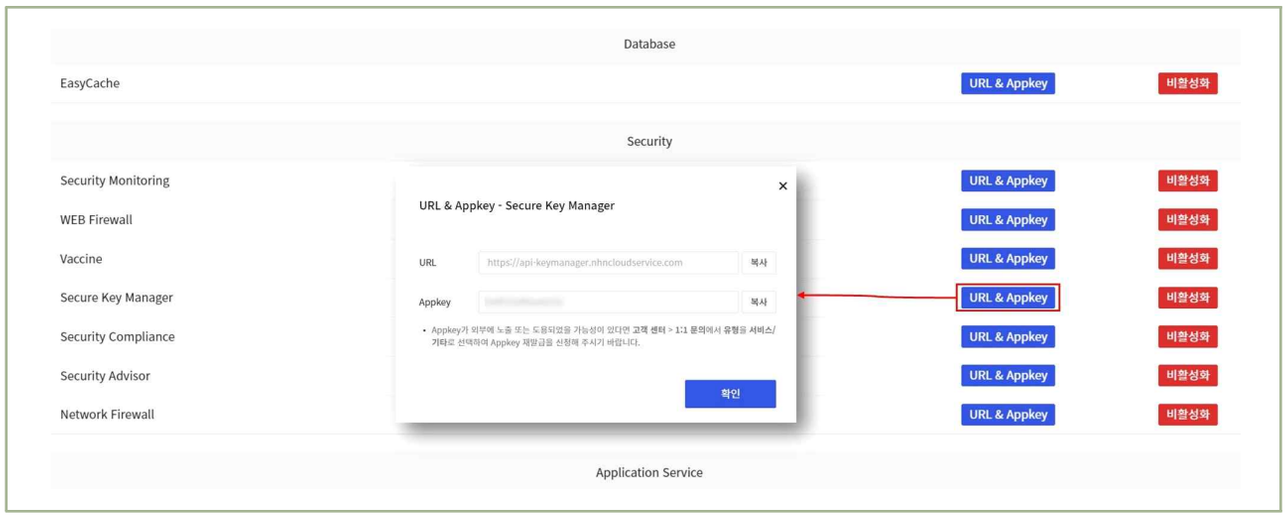
| 그림 4-1-10 | 봉투 암호화(Envelope encryption) 방식

(API)

① 대칭키를 이용하여 데이터 암호화하기

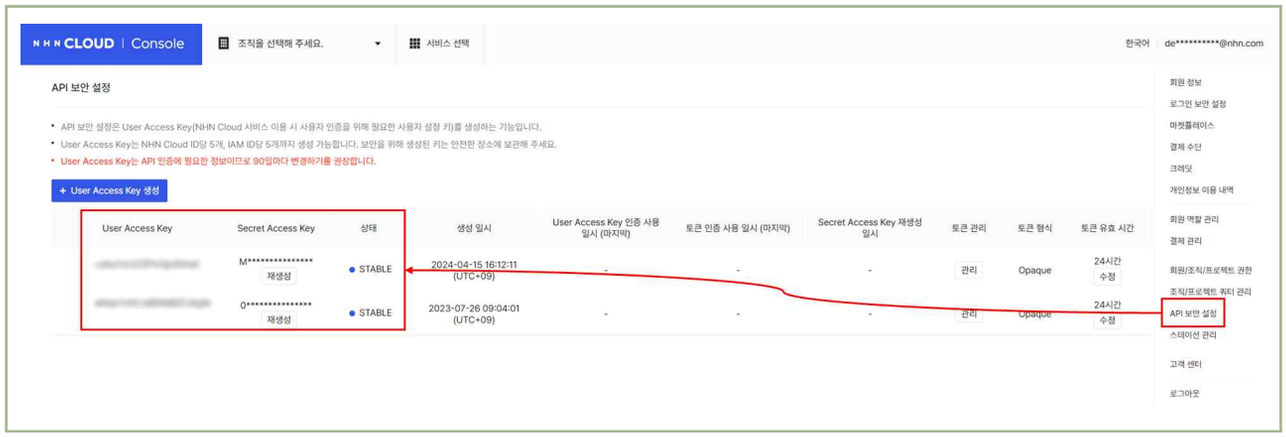
A. SKM의 API를 호출하기 위해서는 appkey와 User Access Key ID, Secret Access Key 정보가 필요합니다.

B. Appkey는 [조직 〉〉 프로젝트 〉〉 프로젝트 관리 〉〉이용중인 서비스]에서 'URL & Appkey'를 클릭하면 확인할 수 있습니다.



| 그림 4-1-11 | SKM Appkey 확인

C. User Access Key ID와 Secret Access Key는 console의 오른쪽 위 계정을 클릭한 후 'API 보안 설정'에서 생성/확인할 수 있습니다.



| 그림 4-1-12 | SKM 사용을 위한 Access Key 확인

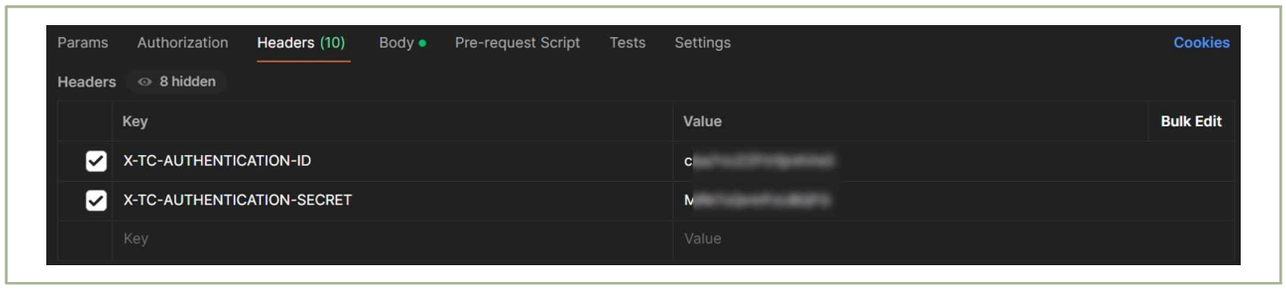
D. 위 정보를 확인했으면 사용자 가이드를 확인하여 HTTP 헤더에 넣어야 할 내용을 확인합니다.

| 그림 4-1-13 | SKM 이용 시 HTTP 헤더에 포함해야 할 인증 값

E. SKM의 API를 이용하려면 필수로 IPv4 또는 MAC, 인증서를 등록하여 인증 값으로 이용해야 합니다.

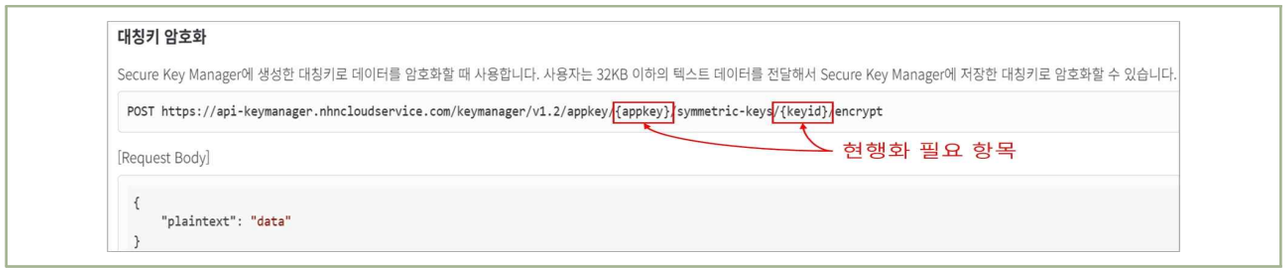
MAC의 경우 위와 같이 HTTP 헤더에 포함하여 API를 호출하면 되고, IPv4의 경우 '클라이언트 정보 조회' API를 통해 조회되는 IP 주소를 넣으면 됩니다.

F. API 호출을 위해 '그림 4-1-13 SKM 이용 시 HTTP 헤더에 포함해야 할 인증 값'을 참고하여 HTTP 헤더에 access key를 추가합니다.



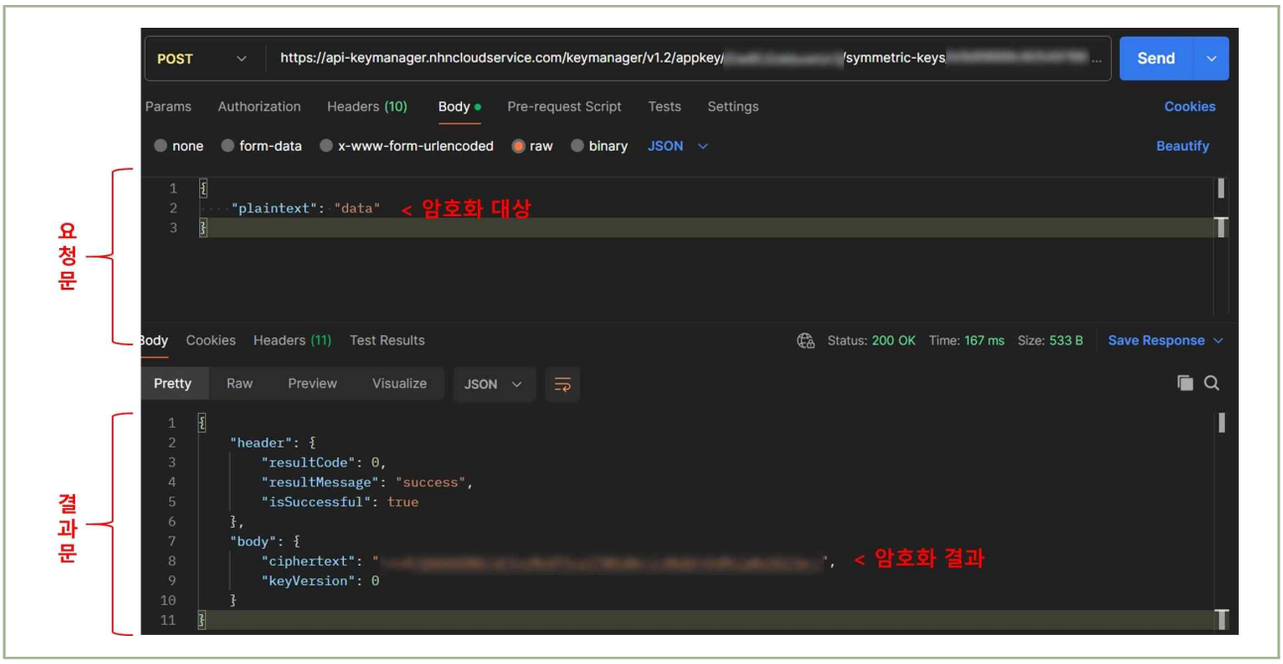
| 그림 4-1-14 | HTTP 헤더에 access key 입력

G. 사용자 가이드에서 API endpoint 및 body 양식 정보를 확인합니다. API endpoint에서 {appkey}와 {keyid} 부분을 현행화 하여야 합니다.



| 그림 4-1-15 | 대칭키 암호화 API 정보 확인

H. ‘그림 4-1-15 대칭키 암호화 API 정보 확인’을 참고하여 API를 작성하고 호출합니다.

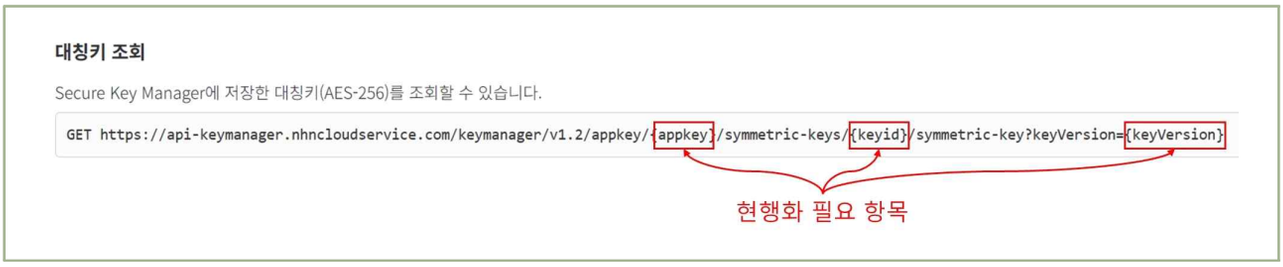


| 그림 4-1-16 | 대칭키를 이용하여 데이터 암호화

② 대칭키 조회하기

A. SKM으로 생성하거나, SKM에 저장한 대칭키를 API로 조회하여 데이터 암호화에 활용할 수 있습니다.

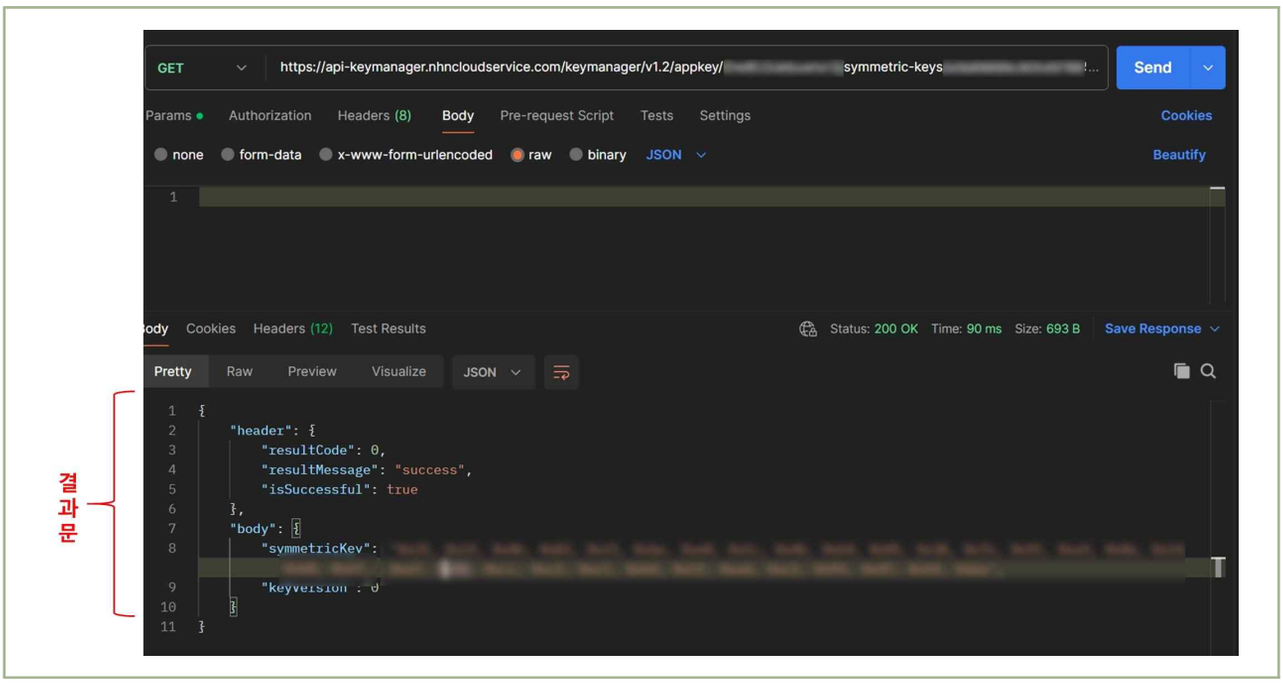
B. 사용자 가이드에서 API endpoint 및 필요한 정보를 확인합니다.



| 그림 4-1-17 | 대칭키 조회 API 정보 확인

C. ‘그림 4-1-17 대칭키 조회 API 정보 확인’을 바탕으로 API를 작성합니다.

D. API 작성 시 HTTP 헤더에 Access key 정보를 반드시 포함하여야 합니다.



| 그림 4-1-18 | 대칭키 조회 결과

4 참고 사항

- 「DB 암호화 솔루션」제품군의 마켓플레이스 제품을 이용하여 DB 암호화를 구현할 수 있으며, HSM (Hardware Security Module)이 필요한 경우에도 마켓플레이스 제품을 이용하여 구성할 수 있습니다.
- NHN Cloud 마켓플레이스

1 기준

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

2 설명

- 암호화 기능 이용 시 암호키 관리 방안을 수립하여야 한다.

  - 예시

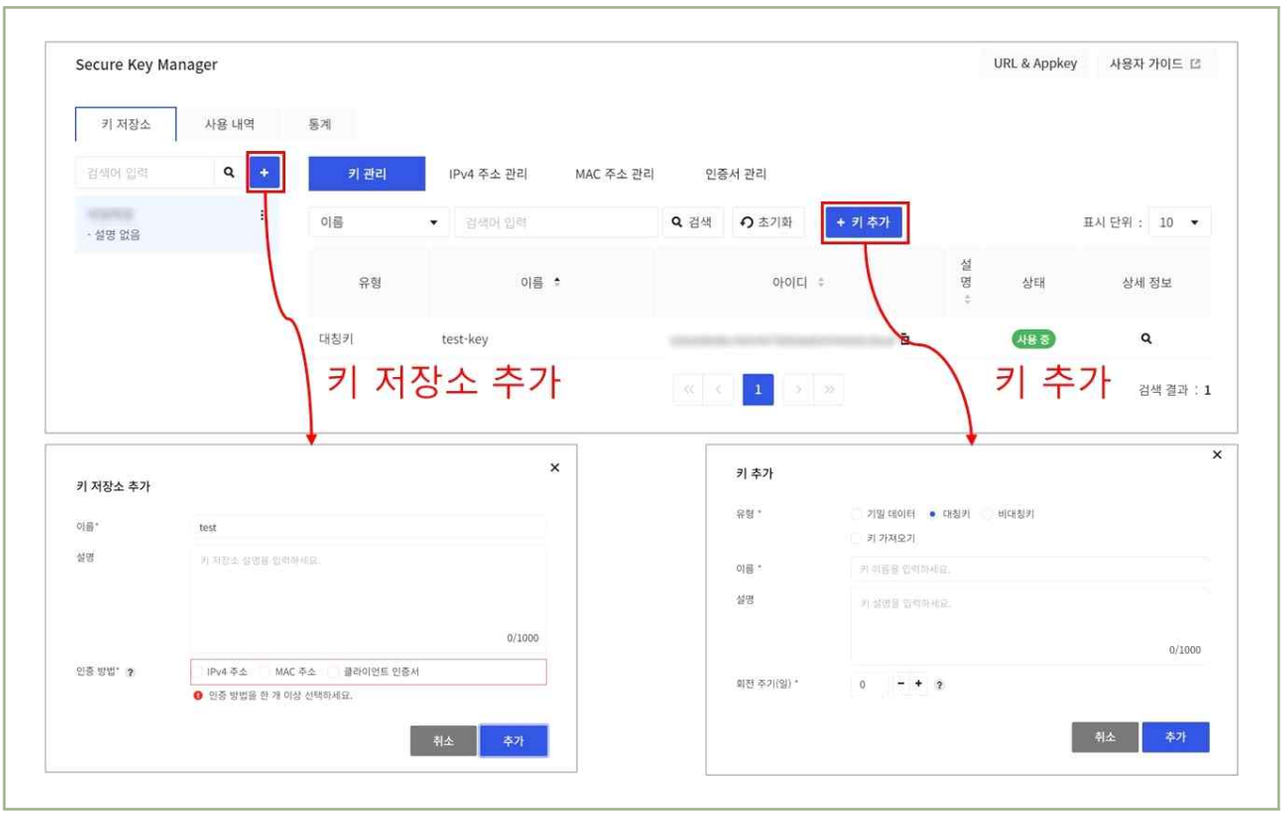
    1) KMS(Key Management Service)를 통한 암호화 키 방안 수립(생성, 변경, 폐기 등)
    2) 클라우드 서비스 제공자가 직접 제공하는 암호화키 이용 시 적절한 관리방안 수립
    3) 키 사용기간 수립 및 암호키 유출 등에 대응할 수 있도록 키 삭제 및 재적용 관련 기능 수립
    4) 생성된 암호화키를 안전하게 보관할 수 있는 방안 수립 등

3 우수 사례

- **(가상자원관리시스템)**

  ① Secure Key Manager 서비스를 이용하여 암호화 키 생성하기

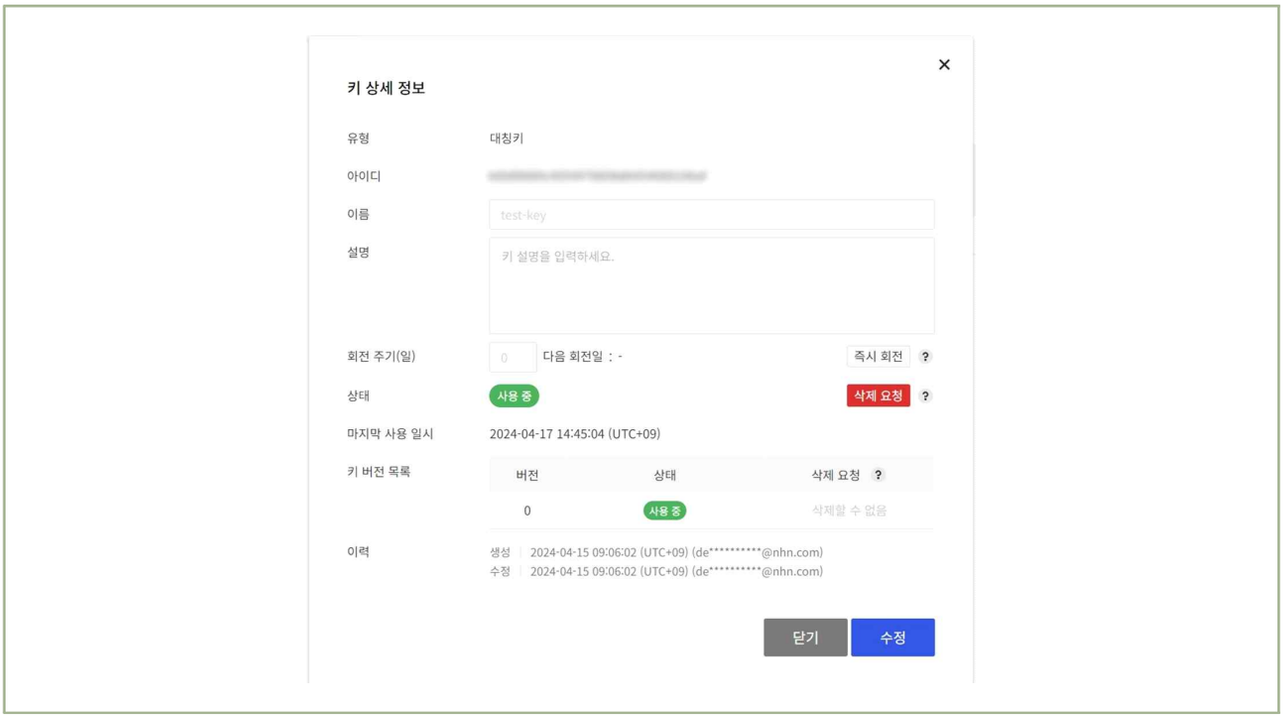
  A. SKM 서비스를 활성화하여 메뉴로 들어가면, 키 저장소 탭에서 키 저장소와 키를 추가할 수 있습니다.



| 그림 4-2-1 | SKM 암호화 키 저장소 및 키 추가

B. 키 저장소 추가 시 IPv4, MAC 주소, 인증서 중 하나의 인증을 반드시 선택하여야 합니다.

C. 상세 정보를 클릭하여 암호화 키에 대한 상세 정보를 확인할 수 있습니다.

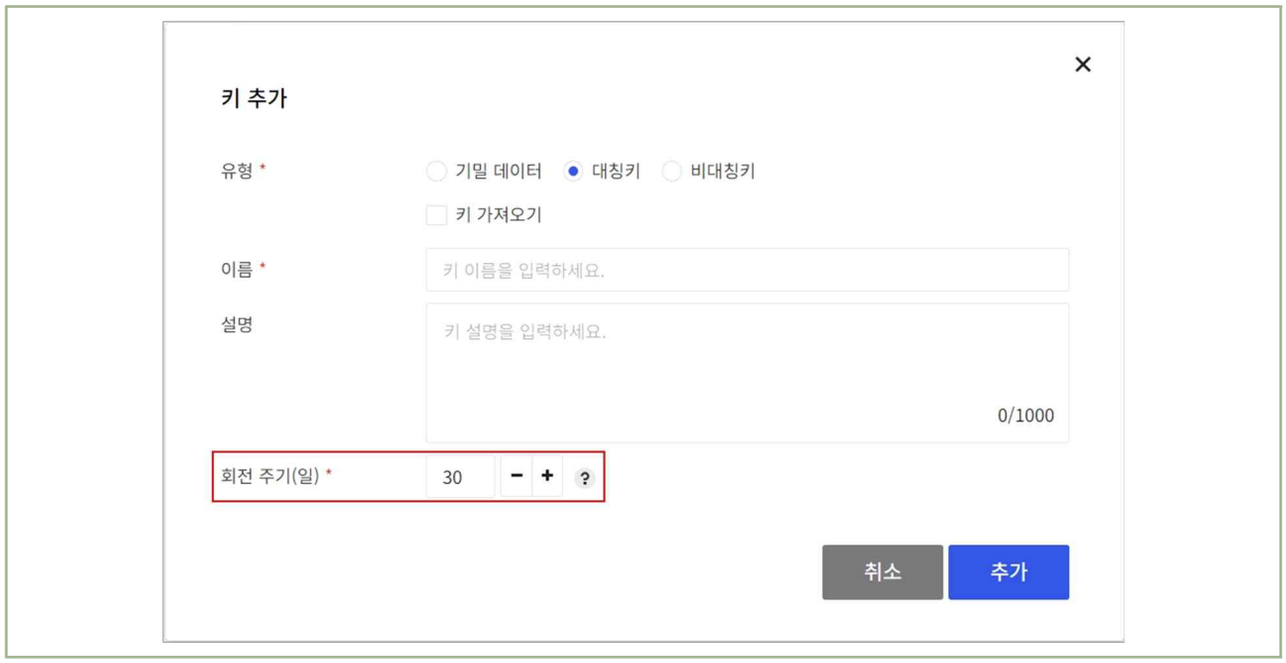


| 그림 4-2-2 | 암호화 키 상세 정보 조회

② Secure Key Manager 서비스를 이용하여 암호화 키 변경하기

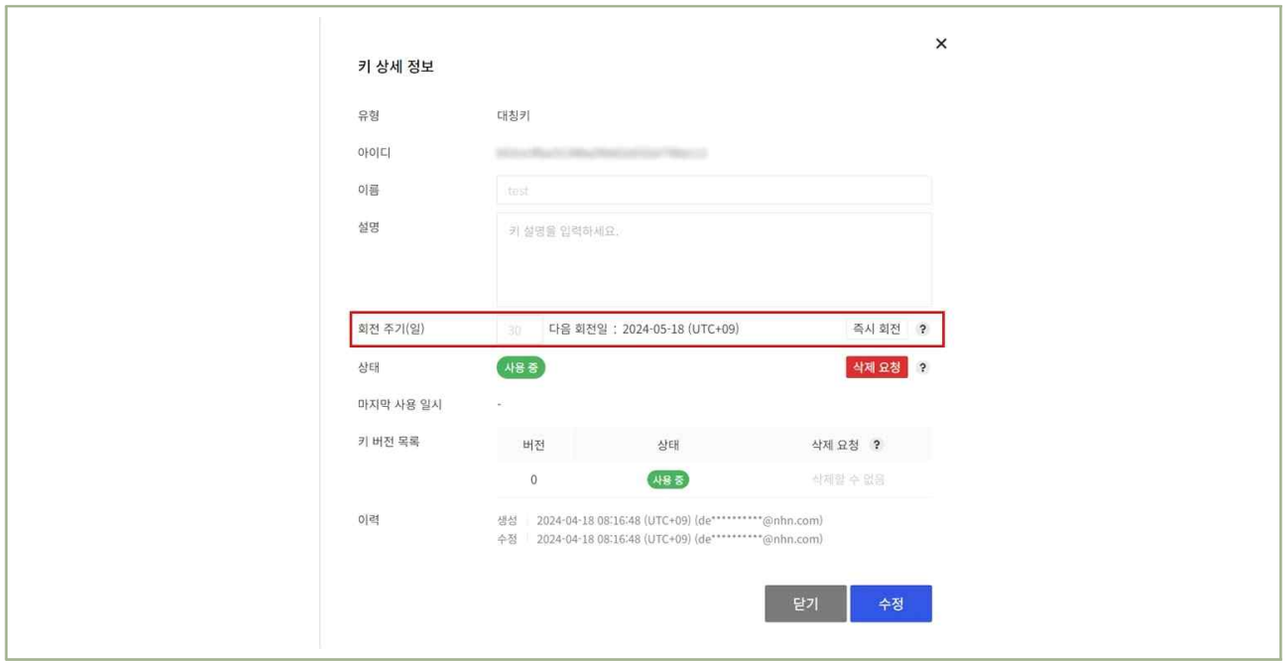
A. SKM 서비스의 경우 암호화 키 회전 기능을 제공하고 있습니다.

B. 키 회전이란 주기적으로 암호화 키를 변경하는 것을 말합니다. 키 추가 시 관련 설정을 할 수 있으며, 정해진 회전 주기일에 따라 자동으로 변경됩니다.



| 그림 4-2-3 | 암호화 키 회전 설정

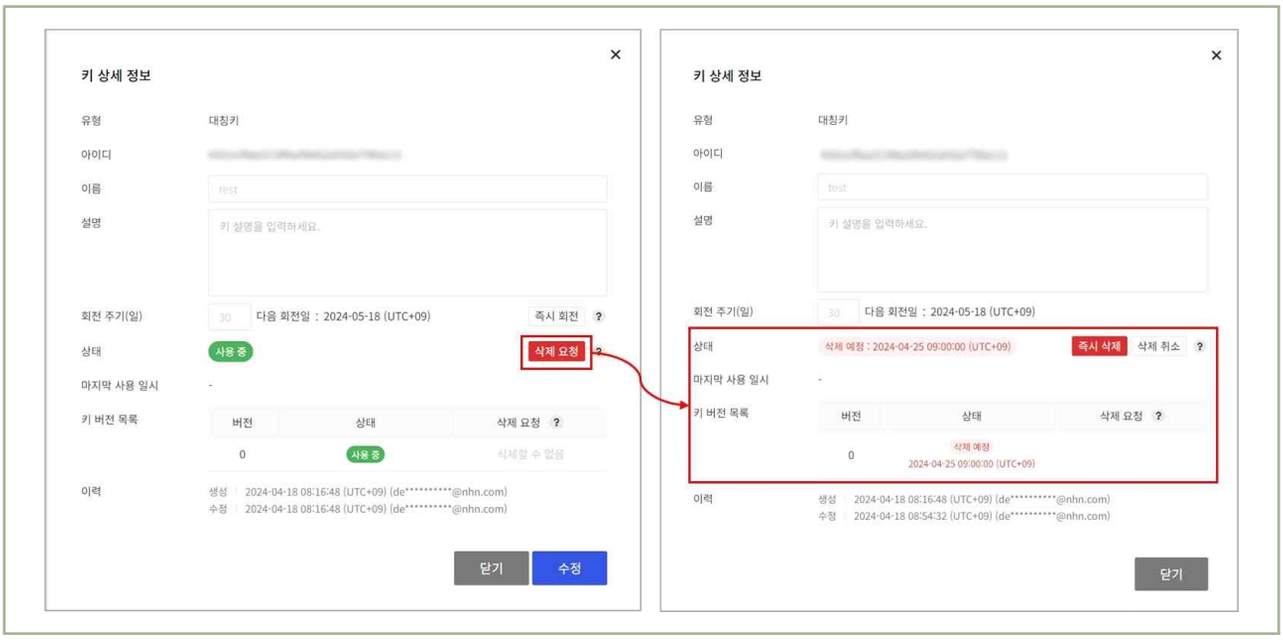
C. 키 상세 정보에서 키 회전 정보를 조회할 수 있으며, 키 버전과 이력 또한 확인할 수 있습니다.



| 그림 4-2-4 | 키 회전 관련 정보 조회

③ Secure Key Manager 서비스를 이용하여 암호화 키 삭제하기

A. 키 상세 정보에서 키 삭제를 요청할 수 있습니다.



| 그림 4-2-5 | 암호화 키 삭제

B. 삭제 요청 시 1주일 뒤 삭제가 진행되며, 즉시 삭제를 클릭하면 바로 삭제가 진행됩니다.

C. 키 삭제 시 해당 키를 사용하는 서비스에 문제가 발생할 수 있으므로 유의하여 키를 삭제합니다.

(API)

① API로 암호화 키 생성하기

A. 사용자 가이드에서 API 호출을 위한 정보를 확인합니다.

대칭키 추가

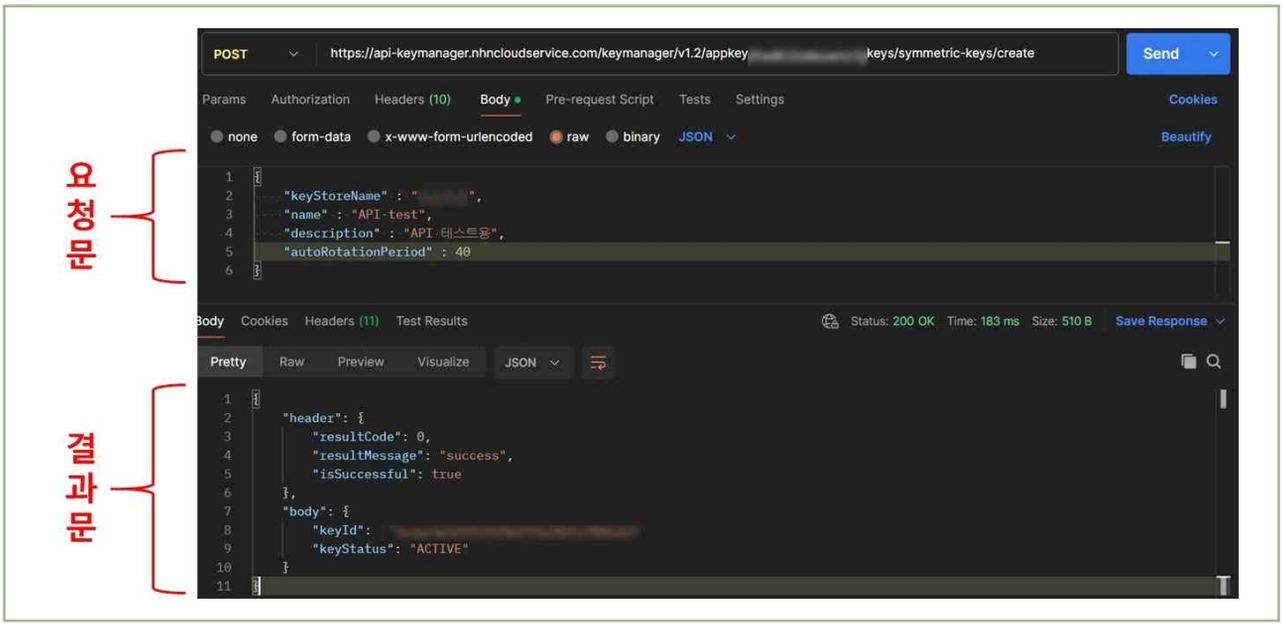
```
POST https://api-keymanager.nhncloudservice.com/keymanager/v1.2/appkey/{appkey}/keys/symmetric-keys/create
```

[Request Body]

```
{
    "keyStoreName" : "Store #1",
    "name" : "Key Sample #2",
    "description" : "Description #2",
    "autoRotationPeriod" : 0
}
```

| 그림 4-2-6 | 대칭키 생성 API 가이드

B. ‘그림 4-2-6 대칭키 생성 API 가이드’를 참조하여 API를 작성합니다.



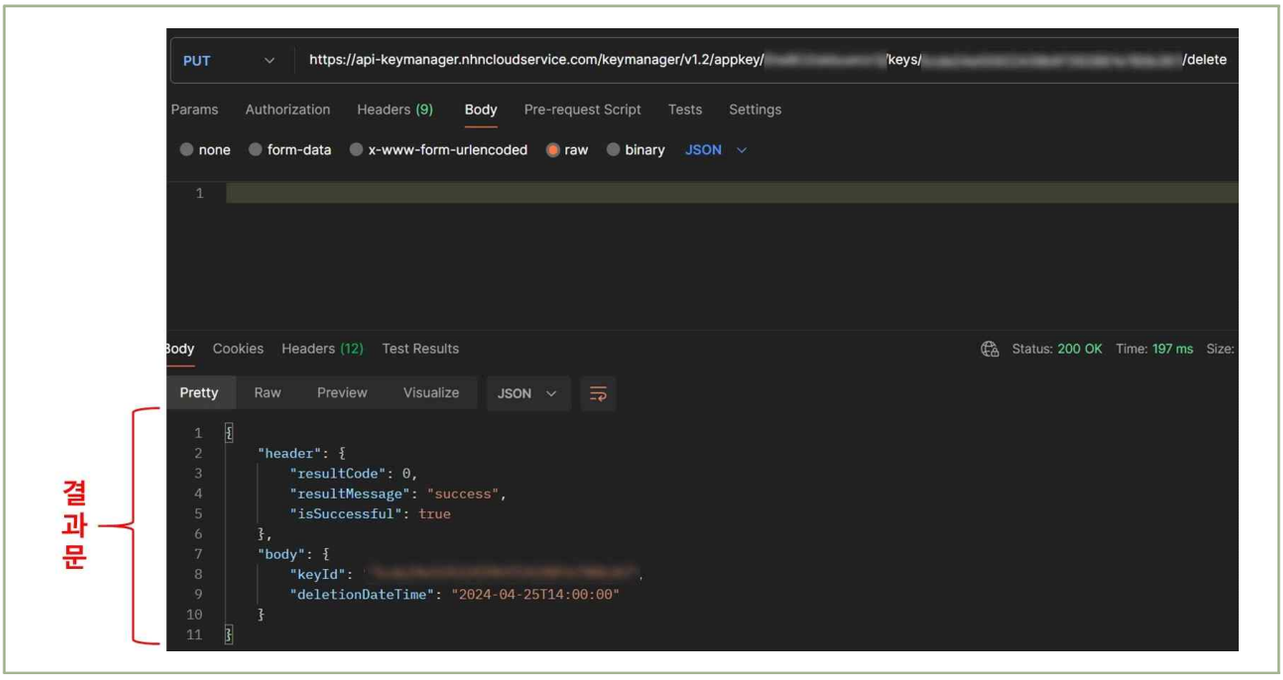
| 그림 4-2-7 | API를 이용하여 대칭키 생성

② API로 암호화 키 삭제하기

A. 사용자 가이드에서 API 호출을 위한 정보를 확인합니다.

| 그림 4-2-8 | 키 삭제 API 가이드

B. ‘그림 4-2-8 키 삭제 API 가이드’를 참조하여 API를 작성합니다.



| 그림 4-2-9 | API를 이용하여 키 삭제

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 부여 현황에 대해 상시모니터링 수행

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

3 우수 사례

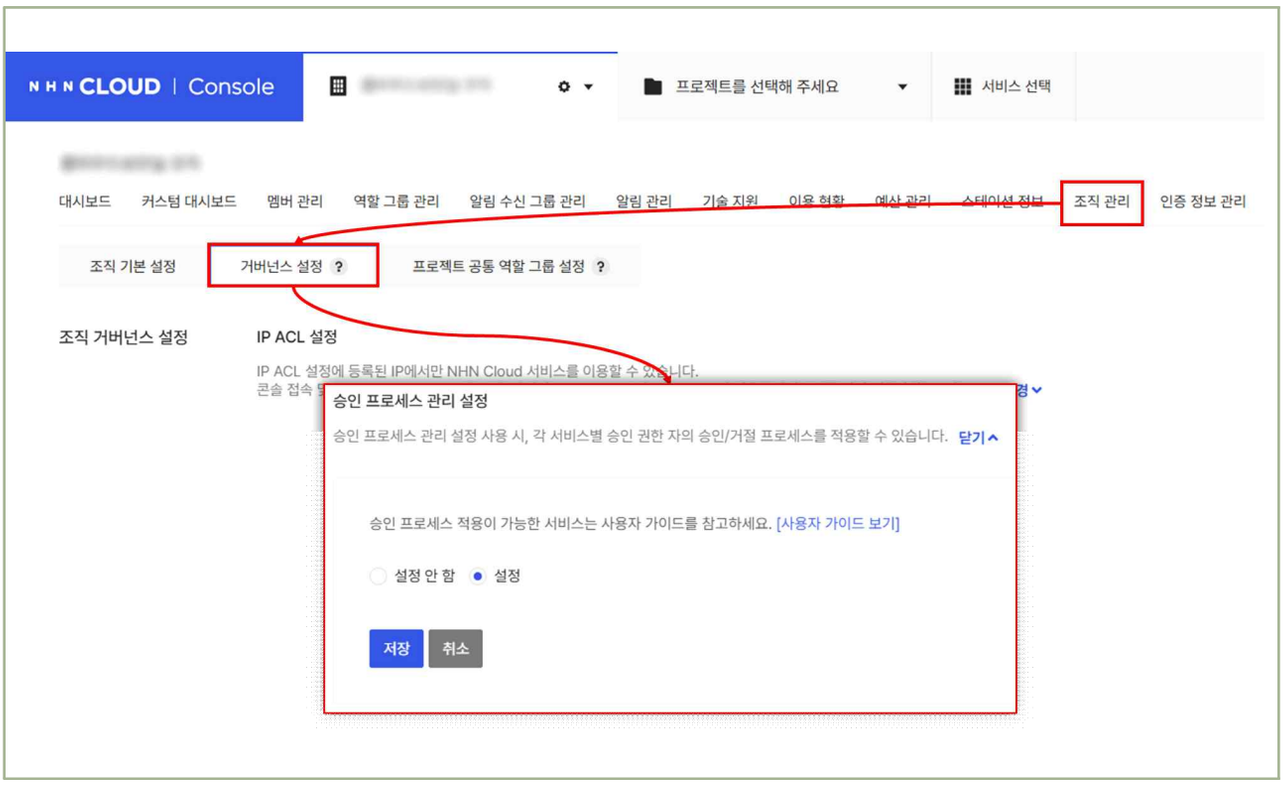
- **(가상자원관리시스템)**

  ① Secure Key Manager 승인 기능 활성화하기

  A. NHN Cloud의 SKM 서비스는 승인 기능을 추가하여 키 생성/변경 시 승인을 받도록 구성할 수 있습니다. 키 생성, 변경에 대한 승인 기능을 활성화하면 모든 변경 행위에 대해 담당자가 모니터링하며, 불필요한 변경행위를 사전에 통제할 수 있습니다.

  B. 승인 기능은 키 저장소 추가, 키 추가, 인증 추가(IPv4 주소, MAC 주소, 인증서), 키 삭제 등 SKM의 다양한 활동을 승인을 통해서만 동작하도록 구현합니다.

  C. [조직 〉 조직 관리 〉 거버넌스 설정]에서 '승인 프로세스 관리 설정' 기능을 확인할 수 있으며, 해당 기능을 '설정'으로 변경하는 경우 승인 프로세스를 진행할 수 있습니다.



| 그림 4-3-1 | Secure Key Manager 승인 기능 활성화

② Secure Key Manager 권한 분리하기

A. SKM의 경우 Console에서 접근 권한을 차등 부여할 수 있습니다.

B. Console에서 SKM의 권한은 4가지로 구분되는데, 그 구분은 다음 그림과 같습니다.

권한	키 생성	키 사용	키 요청	키 승인
SKM Admin	●	●	●	X
SKM Approval Admin	●	●	●	●
SKM Viewer	X	●	X	X
SKM Permission	X	X	X	X

| 그림 4-3-2 | Secure Key Manager console 권한

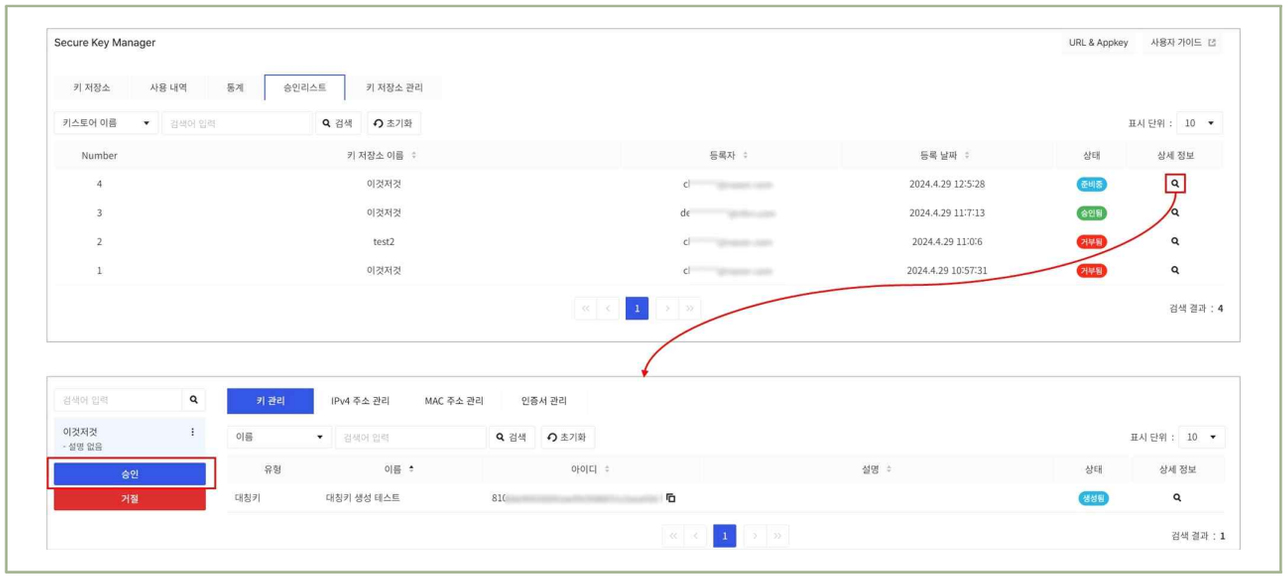
C. Console 권한 중 Approval Admin 권한은 '승인 기능'을 활성화해야만 적용이 가능합니다.

D. SKM Key에 대한 생성 및 승인이 필요한 직무 담당자는 SKM Approval Admin 권한을 부여하고, 단순히 암호화 키를 사용만 하는 직무는 Viewer 권한으로 부여하여 역할 분리가 가능합니다.

③ Secure Key Manager 키 요청/승인 절차

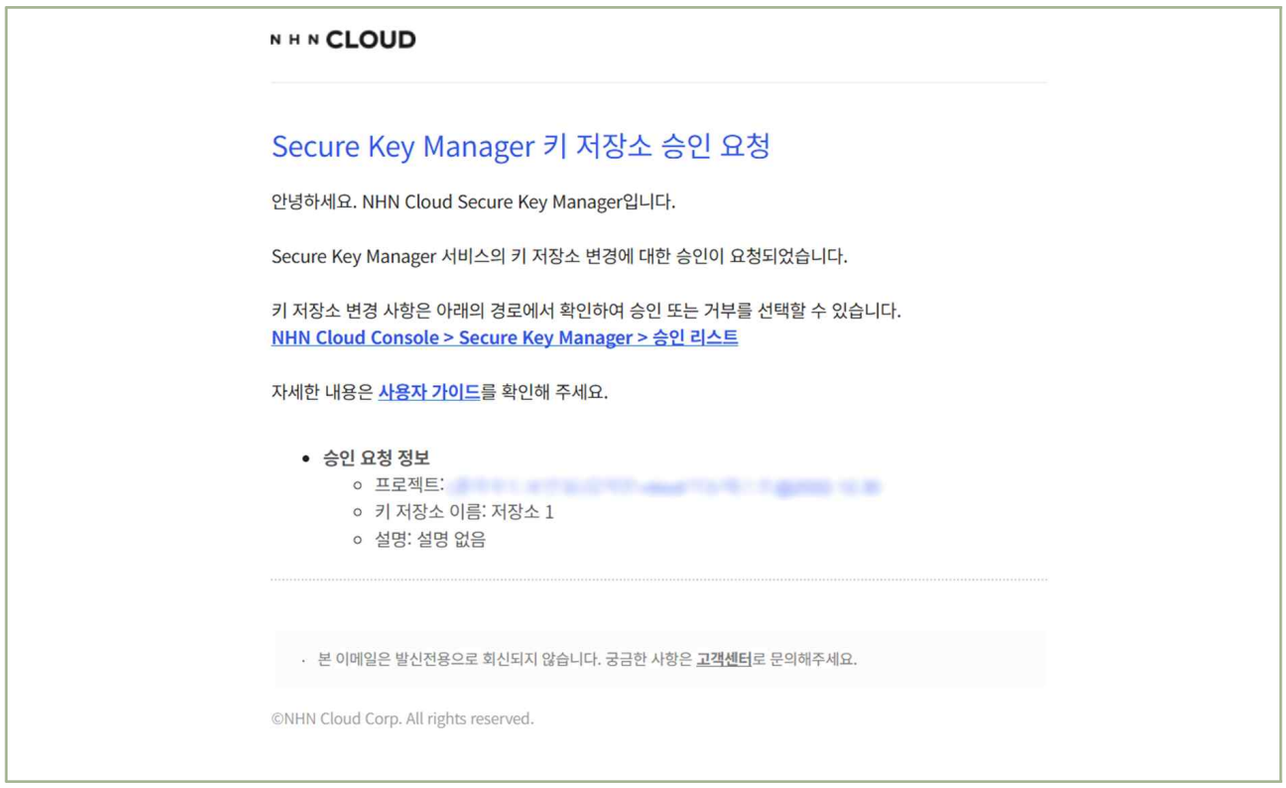
A. SKM Admin 권한의 사용자가 '키 추가'를 하게 되면 대칭키가 추가되고 왼쪽에 '승인 요청' 버튼이 생성되는 것을 확인할 수 있으며, '승인 요청' 클릭 시 승인 요청이 상신됩니다. 그리고 승인자는 승인리스트 탭에서 승인 요청 내역을 확인할 수 있습니다.

| 그림 4-3-3 | SKM Admin 권한에서 키 추가 승인 요청



| 그림 4-3-4 | Approval Admin 권한에서 키 추가 요청 내역 확인 및 승인

B. 승인 요청을 하게 되면 그 요청 내역이 Approval Admin 계정 전체에 메일로 전달되어 승인자가 승인 요청 사실을 인지할 수 있습니다.



NHN CLOUD

Secure Key Manager 키 저장소 승인 요청

안녕하세요. NHN Cloud Secure Key Manager입니다.

Secure Key Manager 서비스의 키 저장소 변경에 대한 승인이 요청되었습니다.

키 저장소 변경 사항은 아래의 경로에서 확인하여 승인 또는 거부를 선택할 수 있습니다.
NHN Cloud Console > Secure Key Manager > 승인 리스트

자세한 내용은 사용자 가이드를 확인해 주세요.

- 승인 요청 정보
  - 프로젝트: [redacted]
  - 키 저장소 이름: 저장소 1
  - 설명: 설명 없음

· 본 이메일은 발신전용으로 회신되지 않습니다. 궁금한 사항은 고객센터로 문의해주세요.

©NHN Cloud Corp. All rights reserved.

| 그림 4-3-5 | 메일로 전달된 SKM 승인 요청 내역

④ Secure Key Manager의 Key 사용 내역 확인하기

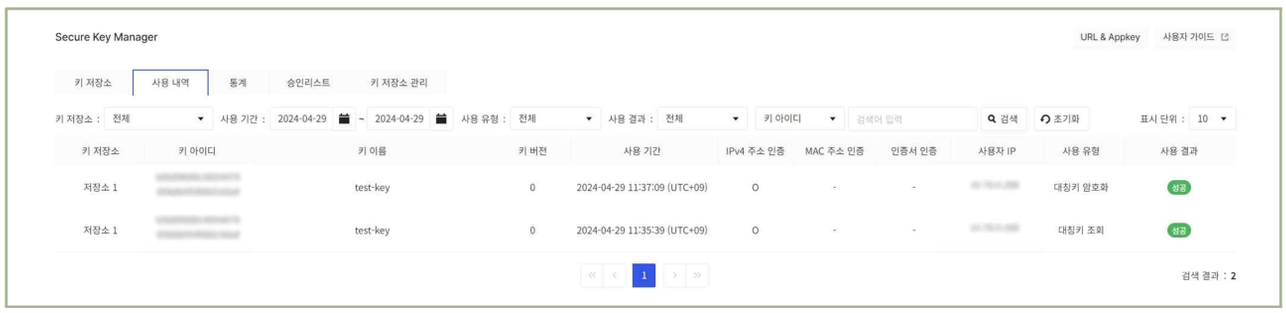
A. Console의 SKM 메뉴에서 암호화 키의 사용 내역을 확인할 수 있습니다.

B. '사용 내역'은 대칭키 조회, 암/복호화 등 암호화 키를 이용한 내역을 확인하는 기능으로 해당 메뉴를 통해 키 사용 내역을 모니터링 할 수 있습니다.

단, 단말에서 API 호출을 직접 하는 경우에만 '사용 내역' 메뉴에서 조회되고, 콘솔을 통해 요청한 내역은 CloudTrail 서비스에서 조회됩니다.

C. '사용 내역' 메뉴에서는 키 저장소별, 사용 유형별, 키 아이디, 사용자 IP 등을 지정하여 조회할 수 있으며, 해당 내역은 1년동안 저장되어 조회할 수 있습니다.

※ 저장 기간은 회사 사정에 따라 변경될 수 있습니다.



Secure Key Manager

URL & Appkey | 사용자 가이드

키 저장소 | 사용 내역 | 통계 | 승인리스트 | 키 저장소 관리

키 저장소 : 전체 | 사용 기간 : 2024-04-29 ~ 2024-04-29 | 사용 유형 : 전체 | 사용 결과 : 전체 | 키 아이디 | 검색어 입력 | 검색 | 초기화 | 표시 단위 : 10

키 저장소	키 아이디	키 이름	키 버전	사용 기간	IPv4 주소 인증	MAC 주소 인증	인증서 인증	사용자 IP	사용 유형	사용 결과
저장소 1	[redacted]	test-key	0	2024-04-29 11:37:09 (UTC+09)	O	-	-	[redacted]	대칭키 암호화	성공
저장소 1	[redacted]	test-key	0	2024-04-29 11:35:39 (UTC+09)	O	-	-	[redacted]	대칭키 조회	성공

« ‹ 1 › »

검색 결과 : 2

| 그림 4-3-6 | 암호화 키 사용 내역 조회

1 기준

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

2 설명

- 클라우드 암호키 호출에 관한 사항(암호화, 복호화, 암호키 변경, 삭제 등)은 이용자의 권한 및 업무에 따라 적절하게 부여하고 관리하여야 한다.

  - 예시

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

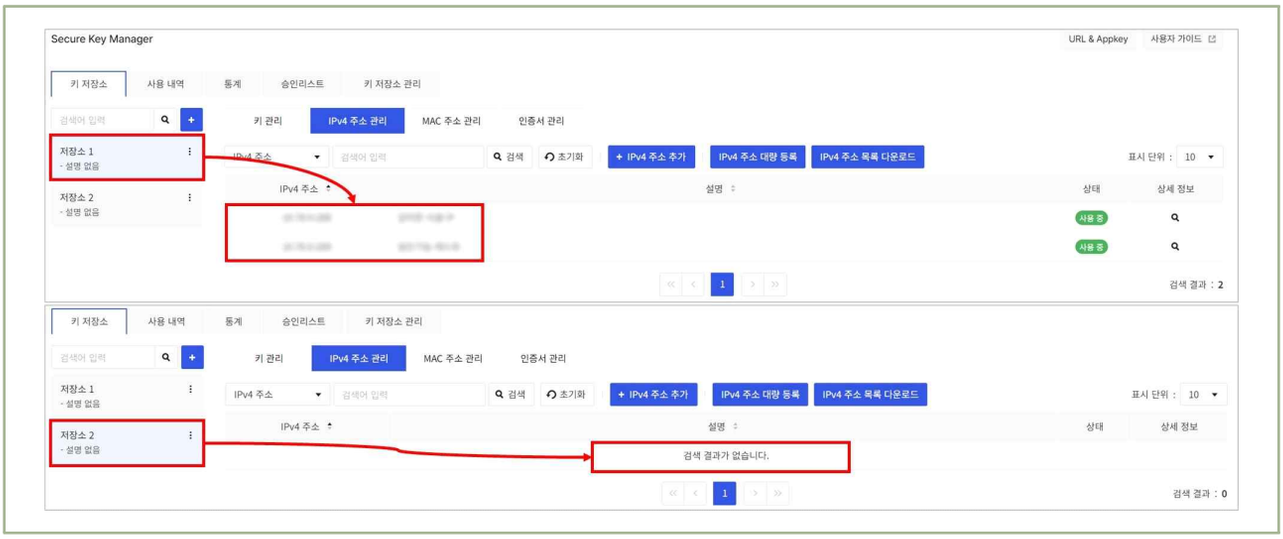
    2) 암호키 호출 권한 현황에 대한 모니터링 및 주기적 검토 수행

3 우수 사례

- **(가상자원관리시스템)**

  ① Secure Key Manager의 키 저장소별 접근제한

  A. SKM의 접근제한 기능인 IPv4 주소, MAC 주소, 인증서는 키 저장소 별로 설정할 수 있습니다.



| 그림 4-4-1 | 키 저장소 별 IPv4 주소 지정

B. ‘그림 4-4-1 키 저장소 별 IPv4 주소 지정’을 보면 저장소 1의 IPv4 주소 내역과 저장소 2의 IPv4 주소 내역이 상이한 것을 볼 수 있습니다.

위 그림과 같이 키 저장소 별로 접근 IP를 다르게 지정하면, 암호화 키 별로 사용자 접근을 분리 지정할 수 있습니다.

C. 그리고 암호화 키 저장소를 키 사용 목적별로 추가한다면, 호출 목적에 따라 권한을 부여할 수 있습니다.

부 서	키 구분	용 도	IP 허용 목록	SKM 권한
시스템운영팀	키 저장소 1	Blockstorage 암호화	10.50.200.1, 10.50.200.2,...	Admin-1,2명 Viewer-나머지
DB운영팀	키 저장소 2	고객정보 암호화 키 관리&이용	10.50.210.1, 10.50.210.2,...	Admin-1,2명 Viewer-나머지
웹서비스개발팀		고객정보 암호화 키 이용	10.50.250.1, 10.50.250.2,...	Viewer-전체
정보보호팀	-	암호화 키 승인 및 목록 관리	-	Approval Admin-전체

| 그림 4-4-2 | 암호화 키 권한 분류 예시

D. ‘그림 4-4-2 암호화 키 권한 분류 예시’는 용도에 따라 키 저장소를 분리하고 SKM 권한을 차등으로 분리한 예시입니다.

키 저장소에 따라 IP 주소를 분리하였으므로 시스템운영팀은 ‘키 저장소 2’에 저장된 암호화 키를 호출할 수 없습니다.

그리고 시스템운영팀 및 DB운영팀, 웹서비스개발팀은 Approval Admin 권한이 없으므로 암호화 키에 대한 변경을 승인할 수 없습니다.

② 키 사용 내역 모니터링 하기

A. ‘사용 내역’ 메뉴에서 암호화 키 사용 로그(단말에서 API로 호출한 내역)가 조회되는 것은 위에서 확인하였습니다.

여기서는 실제 모니터링 할 수 있는 몇 가지 예시를 들어서 살펴보겠습니다.

B. 모니터링 할 수 있는 조건 값은, ‘키 저장소’. ‘사용 유형’, ‘사용 결과’, ‘키 아이디/사용자IP’ 입니다.

| 그림 4-4-3 | SKM 사용 내역 조회 조건

C. '그림 4-4-3 SKM 사용 내역 조회 조건'의 값들을 조합하여 정기적으로 검토를 수행할 수 있습니다.

| 그림 4-4-4 | SKM 사용 내역 검토 조건 예시

D. '그림 4-4-4 SKM 사용 내역 검토 조건 예시'에서 암호키 정보(키 ID 등)가 유출됐다고 가정하면 비인가 IP에서 키를 조회하는 API 호출 내역을 검사하여 확인할 수 있습니다.

또한 키 사용자의 빈번한 데이터 복호화 여부를 검색 조건으로 지정하여 확인할 수도 있습니다.

1 기준

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

2 설명

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

  - 예시

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

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

3 우수 사례

- Secure Key Manager 서비스의 대칭키는 AES 알고리즘을 이용하고 있으며, 키 길이는 256비트입니다. 상세 내용은 Secure Key Manager의 대칭 키 사용에 대한 사용자 가이드에서 확인할 수 있습니다.

5. 로깅 및 모니터링 관리

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

5 로깅 및 모니터링 관리

1 기준

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

2 설명

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

  – 예시

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

3 우수 사례

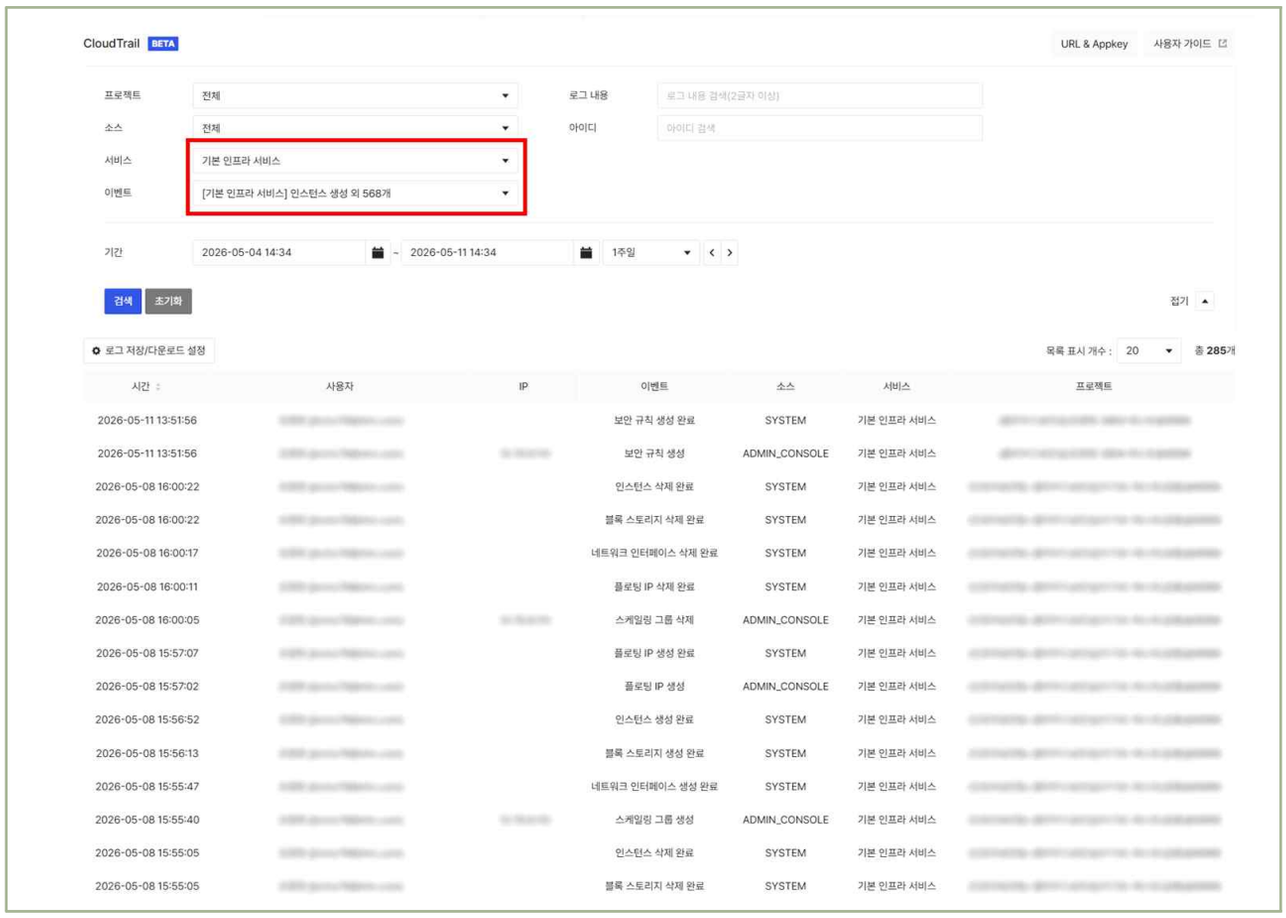
- **(가상자원관리시스템)**

  ① CloudTrail 로그로 가상자원 변경 로그 확인하기

  A. Console을 이용한 가상자원의 생성/변경/삭제 행위는 CloudTrail 서비스에 기록/저장됩니다.

  B. ‘1.4 가상자원 생성 시 네트워크 설정 적용’에서 CloudTrail 관련하여 간단하게 설명했습니다.

  C. CloudTrail에서는 NHN Cloud에서 제공하는 서비스의 가상자원 생성/변경/삭제 로그를 조회할 수 있습니다.



| 그림 5-1-1 | CloudTrail log 조회

D. '그림 5-1-1 CloudTrail log 조회' 에서와 같이 서비스를 '기본 인프라 서비스'로 제한한 경우 '기본 인프라 서비스'에 포함된 Compute, Network 등의 서비스 변경 로그를 확인할 수 있습니다.

E. 또한 "로그 저장/다운로드 설정"을 이용하여 Object Storage로 내려 받는 경우 상세로그를 확인할 수 있습니다.

※ 90일 이상 저장이 필요한 경우 반드시 "로그 저장/다운로드 설정"기능을 통해 별도 저장소에 보관/저장하여야 합니다.

② SIEM 서비스를 이용하여 가상자원 로그 저장하기

A. 클라우드 상에서 발생하는 다양한 로그를 통합 저장하고, 실시간 조회, 조건부 검색 등의 대응을 위해 SIEM(Security Information and Event Management, 보안 정보 및 이벤트 관리)을 구성할 수 있습니다.

B. NHN Cloud에서 제공하는 SIEM 서비스는 고객의 가상화 영역 내 SIEM을 구성하여 이용하게 됩니다.

C. SIEM은 이기종 간의 다양한 로그를 통합 저장할 수 있으며, 상관 분석을 통해 실시간으로 위협을 탐지하거나 검색할 수 있습니다.

D. SIEM에 CloudTrail 로그를 연동하여 저장하고, 시스템 로그(event log, audit log 등), Application 로그, 보안 장비 로그 등을 연동하여 이용할 수 있습니다.

E. Cloud에서의 설치 및 이용과 관련해서는 고객센터 또는 1:1문의 채널을 이용하시기 부탁드립니다.

4 참고 사항

- 가상자원에 원격접속(SSH, RDP 등)하여 이용하는 접근로그의 경우 마켓플레이스의 「서버/데이터베이스 접근제어」 제품군을 구성하여 로그를 남길 수 있습니다.
- NHN Cloud 마켓플레이스

1 기준

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

2 설명

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

  - 예시

    1) 클라우드 가상자원 이용에 관한 행위추적성 증적(ex. 감사로그 등)에 대한 상시 모니터링 수행
    2) 금융회사 내부규정등 관련 규정을 통해 수립된 검토 기간에 맞추어 클라우드 가상자원 이용에 관한 행위추적성 증적에 대한 주기적 검토 수행

3 우수 사례

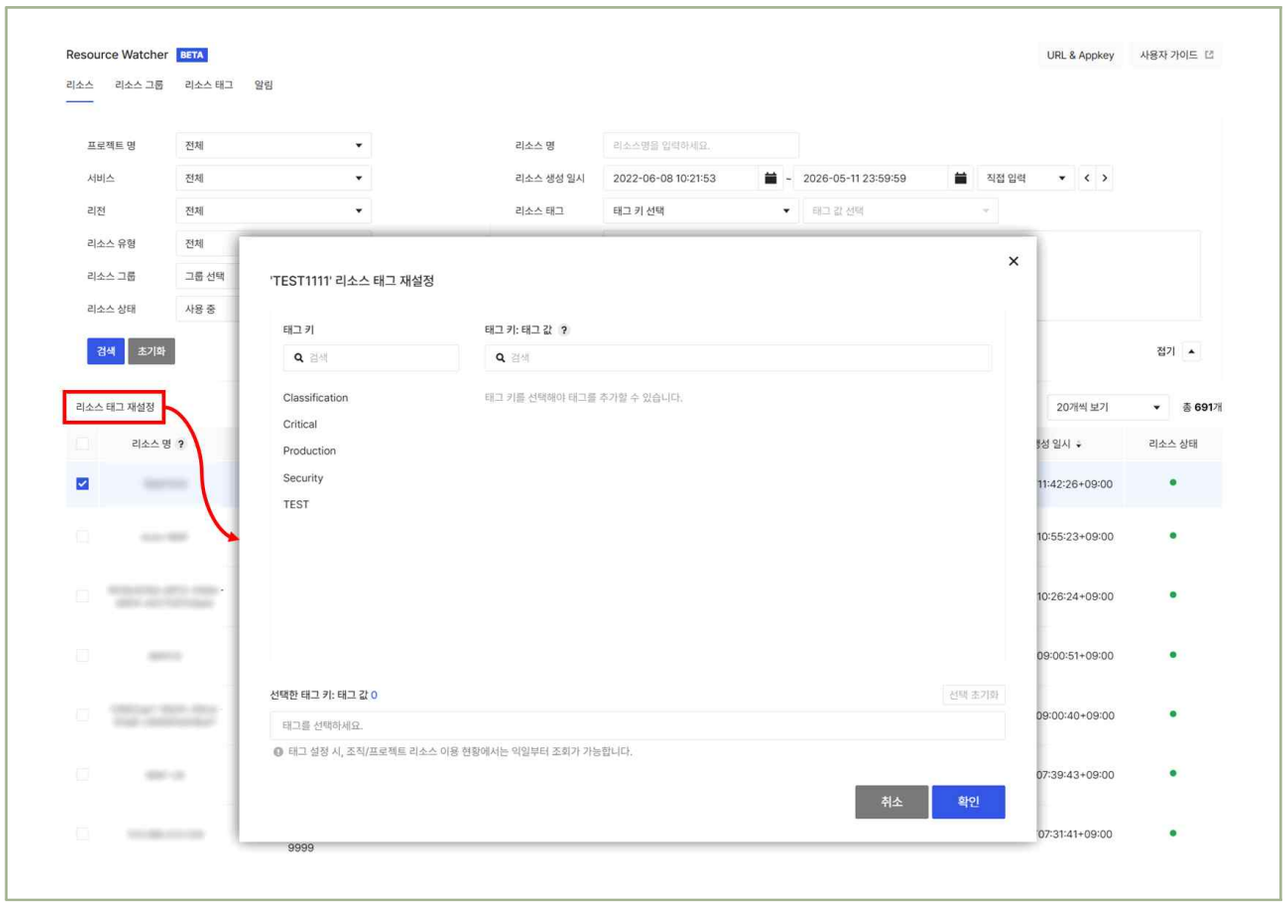
- **(가상자원관리시스템)**

  ① Resource Watcher 서비스로 가상자원 변경 모니터링 알림 받기

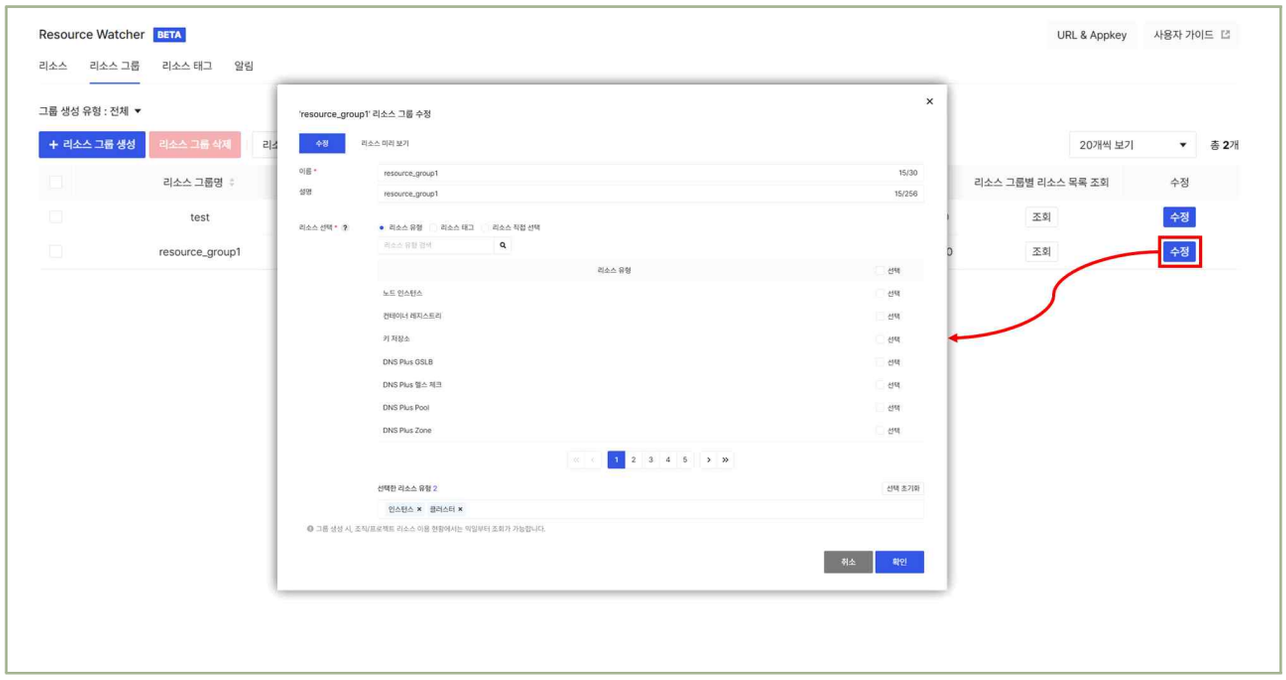
  A. NHN Cloud의 다양한 서비스 리소스에서 변경 사항이 발생하는 경우 알림을 받도록 설정할 수 있습니다.

  B. 자원별로 리소스 태그를 설정하거나, 리소스 그룹을 지정하여 알람 대상을 지정할 수 있습니다.

  ※ 리소스 유형은 노드 인스턴스, 키 저장소, NAS 스토리지, 클러스터 등 다양한 가상자원을 선택할 수 있습니다.

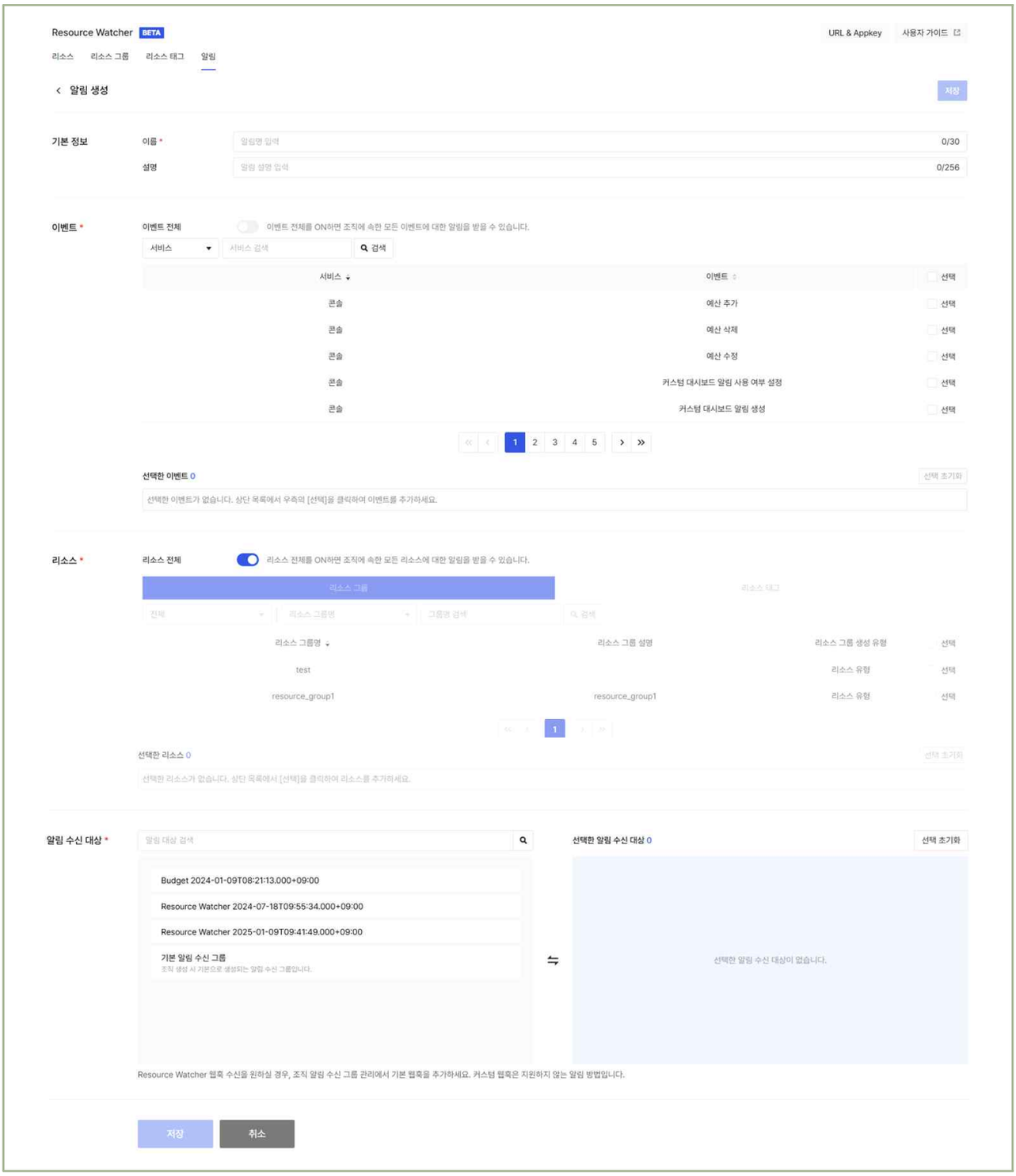


| 그림 5-2-1 | 리소스별 태그 설정



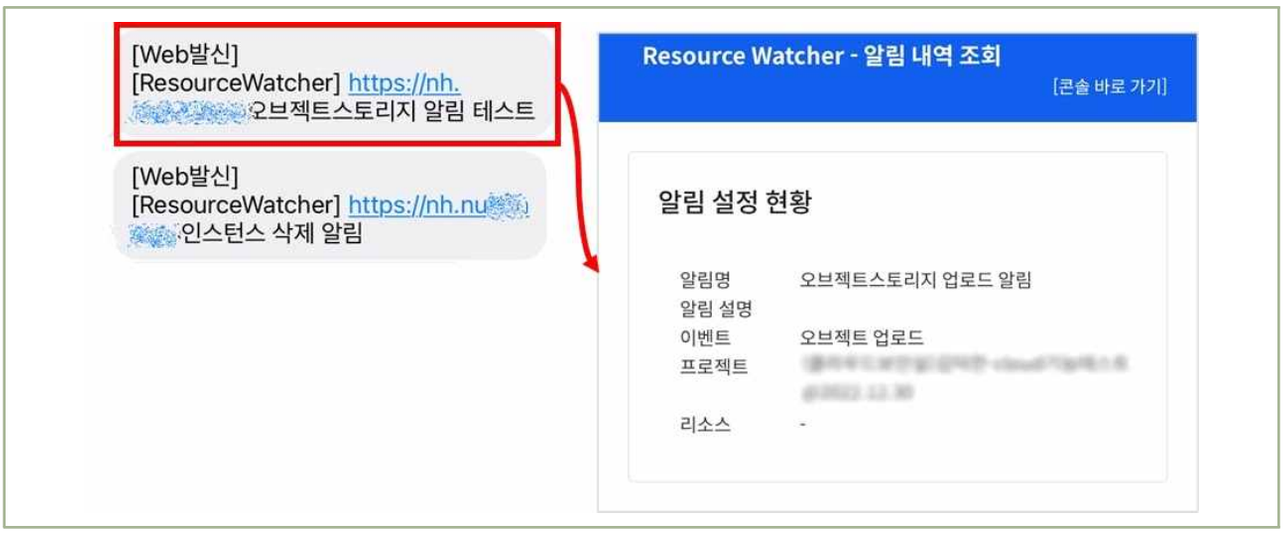
| 그림 5-2-2 | 리소스 그룹 지정

C. 알림 메뉴에서는 리소스의 특정 이벤트 발생 시 알림을 받도록 설정할 수 있습니다.



| 그림 5-2-3 | Resource Watcher의 알림 설정 화면

D. 알림을 받을 이벤트를 정의하고 리소스를 지정, 알림을 받을 사람 및 수단을 확정하면 해당 이벤트 발생 시 알림을 수신하게 됩니다.



| 그림 5-2-4 | 실제 문자 알림 내역

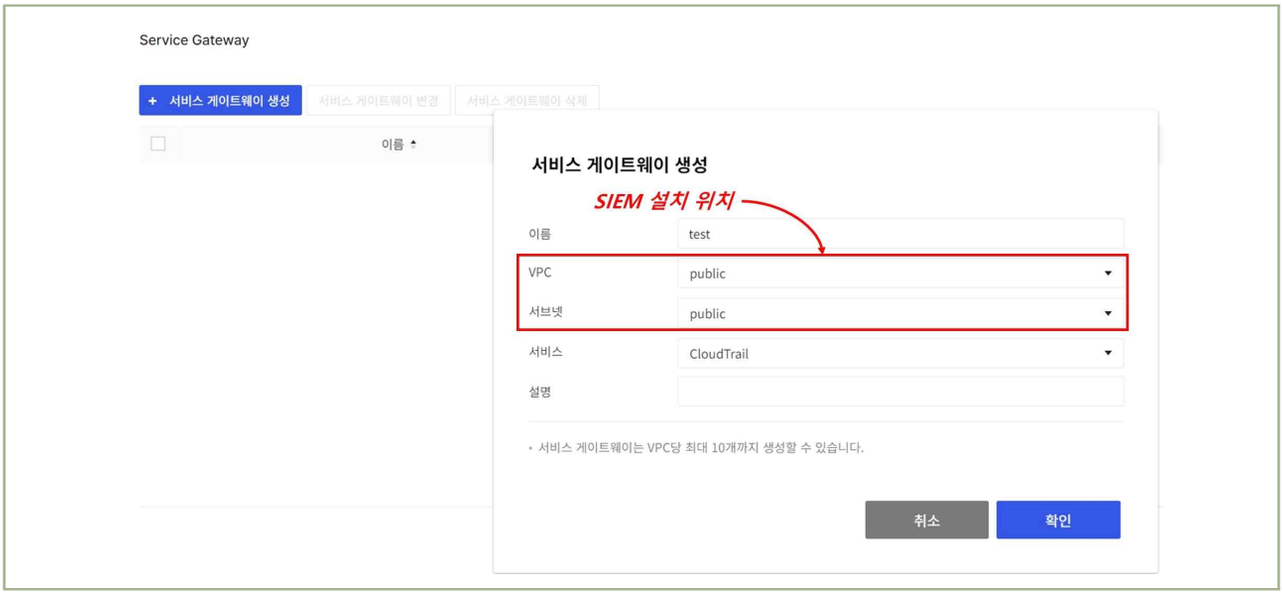
E. 이벤트 설정 시 IaaS 자원과 관련한 이벤트는 “기본 인프라 서비스”로 조회 시 확인이 가능합니다.

F. 이벤트에 따라 다수의 알림을 받을 수도 있으니 리소스 그룹과 태그를 잘 활용하여 꼭 필요한 대상으로만 알림을 설정하여야 합니다.

② SIEM을 통해 모니터링 구성하기

A. SIEM을 통해 CloudTrail log 및 가상자원의 log 파일을 저장하고, 대시보드, 알림 설정 등을 통해 모니터링을 구성할 수 있습니다.

B. CloudTrail log를 연동하기 위해서는 Service Gateway를 설정하여 사설통신으로 연동될 수 있도록 구성합니다.



| 그림 5-2-5 | CloudTrail log 연동을 위한 Service Gateway 생성

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

- **(가상자원관리시스템)**

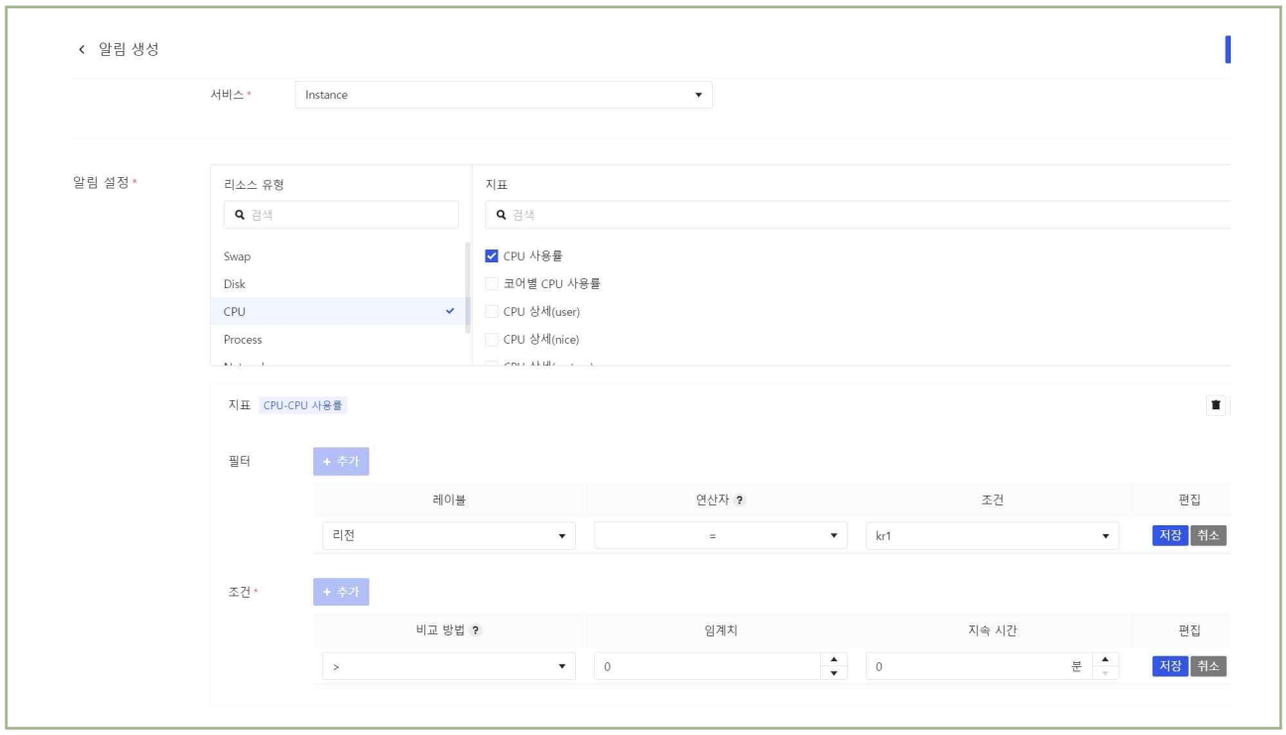
  ① Cloud monitoring 서비스를 이용하여 가상자원 상태 모니터링하기

  A. Cloud monitoring 서비스는 NHN Cloud 리소스들에 대한 시스템 및 서비스 지표를 수집하고 제공하는 서비스입니다.

  B. Swap, Disk, CPU, Process, Network, Memory 리소스를 대상으로 사용량, 송/수신량, 부하 등의 지표를 등록하고 대시보드로 모니터링할 수 있습니다.

| 그림 5-3-1 | Cloud monitoring 위젯 추가 설정

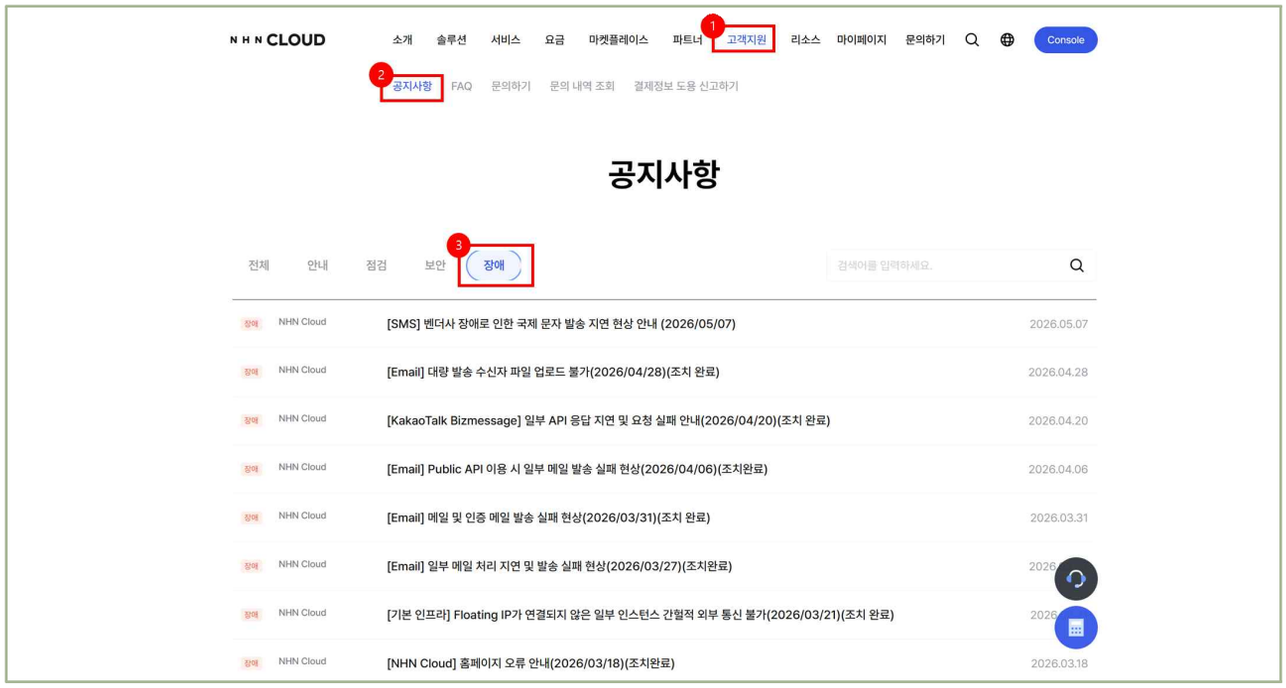
C. 그리고 해당 지표를 필터와 조건으로 알림 설정을 할 수 있습니다.



| 그림 5-3-2 | Cloud monitoring 지표별 알림 설정

② NHN Cloud의 장애 내용 확인하기

A. NHN Cloud의 서비스 장애는 홈페이지 공지사항과 mail로 안내를 하고 있습니다.



| 그림 5-3-3 | 홈페이지 장애 공지

[Email] 대량 발송 수신자 파일 업로드 불가(2026/04/28)(조치 완료)

NHN Cloud <noreply@nhncloud.com> 04.28 17:36
받는 사람:

NHN CLOUD

[Email] 대량 발송 수신자 파일 업로드 불가(2026/04/28)(조치 완료)

엔에이치엔클라우드㈜ 에서 제공하는 "통합 클라우드 서비스" NHN Cloud를 이용해 주시는 고객님께 감사의 말씀을 드립니다.

서버 오류로 인해 Email 서비스 대량 발송 수신자 파일 업로드 불가 현상이 발생하였으나 조치되어 안내드립니다.

자세한 사항은 아래 내용을 참고 부탁드립니다.

- 장애 시간
  - 2026년 04월 28일(화) 08:00~14:00(UTC +09:00)
- 장애 발생 내용
  - 서버 오류로 인한 Email 서비스 대량 발송 수신자 파일 업로드 불가
- 장애 발생 원인
  - 서버 오류
- 장애 영향도
  - Email 서비스 대량 발송 수신자 파일 업로드 불가
- 클라우드컴퓨팅서비스의 제공자의 피해 확산 방지 조치 현황
  - 서버 오류 조치 완료
- 클라우드컴퓨팅서비스의 이용자의 피해 예방 또는 확산 방지 방법
  - 해당 없음
- 담당부서 및 연락처
  - 클라우드운영팀 / 1588-7967(고객 센터)

서비스 이용에 불편을 드려 죄송합니다.

문의 사항이 있으신 경우 NHN Cloud 고객 센터로 연락 주시기 바랍니다.

감사합니다.

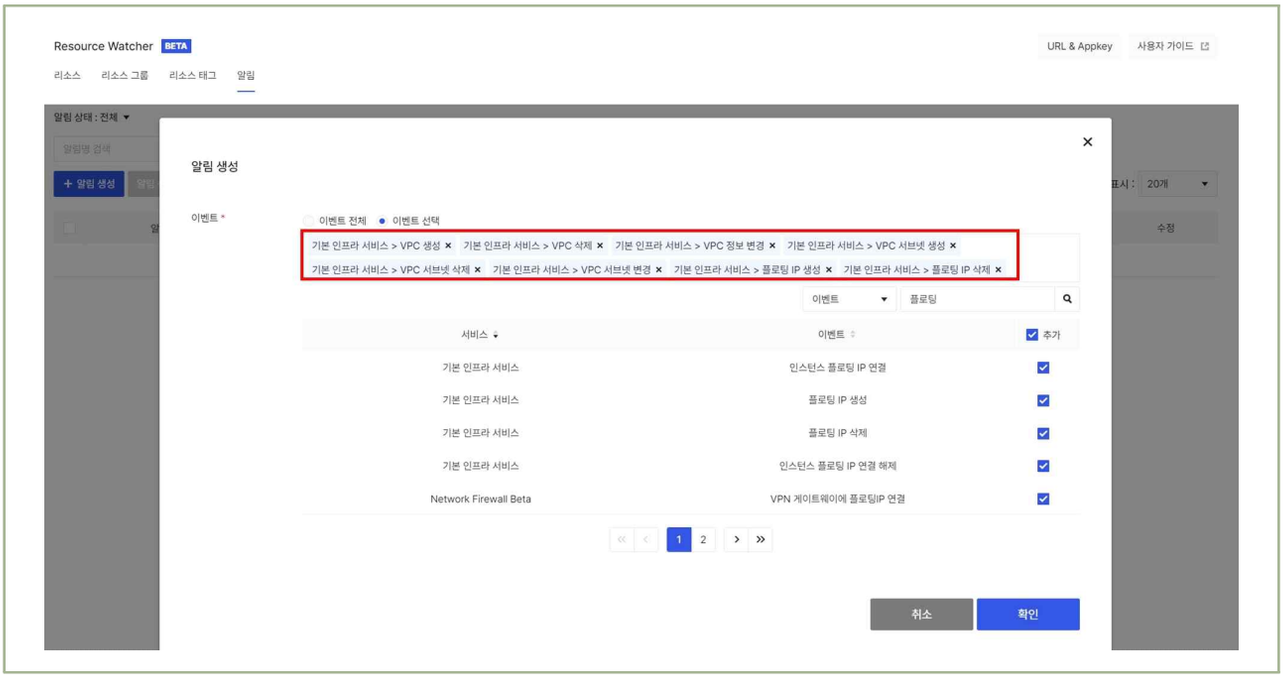
| 그림 5-3-4 | 장애 안내 메일

B. 공지 또는 장애 메일이 확인되지 않았으나, 장애가 의심되는 경우 고객센터를 통해 확인을 요청할 수 있습니다. (홈페이지 1:1 문의 또는 1588-7967)

③ Resource Watcher 서비스를 이용하여 가상자원 네트워크 변경 알림 받기

A. ‘5.2 가상자원 이용 행위추적성 증적 모니터링’에서 resource watcher에 대해 설명하였습니다.

B. 해당 서비스를 이용하여 가상자원 네트워크의 변경을 모니터링 하고 알림을 받도록 설정할 수 있습니다.



| 그림 5-3-5 | 알림 생성 이벤트 추가

C. 해당 알림 발생 시 CloudTrail 내 로그를 확인하거나 해당 가상자원 메뉴로 들어가면 네트워크 변경 내역을 확인할 수 있습니다.

1 기준

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

2 설명

- API 사용 이력에 대한 행위추적성을 확보하여야 한다.

  - 행위 감사로그

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

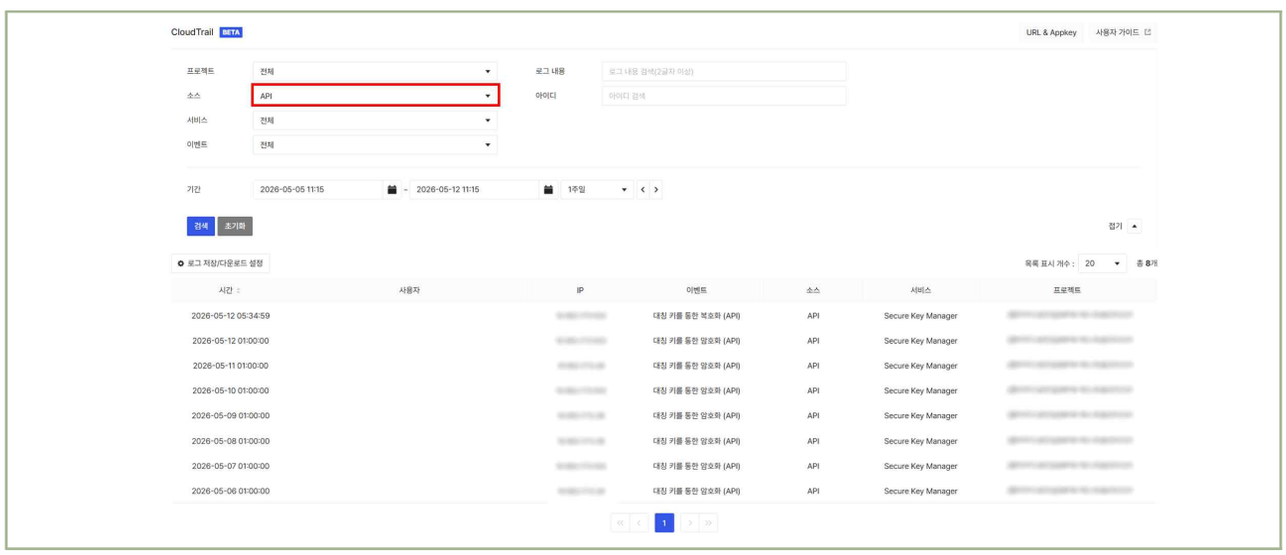
3 우수 사례

- **(가상자원관리시스템)**

  ① CloudTrail을 통한 API 호출 로그 확인

  A. CloudTrail은 API 호출에 관한 정보도 제공하고 있습니다.

  B. CloudTrail 서비스에서 소스를 'API'로 필터 설정하면, API 호출에 관한 사항을 확인할 수 있습니다.



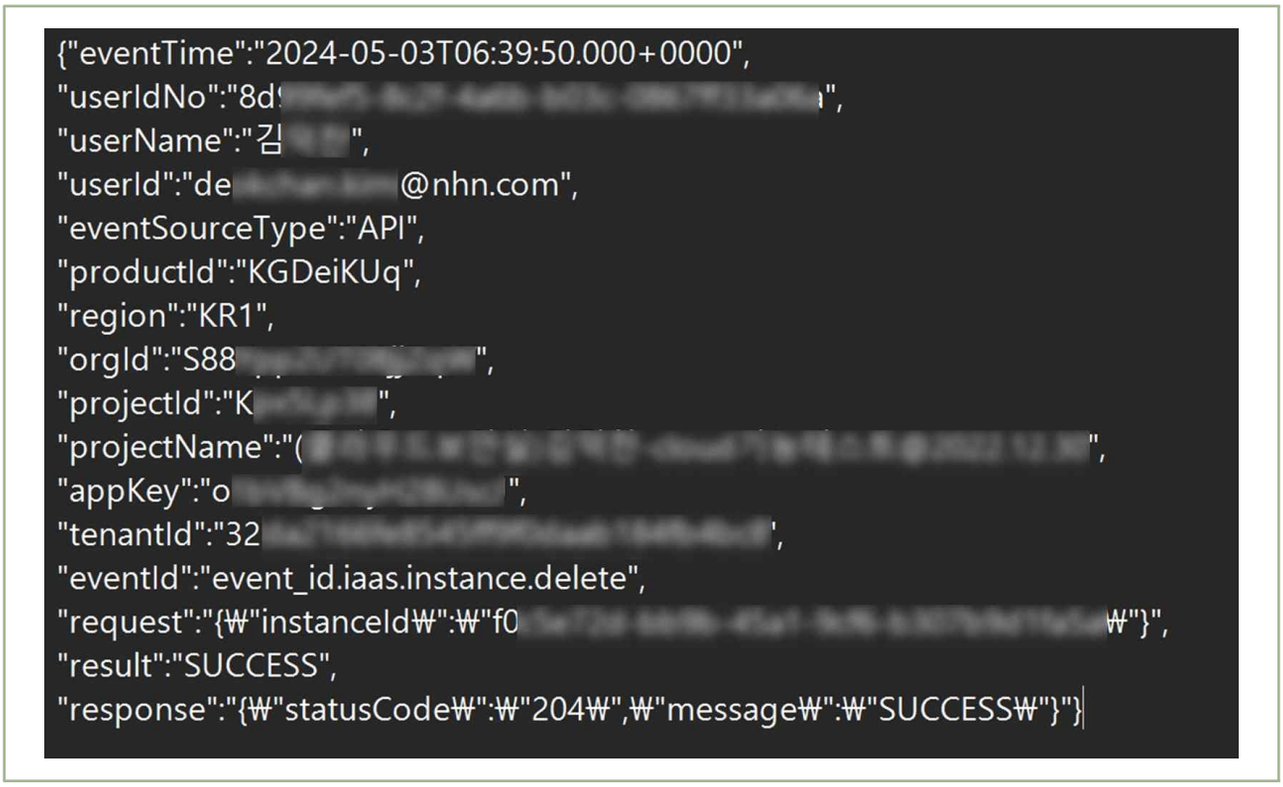
| 그림 5-4-1 | CloudTrail 서비스를 통한 API 호출 내역 확인

C. '그림 5-4-1 CloudTrail 서비스를 통한 API 호출 내역 확인'에서와 같이 API의 호출 일시, 호출자, 이벤트, 서비스, 프로젝트 등을 확인할 수 있습니다.

D. CloudTrail에서 로그를 클릭하면 더 상세한 정보를 확인할 수 있습니다.

| 그림 5-4-2 | Console을 통한 instance 삭제 API 호출 세부 내역 확인

E. CloudTrail 로그를 '로그 저장/다운로드 설정'하게 되면 위의 로그를 Object Storage에 저장할 수 있으며, 그 경우 더 상세한 원시로그를 제공합니다.



| 그림 5-4-3 | CloudTrail 로그 다운로드 시 제공되는 instance 삭제 원시로그

1 기준

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

2 설명

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

  - 행위 감사로그

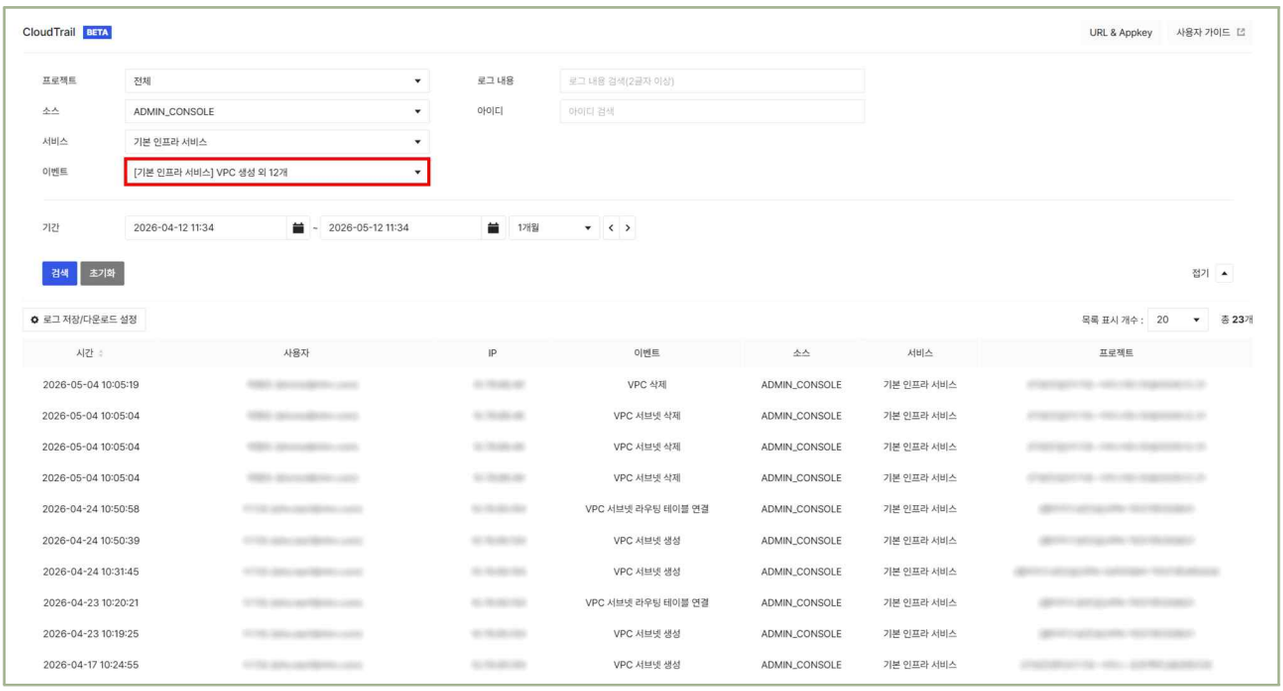
    1) 네트워크 서비스 이용에 관한 사항(VPC, NAT 규칙 생성 및 변경 등) 등

3 우수 사례

- **(가상자원관리시스템)**

  ① CloudTrail 서비스는 Console 및 API를 통한 가상자원의 생성/변경/삭제 관련한 로그를 통합 제공하고 있습니다.

  ② CloudTrail 서비스 내 필터를 이용하여 필요로 하는 이벤트의 로그를 조회할 수 있습니다.



| 그림 5-5-1 | CloudTrail 이벤트 세부 지정

③ '그림 5-5-1 CloudTrail 이벤트 세부 지정'에서는 VPC 관련한 이벤트를 특정하여 조회한 결과 화면입니다.

④ 로그를 클릭하면 세부 내역 확인이 가능하며, '로그 저장/다운로드 설정'을 하게 되면 해당 로그를 Object Storage에 저장할 수 있습니다. 또한 로그 다운로드 시 UI 상에서 조회되는 정보보다 더 많은 정보를 제공받을 수 있습니다.

⑤ 추후 책임추적이 가능한 수준으로 로그를 보관/관리하려면, 반드시 Object Storage에 연동하여서 로그를 저장하셔야 합니다.

| 그림 5-5-2 | Object Storage로 저장한 NAT Gateway 생성/삭제 원시 로그

1 기준

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

2 설명

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

  - 행위 감사로그

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

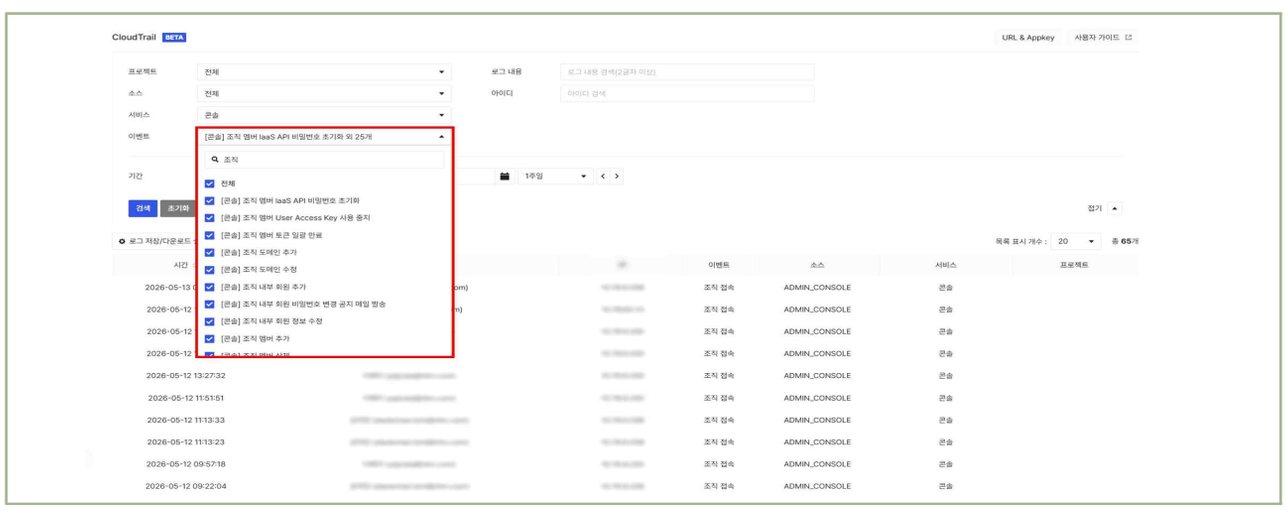
    2) 클라우드 가상자원(서버, 데이터베이스 등) 접속 계정 생성, 변경, 삭제에 관한 사항

3 우수 사례

- **(가상자원관리시스템)**

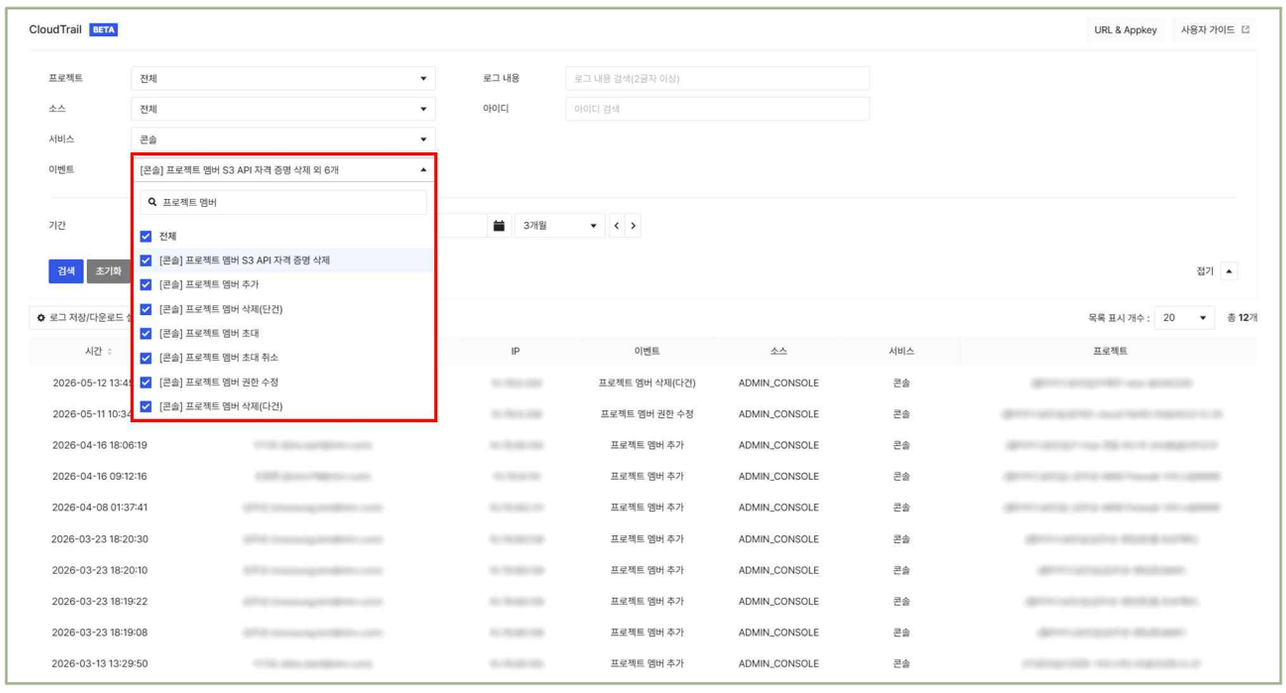
  ① NHN Cloud의 클라우드 가상자원 관리시스템 접속 계정은 NHN Cloud 계정 및 IAM 계정이 존재합니다. 그리고 모든 계정의 조직 및 프로젝트 권한 생성/변경/삭제 관련 로그를 CloudTrail 서비스에서 제공하고 있습니다.

  ② CloudTrail 검색 필터 중 '이벤트'를 '조직'으로 지정하면 '조직'과 관련한 접속, 조직 멤버 추가/변경/삭제 등의 로그를 조회하도록 설정할 수 있습니다.



| 그림 5-6-1 | 조직 멤버 관련 로그 조회

③ CloudTrail 검색 필터 중 '이벤트'를 '프로젝트 멤버'로 지정하면 프로젝트 멤버 초대, 프로젝트 멤버 권한 수정, 프로젝트 멤버 삭제 등 프로젝트 권한의 생성/변경/삭제 관련 로그를 조회하도록 설정할 수 있습니다.



| 그림 5-6-2 | 프로젝트 멤버 권한 변경 로그 조회

④ CloudTrail 로그는 '로그 저장/다운로드 설정' 기능을 통해 OBS로 백업 저장이 가능하며, SIEM과 연계하여 로그를 검색하거나 시나리오 기반으로 위험상황에 알람을 받도록 구성할 수 있습니다.

1 기준

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

2 설명

- 클라우드 서비스 이용 계정 변경사항에 관한 모니터링을 수행하여야 한다.

  - 예시

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

3 우수 사례

- **(가상자원관리시스템)**

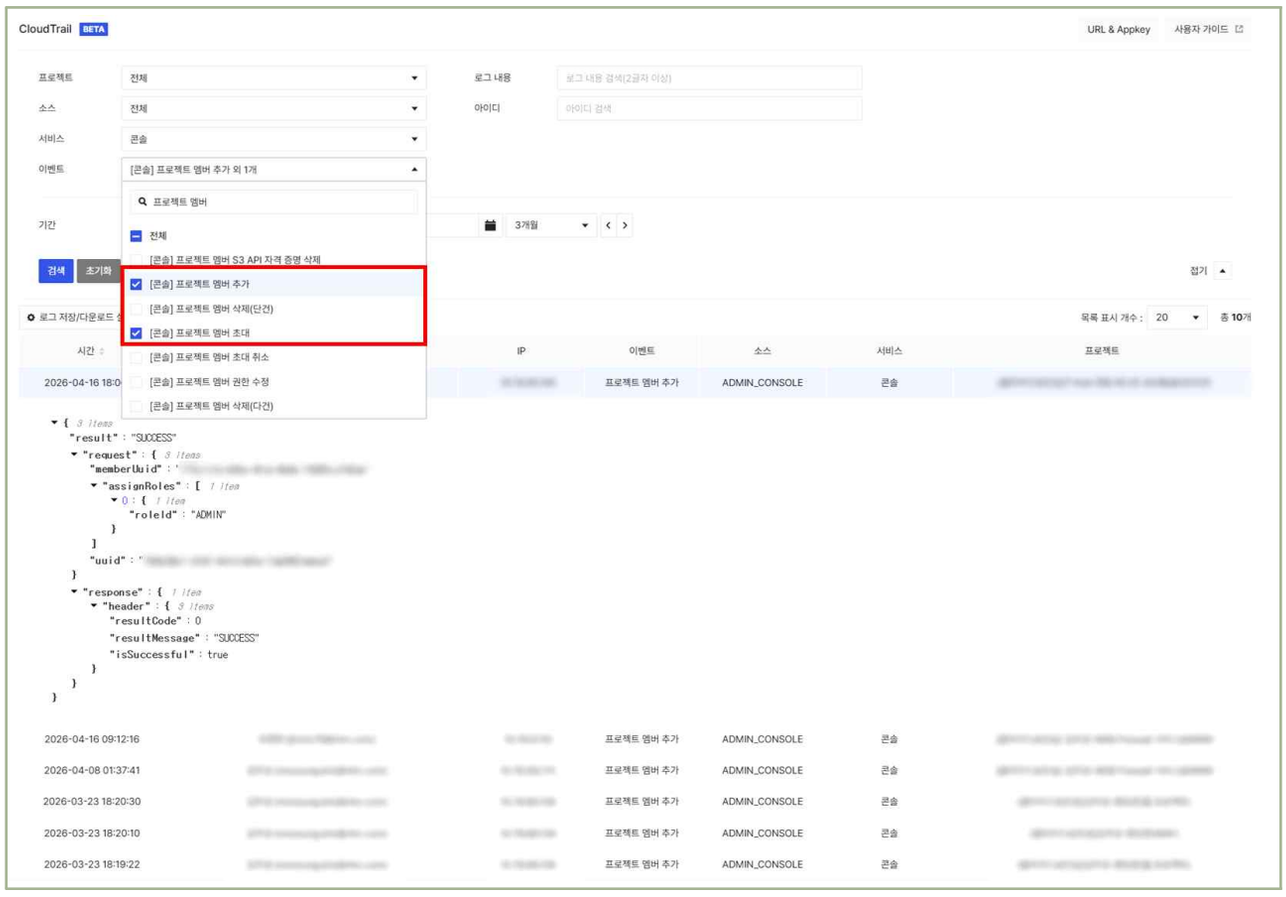
① 클라우드 가상자원 관리시스템의 경우 계정 변경에 관한 사항을 CloudTrail에서 로그로 제공하고 있습니다.

② '5.6 계정 변동사항에 대한 행위추적성 확보'에서 해당 로그를 조회하는 방법에 대해 안내하였습니다.

③ 해당 기능을 이용하여 프로젝트에 계정을 추가하는 행위를 모니터링할 수 있습니다.

④ 이벤트에 '프로젝트 멤버'를 입력하고 '프로젝트 멤버 추가', '프로젝트 멤버 초대'를 선택하는 경우 프로젝트에 사용자를 추가하는 행위를 조회할 수 있습니다.

※ 멤버 초대는 NHN Cloud에 가입되어 있지 않은 email을 멤버로 등록하려는 경우 발생하며, 멤버 추가는 그 외 모든 경우의 등록 시 발생합니다.



| 그림 5-7-1 | 프로젝트 멤버 등록 현황 모니터링

⑤ SIEM 서비스 등과 연계하는 경우 특정 프로젝트 서비스 권한을 부여하는 경우 알람을 보내거나, 이상 시간(22:00~06:00)에 권한을 변경하는 등의 행위 시 알람을 보내는 등의 모니터링 설정이 가능합니다.

6. API 관리

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

6 API 관리

1 기준

식별번호	기준	내용
6.1.	API 호출 시 인증 수단 적용	API 호출 시 이용자를 인증할 수 있는 수단을 적용하여야 한다.

2 설명

- API 호출 시 인증 수단을 적용하여 이용자를 인증한다.

  - 예시

    1) API 호출 가능한 별도 IP 지정

    2) IAM 기능과 연동하여 API를 호출할 수 있는 권한 제어 등

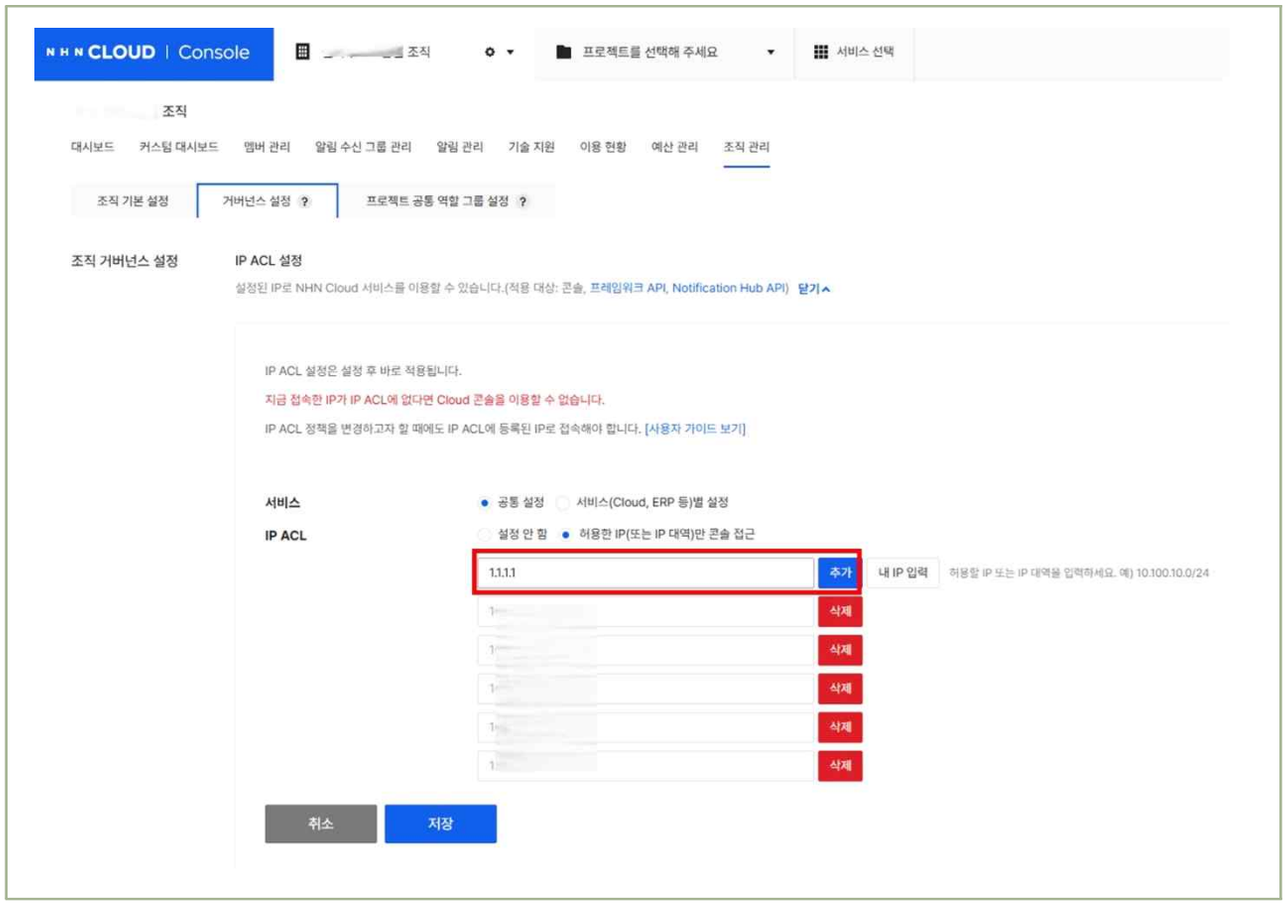
3 우수 사례

- **(가상자원관리시스템)**

  ① API 호출 시 인증을 위한 Bearer 타입의 토큰을 발급하여 사용할 수 있습니다. 토큰 발급을 위해서는 User Access Key ID와 Secret Access Key가 필요합니다.
  User Access Key ID와 Secret Access Key는 NHN Cloud 계정의 API 보안 설정 메뉴를 통해 발급할 수 있습니다.

| 그림 6-1-1 | API 보안 설정

② [조직 관리 〉〉 거버넌스 설정 〉〉 조직 거버넌스 설정 〉〉 IP ACL 설정]을 통해 IP ACL을 설정했을 경우 프레임워크 API 호출 시에 IP 접근을 제어할 수 있습니다.



| 그림 6-1-2 | IP ACL 설정 화면

③ 클라우드 계정의 역할은 필요한 권한만 부여하여 API를 호출하는 서비스 권한을 제어할 수 있습니다. API 사용 방법은 서비스별로 API가 제공되며 서비스 사용자 가이드에서 제공하는 페이지를 통해 보다 상세히 확인할 수 있습니다.

1 기준

식별번호	기준	내용
6.2.	API 호출 시 무결성 검증	API 호출 시 호출 메시지의 무결성을 보장하기 위한 방안을 확보하여야 한다

2 설명

- API 호출 시 호출 메시지의 무결성 보장 방안을 적용한다.

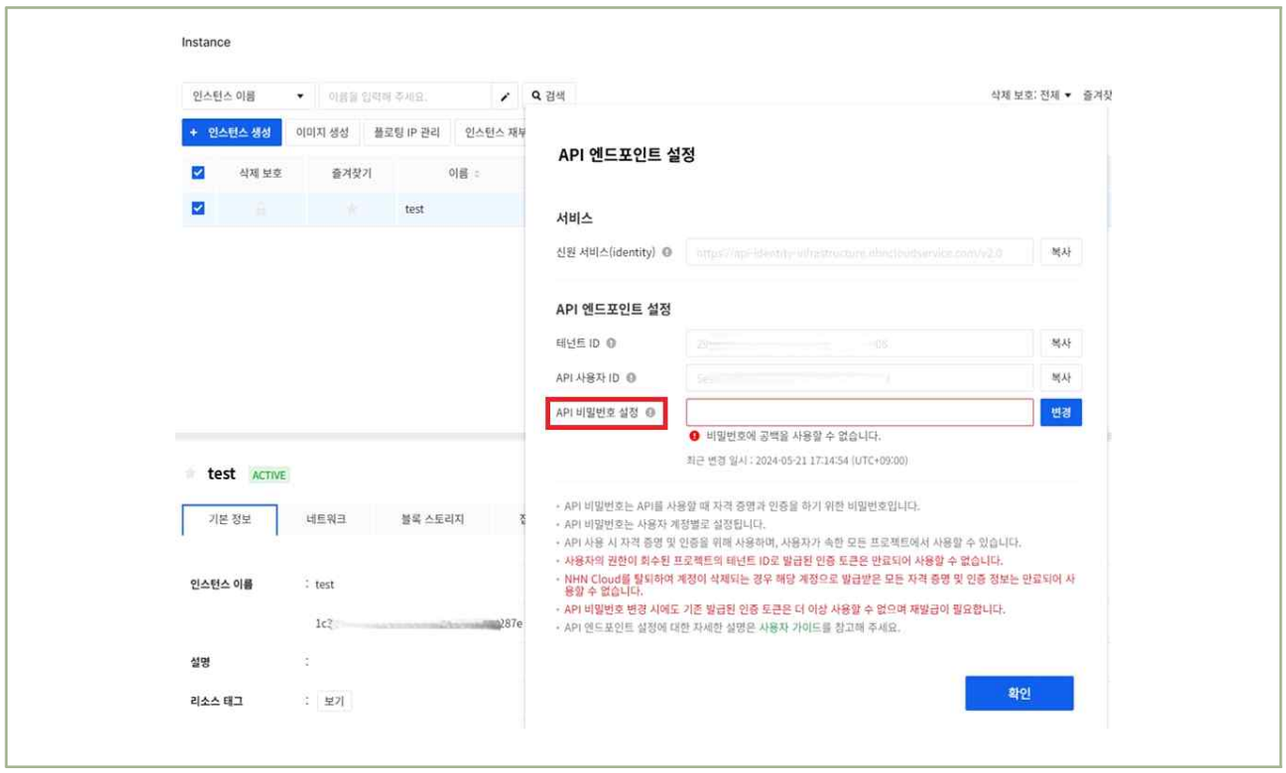
  - 예시

    1) API 보안키와 서명을 통한 변조방지 대책 마련 등

3 우수 사례

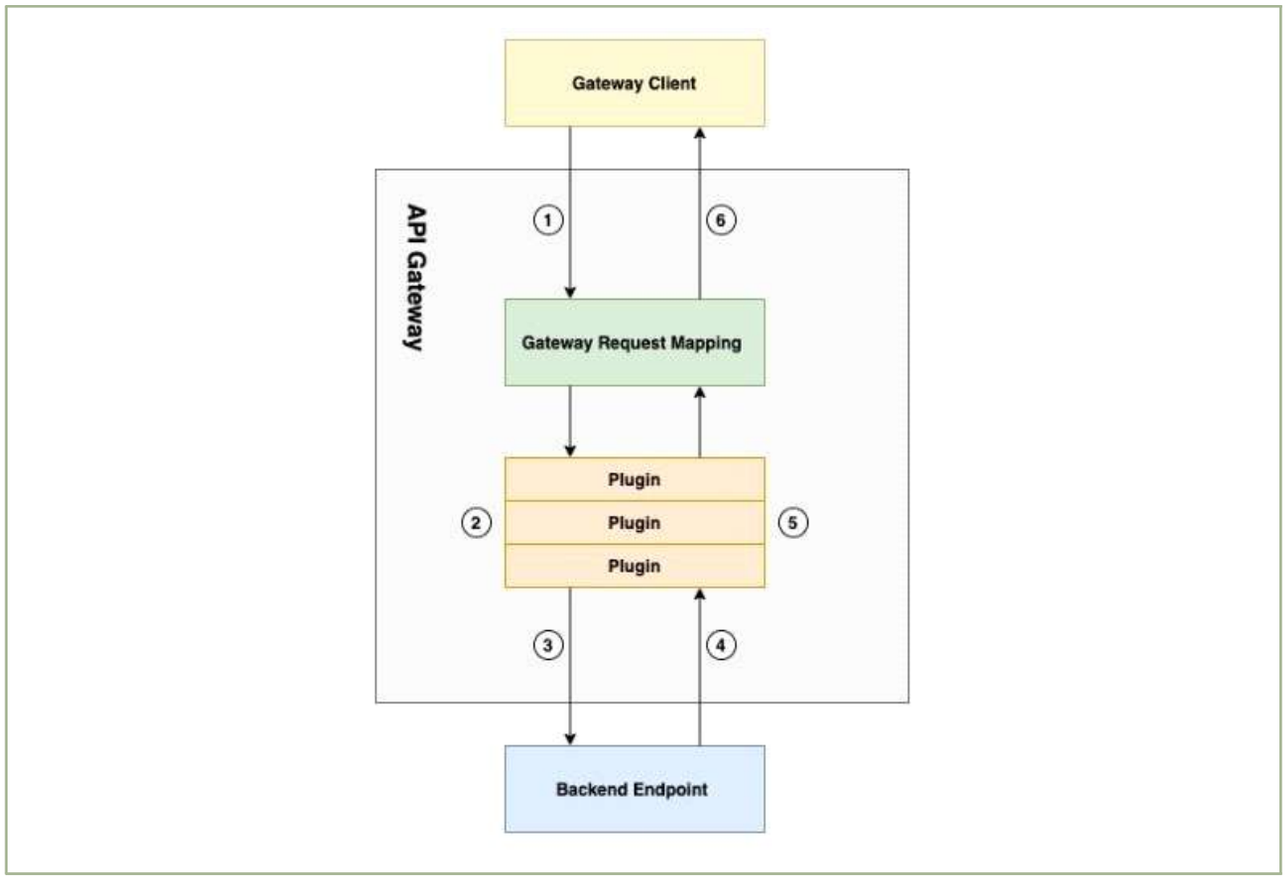
- **(가상자원관리시스템)**

  ① 기본 인프라 서비스 API에는 계정 비밀번호와 별도로 API 비밀번호를 설정하여 사용할 수 있습니다.



| 그림 6-2-1 | API 비밀번호 설정

② 여러 백엔드 엔드포인트 서비스들의 게이트웨이 역할을 하여 API의 엔드포인트를 하나로 통합할 수 있는 API Gateway 서비스를 이용할 경우 HMAC 인증을 적용하여 중간자 공격에 의해 요청이 변조되는 것을 방지할 수 있습니다. 사전에 정의된 API Gateway의 HMAC 설정을 통해 API 클라이언트는 인증 헤더와 요청 시간 헤더를 포함하여 요청해야 합니다.



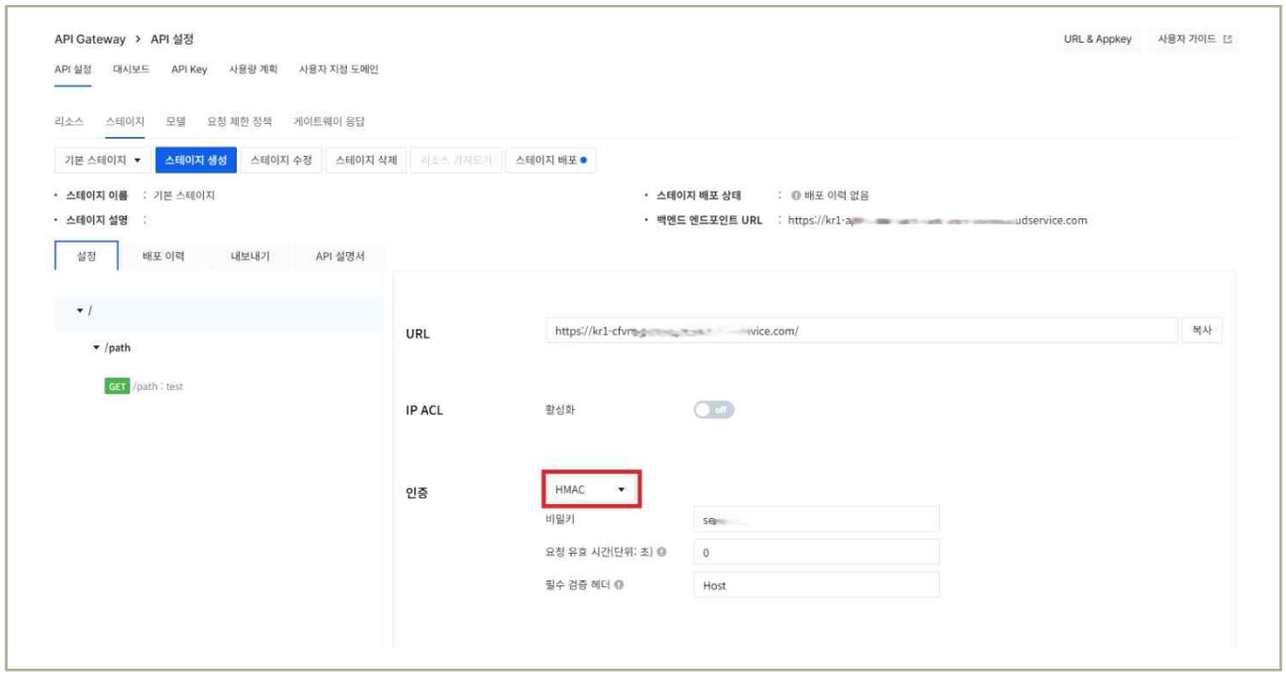
| 그림 6-2-2 | API Gateway 동작 방식

- 모든 API 요청 클라이언트는 API Gateway 리소스에 정의된 API에 대해 요청을 할 수 있습니다. 리소스는 API의 리소스 경로와 메서드를 관리합니다.
- 스테이지는 리소스를 배포하는 단계이며 스테이지별로 고유한 스테이지 URL 이 발급됩니다.
- 생성된 스테이지 탭에서 인증의 HMAC을 선택하고 관련 설정 값을 입력합니다.

  A. 비밀키: SignToString을 암호화할 비밀키를 입력합니다.

  B. 요청 유효 시간(초): 설정된 유효 시간의 양방향 시간(요청 시간의 과거/미래 시간 전 후)을 초과한 요청을 거부합니다. 요청 유효 시간을 0초로 설정할 경우 API Gateway는 유효 시간 체크를 하지 않습니다.

C. 필수 검증 헤더 목록: API 요청 검증에 필수로 포함할 헤더 목록을 작성합니다. 여러 개를 입력하려면 콤마(,)로 구분하여 입력합니다.



| 그림 6-2-3 | API Gateway HMAC 인증설정

1 기준

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

2 설명

- API 호출 시 사용되는 키 값 등은 안전하게 보관 관리해야 한다.

  - 예시

    1) API 보안키 생성 시 이용자에게 1회만 노출 등

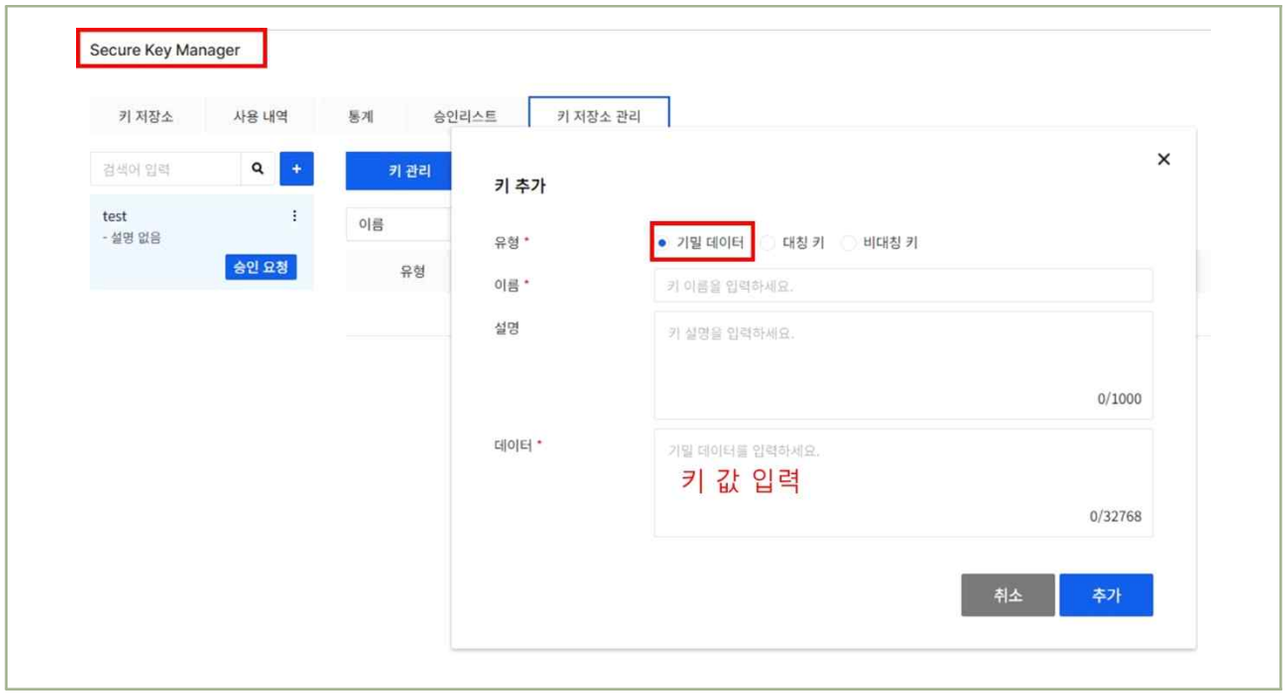
3 우수 사례

- **(가상자원관리시스템)**

  ① API 호출 시 인증에 사용되는 Secret Access Key는 발급 시 1회만 노출이 됩니다. 발급받은 Key는 Secure Key Manager 서비스의 기밀 데이터로 저장하여 관리할 수 있습니다.

| 그림 6-3-1 | Secret Access Key 발급 메시지

② Secure Key Manager의 키 저장소에 “기밀 데이터” 유형으로 Secret Access Key를 추가하여 암호화 된 상태로 안전하게 보관할 수 있습니다.



| 그림 6-3-2 | Secure Key Manager로 키 암호화하여 관리

1 기준

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

2 설명

- API 세션 및 서명 값에 대한 유효기간 설정하고, 유니크 값(보안키 등) 유출 방지대책으로 만료기간을 적용하여야 한다.

  - 예시

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

3 우수 사례

- **(가상자원관리시스템)**

  ① API 인증 시 사용되는 User Access Key 생성 시 토큰 유효 시간을 설정할 수 있습니다.

| 그림 6-4-1 | 토큰 유효 시간 설정

② "그림 6-2-3 API Gateway HMAC 인증설정"과 같이 API Gateway 서비스의 HMAC 인증 사용 시 "요청 유효 시간" 설정을 통해 Reply Attack 공격에 대응할 수 있습니다.

1 기준

식별번호	기준	내용
6.5.	API 호출 구간 암호화 저장	**API를 통한 클라우드 가상자원 관리 수행 시 네트워크 트래픽 보호를 위한 암호화된 통신구간을 적용하여야 한다**

2 설명

- API 사용 시 네트워크 구간 보호를 위해 암호화된 통신구간을 적용해야 한다.

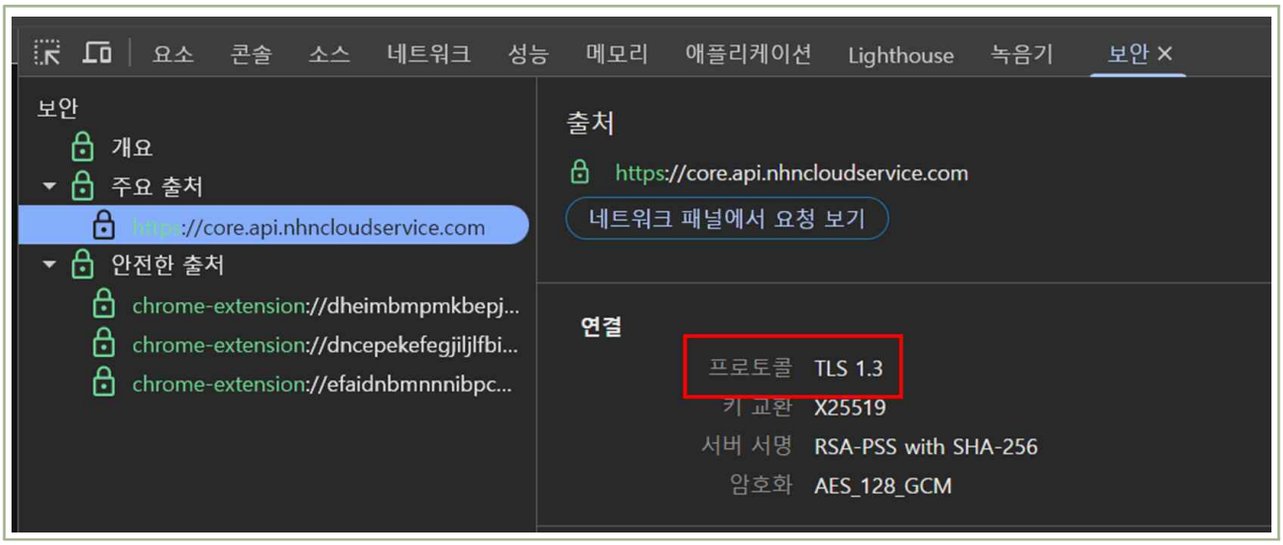
  - 예시

    1) SSL 적용 등

3 우수 사례

- API 호출 시 안전한 통신구간 적용

  ① NHN Cloud의 조직 및 프로젝트를 관리하는 프레임워크 API 도메인은 https://core.api.nhncloudservice.com/입니다. 해당 엔드포인트의 경우 https로 접근하며 TLS 1.3 등을 지원합니다. NHN Cloud는 최신의 TLS 버전 적용을 위해 업데이트가 지속적으로 진행되고 있음을 참고해 주시기 바랍니다.



| 그림 6-5-1 | 프레임워크 API의 TLS 버전 확인

서비스 개별 엔드포인트는 서비스별 사용자 가이드에서 확인 가능합니다.

7. 스토리지 관리

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

7 스토리지 관리

1 기준

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

2 설명

- 스토리지 사용 목적에 따라 적절한 접근 통제를 수행해야 한다.

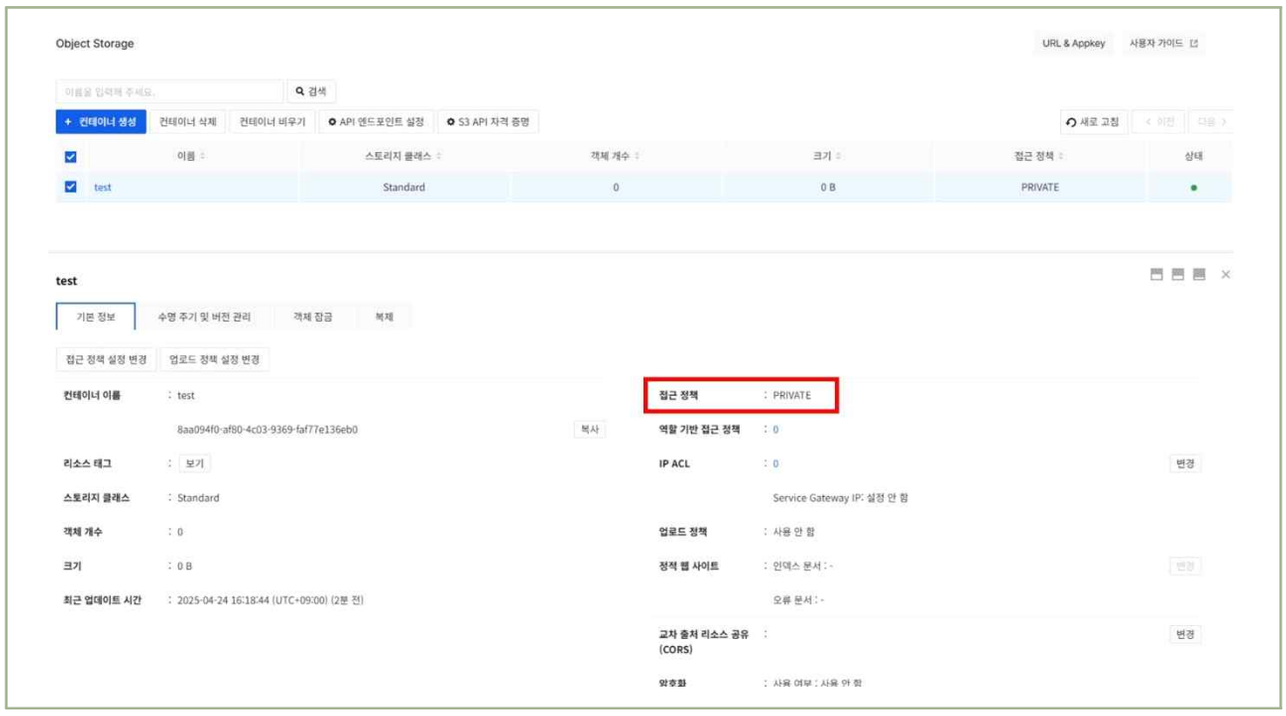
  - 예시

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

3 우수 사례

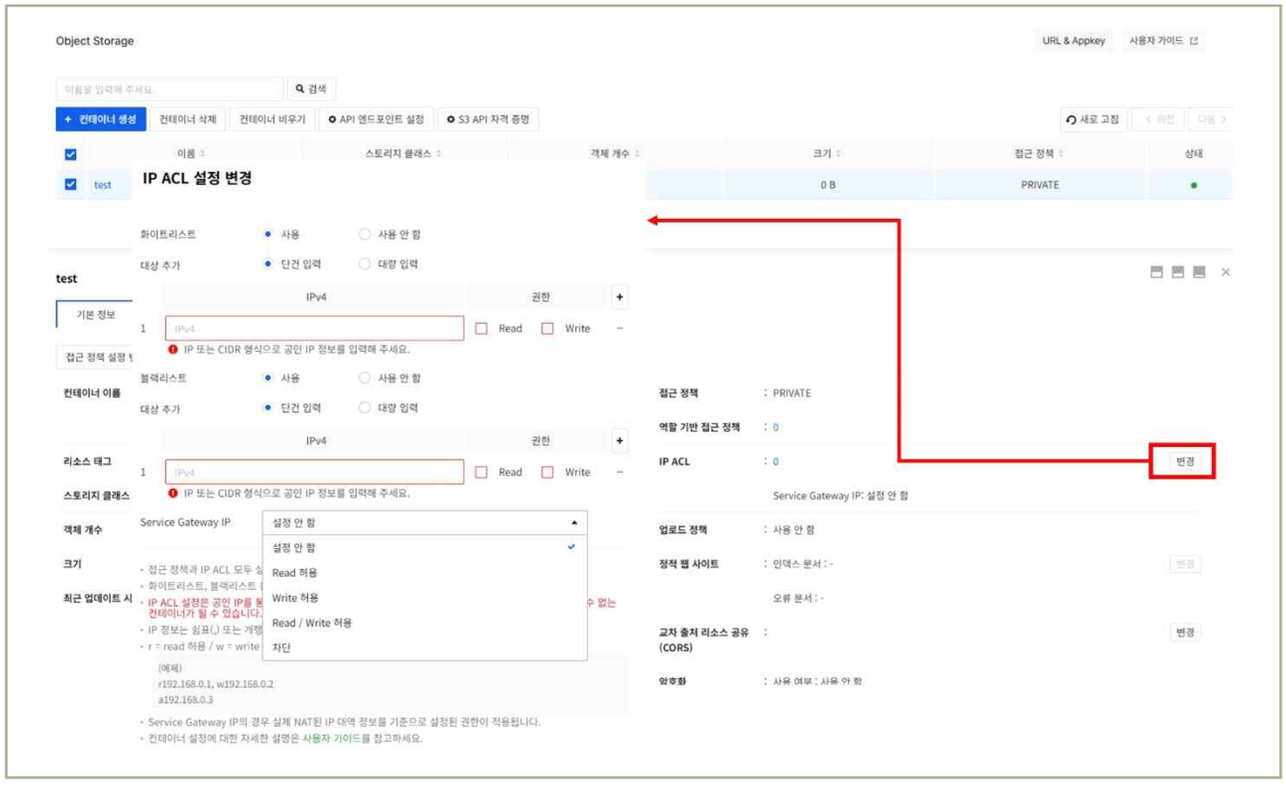
- **(가상자원관리시스템)**

  ① 외부 공개가 불필요한 오브젝트 스토리지는 Private 설정을 통해 외부 접근을 차단할 수 있습니다. Private 설정은 컨테이너가 속한 프로젝트의 사용자에게만 접근 권한을 부여하는 기본 접근 정책입니다.



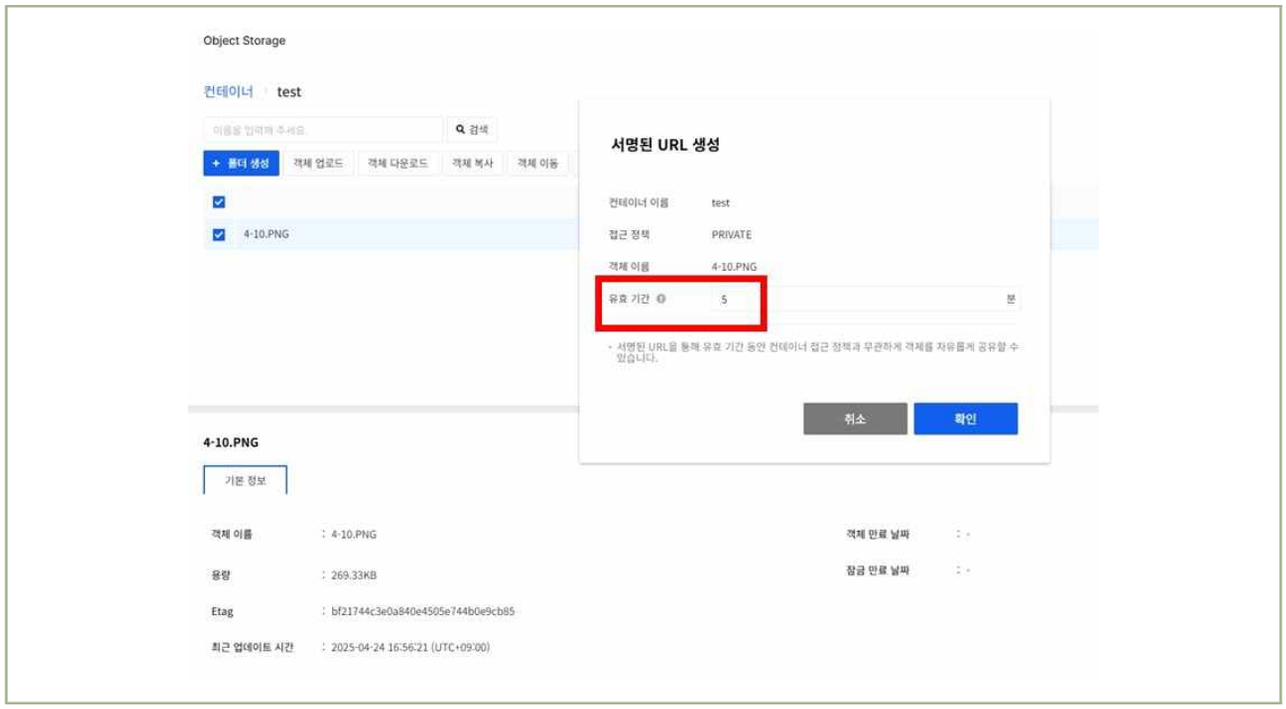
| 그림 7-1-1 | Object Storage 접근 정책 설정

② Whitelist 또는 Blacklist 기반의 세부적인 IP 접근제어와 권한 설정이 가능하며 Service Gateway를 통해 접근하는 것에 대해 Read/Write 권한 설정이 가능합니다.



| 그림 7-1-2 | Object Storage IP ACL 설정

③ Object Storage 컨테이너에 업로드 된 파일에 접근 시 서명된 URL을 생성하여 일정 시간 동안만 접근할 수 있도록 설정할 수 있습니다.



| 그림 7-1-3 | Object Storage IP ACL 설정

1 기준

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

2 설명

- 스토리지 사용 목적에 따라 읽기, 쓰기 등 권한을 세분화하여 관리한다.

  - 예시

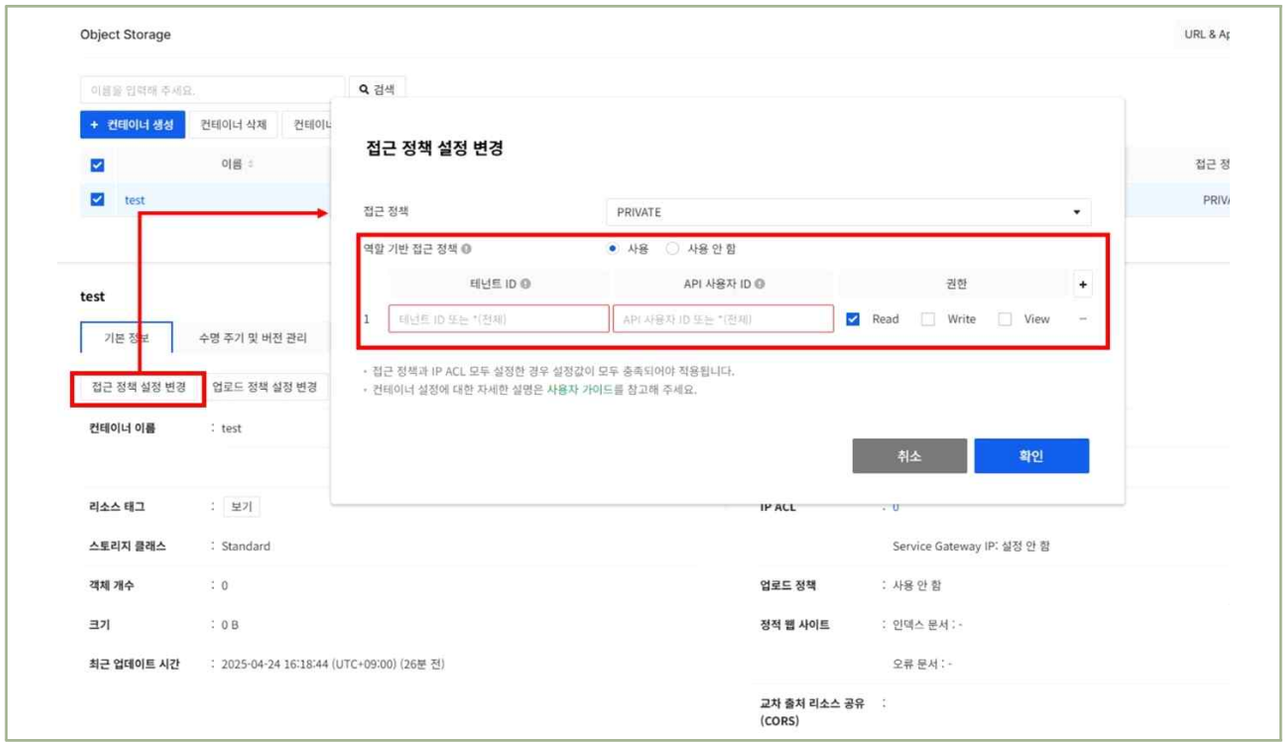
    1) 스토리지 객체 권한(읽기, 쓰기 등)을 목적에 따라 적용

    2) 스토리지 권한 부여 현황에 대해 주기적인 검토 수행 등

3 우수 사례

- **(가상자원관리시스템)**

  ① 클라우드 콘솔에서 '접근 정책 설정 변경' 메뉴를 통해 접근 허용할 테넌트 및 API 사용자 ID를 설정할 수 있습니다.

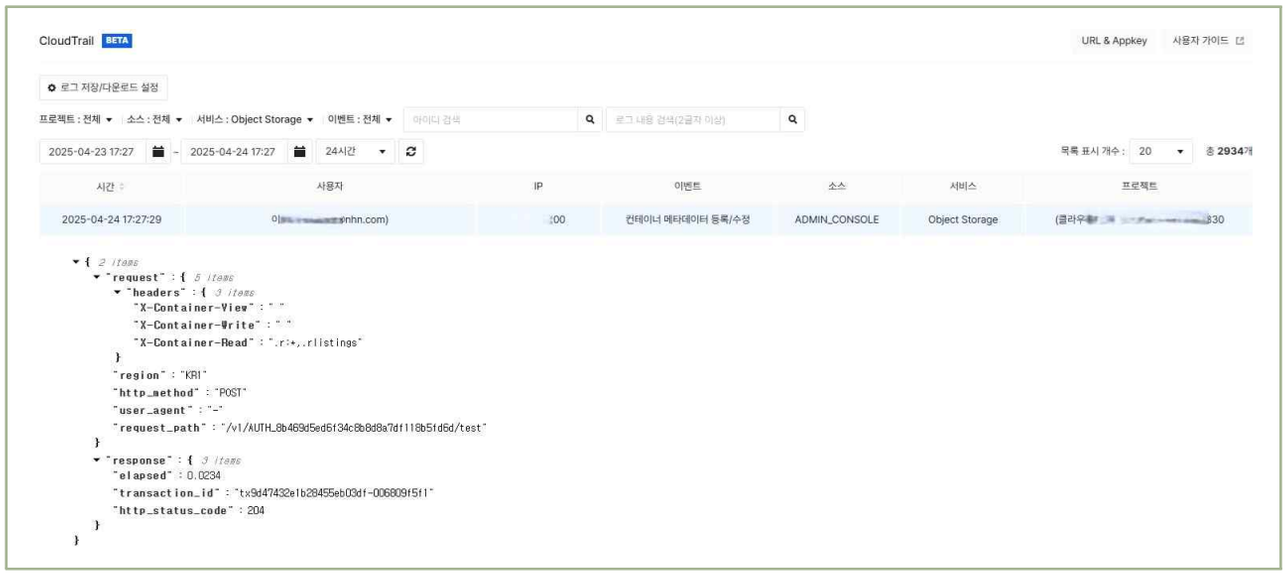


| 그림 7-2-1 | 접근 정책 설정 변경

② API를 사용해 컨테이너의 X-Container-Read, X-Container-Write 속성에 역할 기반 접근 정책 요소를 입력하면 여러 가지 상황에 맞게 접근 정책을 설정할 수 있습니다.

역할 기반 접근 정책 요소 리스트는 사용자 가이드(접근 정책 설정 가이드)를 통해 확인할 수 있습니다.

③ Object Storage의 접근 정책 변경 등은 CloudTrail 로그를 통해 상세 내역을 확인할 수 있습니다.



| 그림 7-2-2 | 접근 정책 변경 CloudTrail 로그

1 기준

식별번호	기준	내용
7.3.	**스토리지 업로드 파일 제한**	**스토리지 목적에 맞는 파일만 업로드 될 수 있도록 업로드 가능한 파일을 제한하여야 한다**

2 설명

- 스토리지 목적에 맞는 파일만 업로드 가능하도록 제한한다.

  - 예시

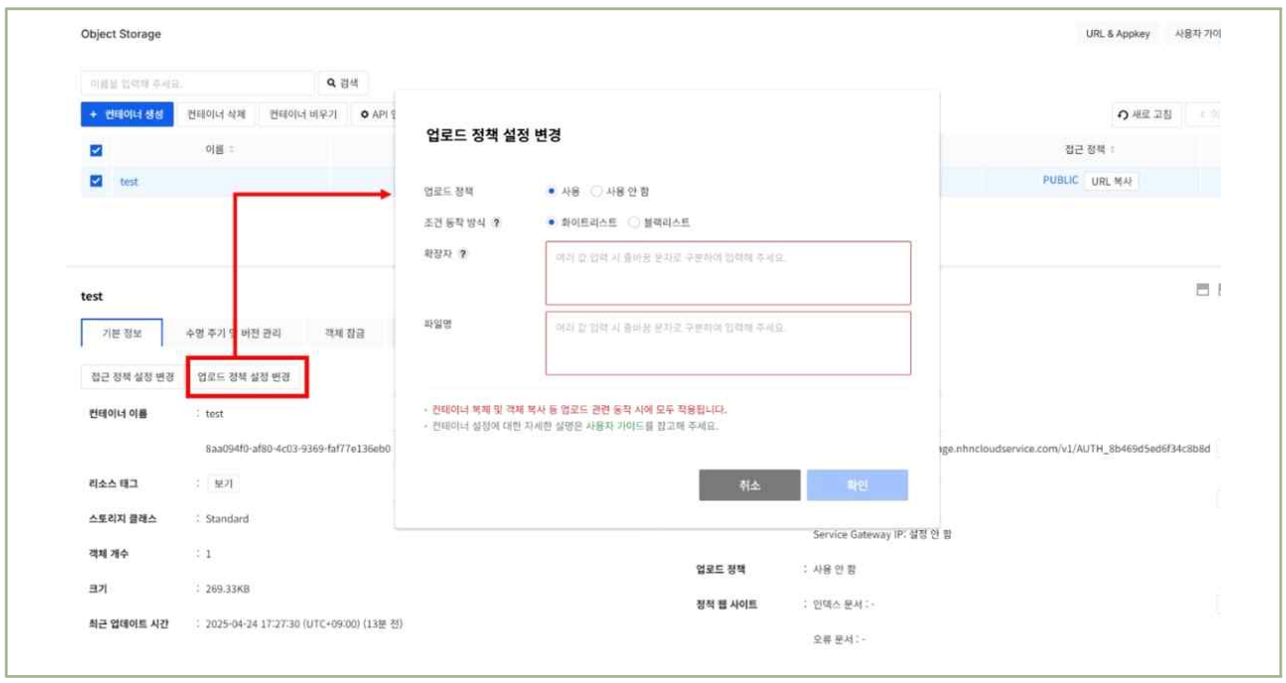
    1) 스토리지 버킷 정책 설정을 통한 업로드 파일 확장자 제한

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

3 우수 사례

- **(가상자원관리시스템)**

  ① 업로드 정책 설정 기능으로 파일 확장자, 파일명 등의 설정을 통해 업로드 되는 파일을 제한할 수 있습니다.



| 그림 7-3-1 | 업로드 정책 설정

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 행위 추적성 증적(로그 등) 백업**	**클라우드 이용 시 발생하는 로그에 대해 백업을 수행 1년 이상 보관하여야 한다**

2 설명

- 클라우드 이용 시 발생하는 로그는 1년 이상 보관하여야 한다.

  - 예시

    1) 스토리지 행위 감사로그 백업

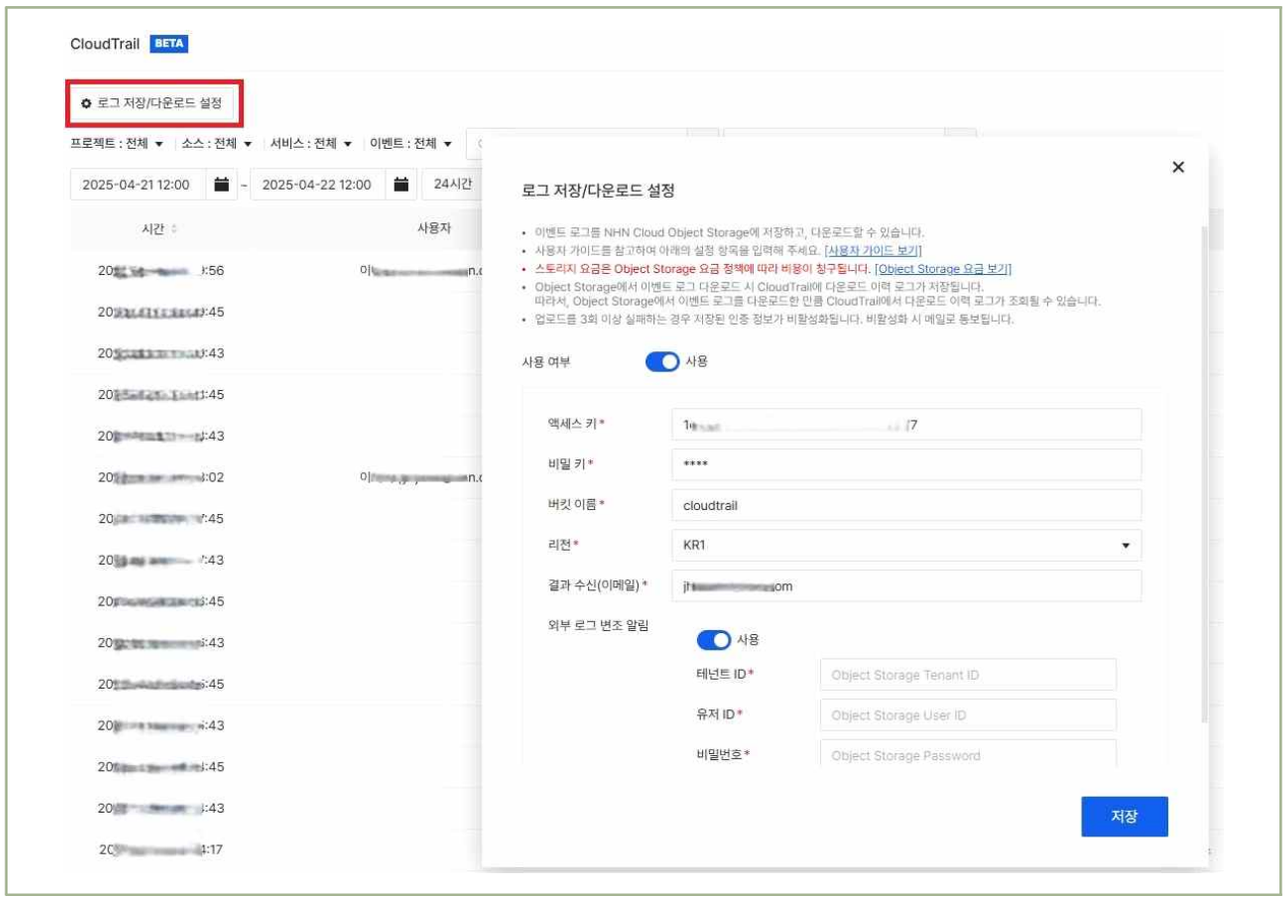
    2) 클라우드 웹 콘솔 감사로그 별도의 파일로 보관 등

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

3 우수 사례

- **(가상자원관리시스템)**

  ① CloudTrail을 통해 스토리지, 웹 콘솔 관련 행위 등의 로그가 기록되고 확인할 수 있습니다. CloudTrail에는 최대 3개월의 로그가 저장되며 로그를 장기 보관하기 위해서는 NHN Cloud Object Storage를 활용하여 저장/다운로드 할 수 있습니다.



| 그림 8-1-1 | CloudTrail 로그 저장

1 기준

식별번호	기준	내용
8.2.	**행위추적성 증적(로그 등) 백업 파일 무결성 검증**	**이용자의 행위추적성 백업 증적 로그 등은 무결하게 보관하여야 한다.**

2 설명

- 이용자의 행위추적성 백업 로그 등은 무결하게 보관해야 한다.

  - 예시

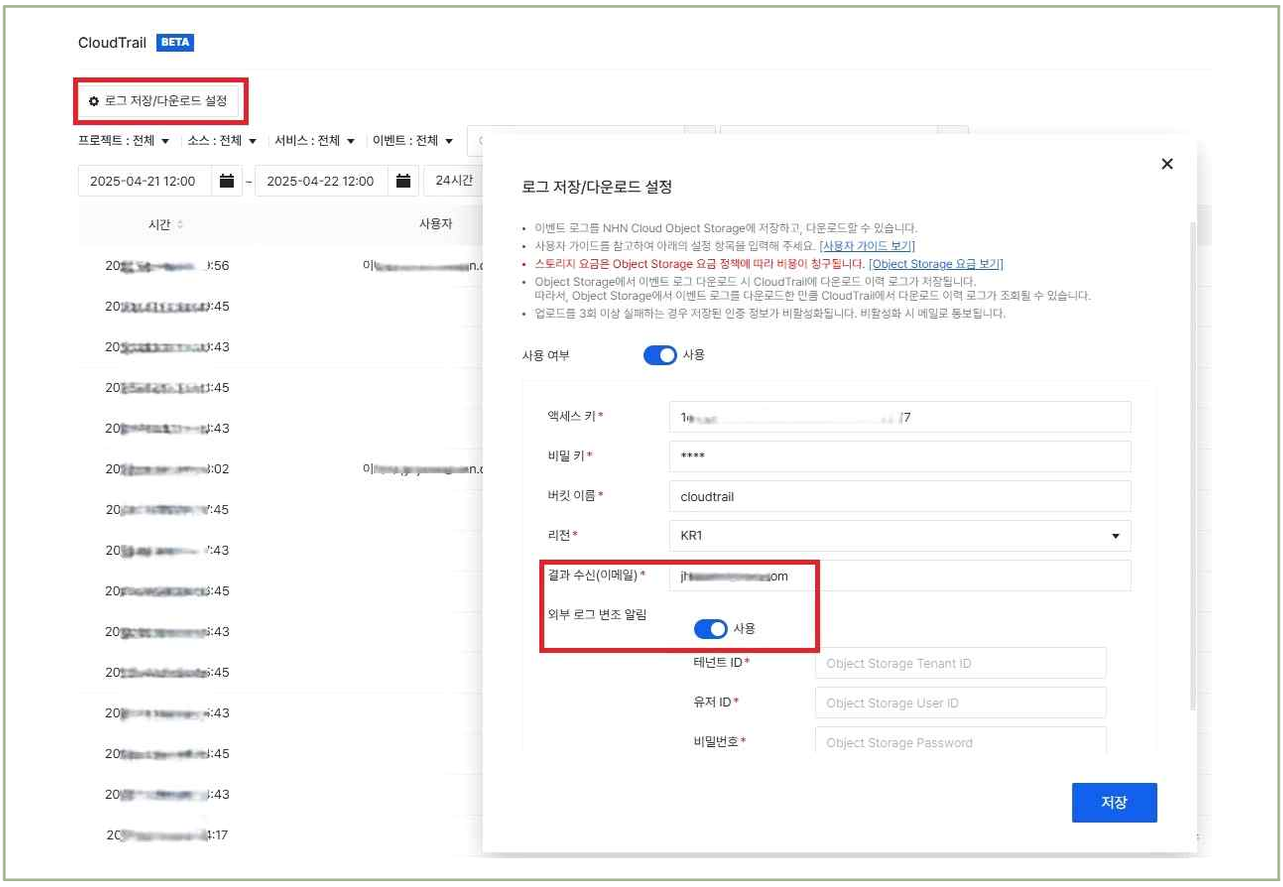
    1) 감사로그 훼손 탐지에 대한 알람 설정

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

3 우수 사례

- **(가상자원관리시스템)**

  ① CloudTrail에 저장되는 로그를 외부 Object Storage을 통해 장기 보관할 수 있습니다. Object Storage 내 로그들이 임의로 수정 또는 삭제될 때 알림 기능을 통해 이메일로 알림을 받을 수 있습니다. 외부 로그 변조 알림은 NHN Cloud Object Storage를 사용하는 경우 제공되는 기능이며 메일은 0분/30분 단위로 발송됩니다.

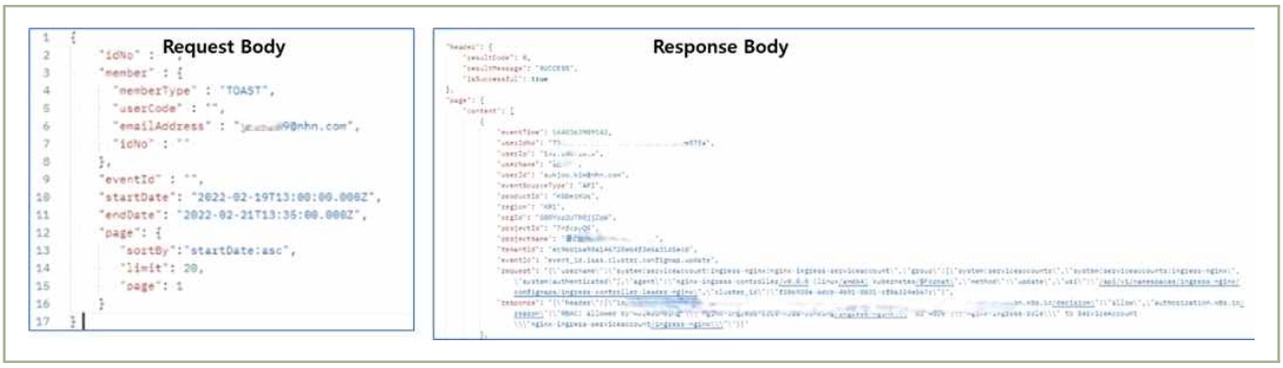


| 그림 8-2-1 | CloudTrail 외부 로그 변조 알림 기능

| 그림 8-2-2 | 로그 변조 시 메일 알림 예시

4 참고 사항

- CloudTrail에 API를 호출해, 사용자가 설정한 조건에 맞는 이벤트를 조회하고 결과를 NHN Cloud 외부에서 별도로 관리할 수 있습니다. 단, 외부에서 별도로 관리하는 로그는 로그를 관리하는 솔루션의 무결성 체크 기능 등을 통해서 무결성 관리가 필요합니다. NHN Cloud의 마켓플레이스 등에서 제공하는 통합 로그 솔루션 등을 활용할 수 있으며 CloudTrail API 상세 내용은 사용자 가이드를 통해 상세히 확인 가능합니다.



| 그림 8-2-3 | CloudTrail API 호출 Request, Response 예시

- 백업 파일을 로컬 또는 자체 파일서버, 백업 서버 등에 저장하는 경우 hash check를 통해 무결성을 확인할 수 있습니다. 파일의 hash값을 저장하고, 매일 기존에 저장된 hash값과 점검 시 계산된 hash 값을 비교하도록 script를 작성하여 무결성 점검을 수행할 수 있습니다.
- NHN Cloud 마켓플레이스

1 기준

식별번호	기준	내용
8.3.	**금융회사 전산자료 백업**	**관련 법령(전자금융감독규정 등)에 따라 백업이 필요한 금융회사 중요 전산자료는 별도 보관 및 관리하여야 한다**

2 설명

- 백업이 필요한 금융회사 중요 전산자료는 별도 보관, 관리하여야 한다.

  - 예시

    1) 클라우드 서비스 제공자(CSP)의 백업 서비스 이용

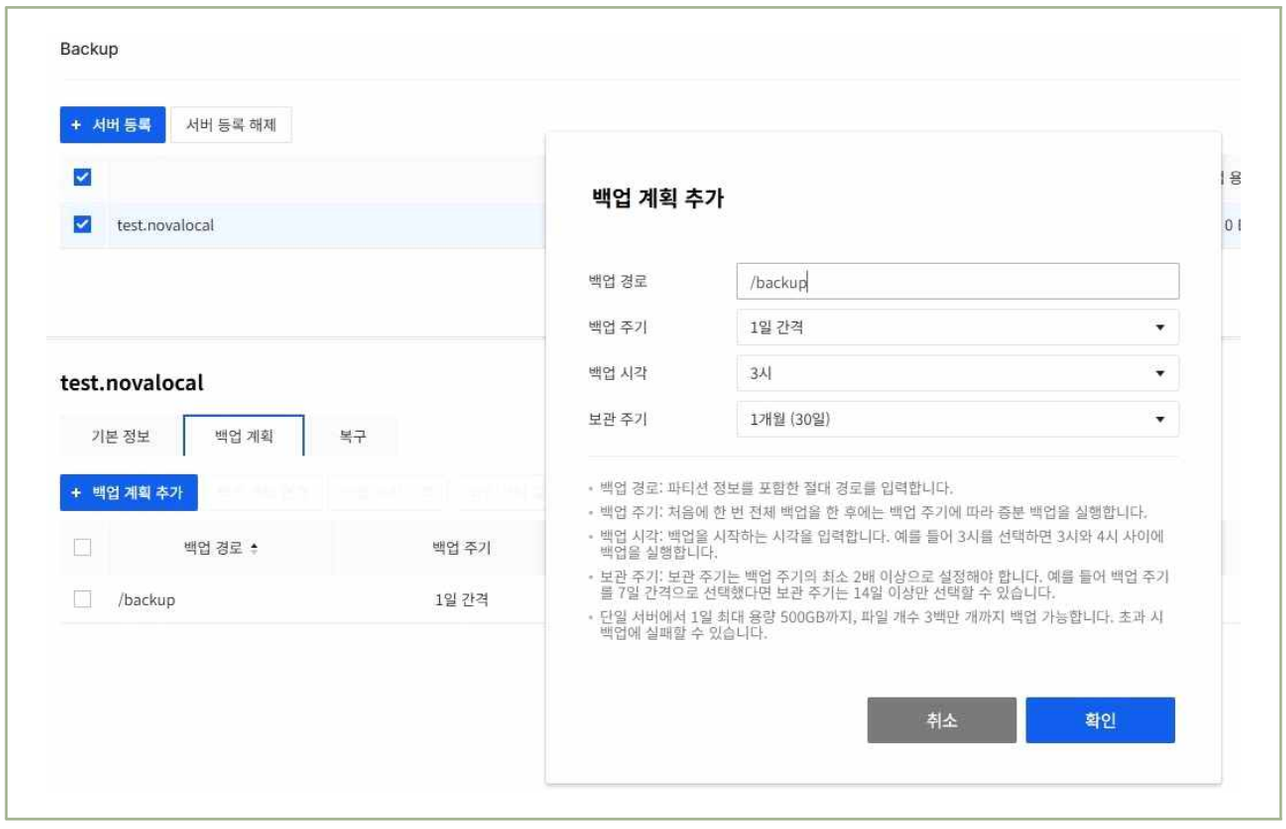
    2) 전산자료를 별도로 다운받아 금융회사가 관리하는 백업 서버 내 보관 등

3 우수 사례

- **(가상자원관리시스템)**

  ① Backup 서비스를 이용하여 위협, 사용자의 조작 실수, 시스템 장애 등으로 인한 데이터 손실에 대비해 데이터의 복제본을 만들고 안전하게 보관할 수 있습니다. Backup 서비스에서 제공하는 에이전트를 서버에 설치하고 백업할 경로를 지정하여 중요 데이터를 주기적으로 백업하도록 설정할 수 있습니다. 에이전트 설치 방법은 Backup 서비스 사용자 가이드를 통해 상세히 확인하실 수 있습니다.

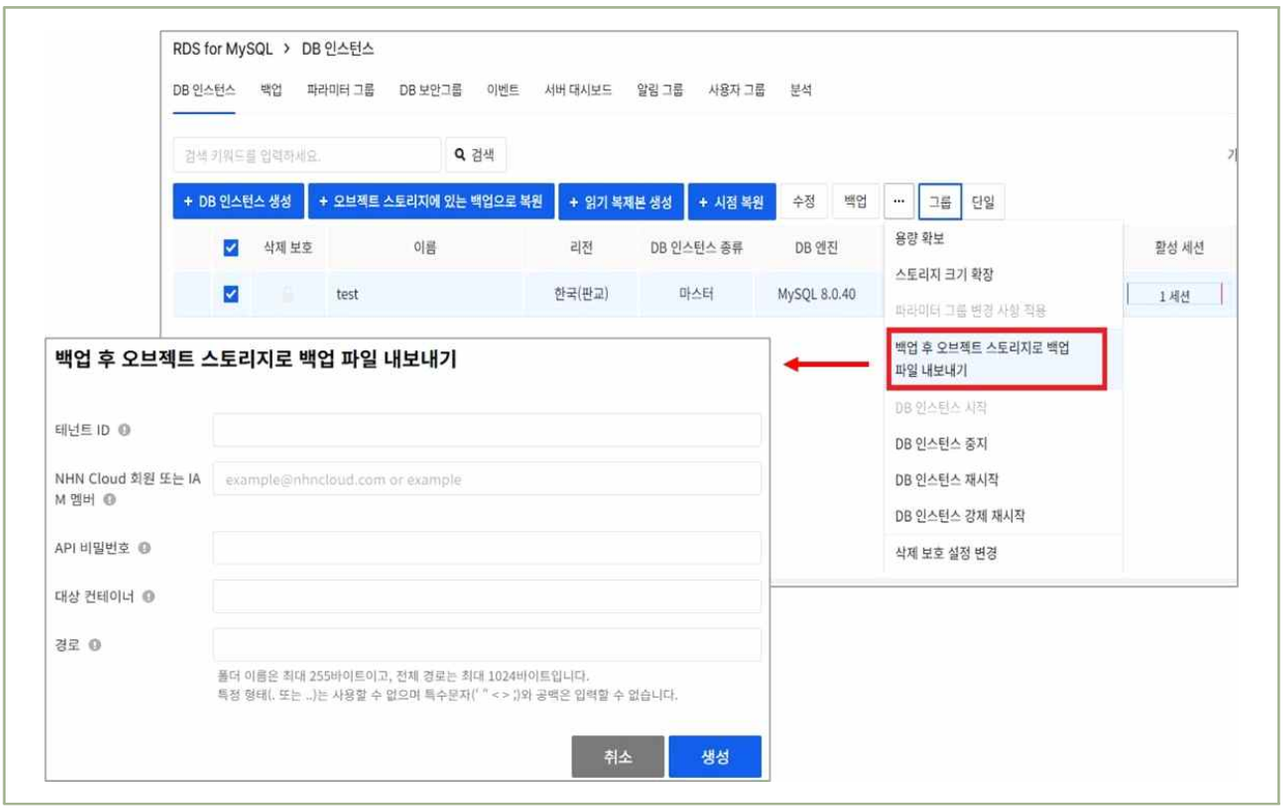
  백업 에이전트가 설치된 서버를 클라우드 콘솔에서 추가하여 백업 계획 및 백업 대상 경로를 설정하여 주기적으로 데이터가 백업될 수 있도록 설정합니다.



| 그림 8-3-1 | Backup 서비스를 이용한 주기적인 데이터 백업

② RDS의 백업 및 복원 기능을 사용하여 데이터를 백업할 수 있습니다. RDS for MySQL, RDS for PostgreSQL, RDS for Maria, RDS for MS-SQL의 RDS 생성 시 “백업 및 복원” 기능을 설정하여 주기적으로 데이터가 백업되도록 합니다.

백업 후 백업 파일을 오브젝트 스토리지로 내보낼 수 있습니다. (전체 백업에 대해 지원)



| 그림 8-3-2 | RDS의 백업 및 오브젝트 스토리지로 내보내기

4 참고 사항

- 사용자가 생성한 클라우드 DB, 스토리지 등에 생성/저장되는 데이터 등은 마켓플레이스의 「스토리지」 제품군 내 백업 상품을 구성하여 다양한 방법으로 백업할 수 있습니다.
- NHN Cloud 마켓플레이스

1 기준

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

2 설명

- 백업 파일의 무결성이 보장되어야 한다.

  - 예시

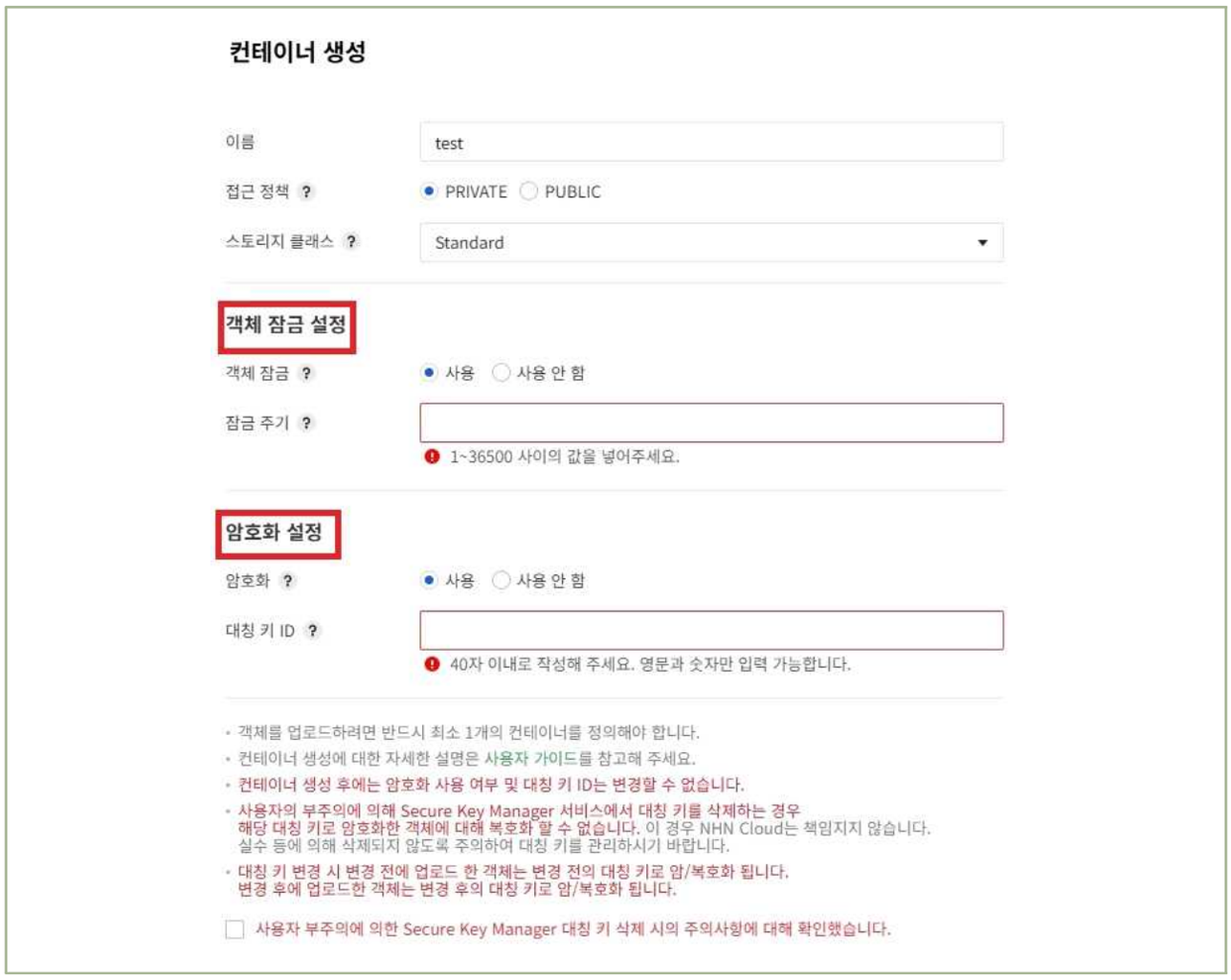
    1) 백업 파일 훼손에 대한 탐지 및 알람 설정
    2) 백업 기능(객체 잠금 등)을 통해 무결성 보장 등

3 우수 사례

- **(가상자원관리시스템)**

  ① 오브젝트 스토리지로 보관되는 백업 파일은 객체 잠금(Write Once Read Many, WORM) 주기를 일 단위로 설정하여 사용자의 부주의한 덮어쓰기, 삭제 요청으로부터 데이터를 보호하거나 암호화 기능을 통해 데이터를 보다 안전하게 관리할 수 있습니다. 단, 암호화는 권한이 없는 외부인이 내용을 확인하거나 변경하지 못하도록 할 수는 있으나 암호화 전 데이터가 위/변조되었는지 또는 암호문이 손상되었는지 등의 무결성을 보장하기는 어렵습니다.

  따라서 백업 파일의 무결성 보장을 위해서는 NHN Cloud의 마켓플레이스 솔루션이나 금융 기관 내에서 자체적으로 사용하는 백업 솔루션 등에서 제공하는 무결성 보장 기능 등을 활용하여 무결성 여부를 확인하도록 합니다.



| 그림 8-4-1 | Object Storage 잠금 및 암호화 적용

1 기준

식별번호	기준	내용
8.5.	**행위추적성 증적 및 전산자료 등 백업에 관한 기록 및 관리**	**백업 자료의 생성 변경 삭제 등 관련 내역을 기록하고 관리하여야 한다.**

2 설명

- 백업 자료의 생성, 변경, 삭제 관련 기록이 저장/관리되어야 한다.

  - 예시

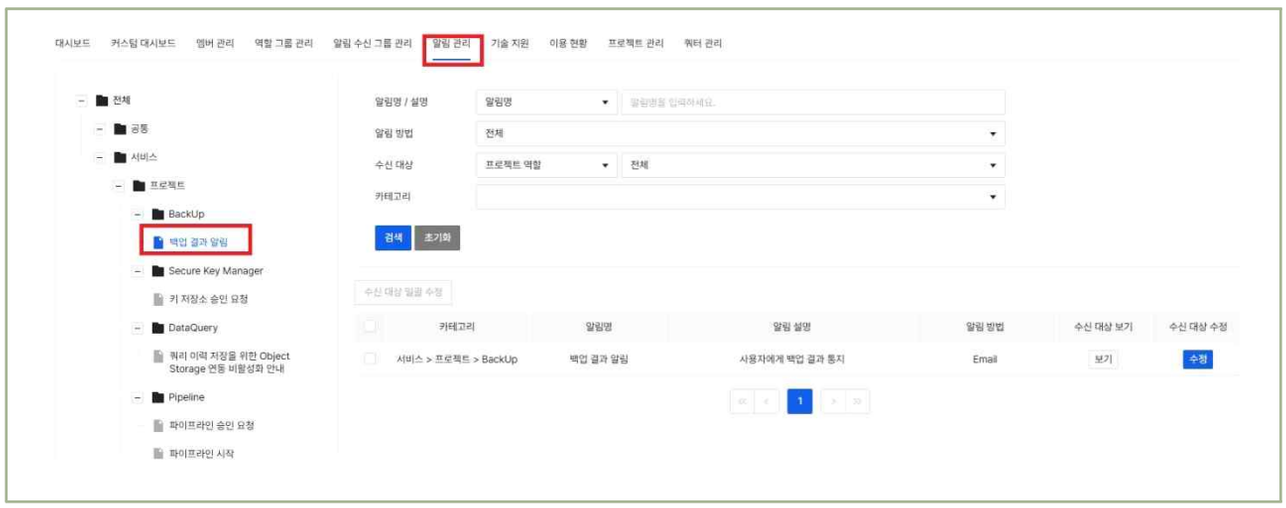
    1) 백업 작업 로그 저장

    2) 정상적인 백업 수행 여부에 대한 모니터링

3 우수 사례

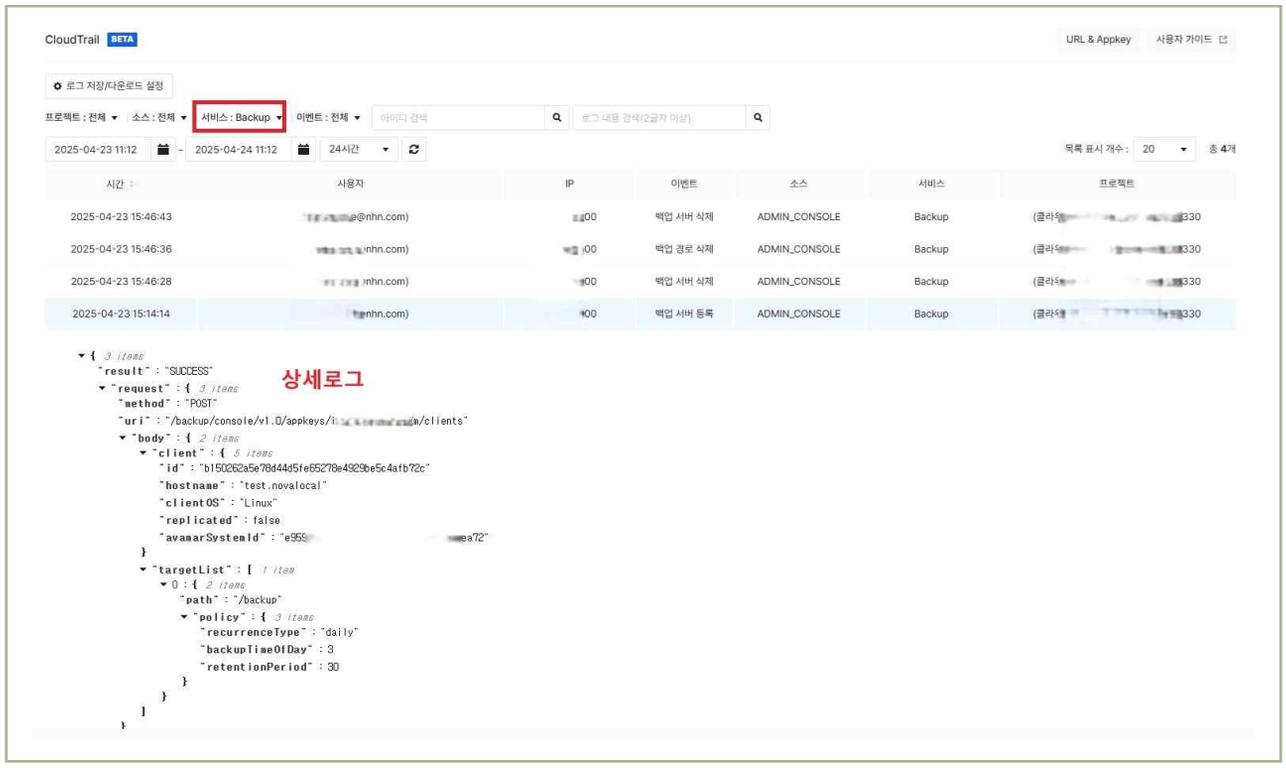
- **(가상자원관리시스템)**

  ① “[프로젝트 〉〉 알림 관리]” 메뉴 이동 후 백업 결과 알림 통지 설정을 통해 백업 결과를 모니터링할 수 있습니다. 설정된 이메일 주소로 백업 결과가 통지됩니다.



| 그림 8-5-1 | 백업 결과 알림 관리

② CloudTrail에서 제공하는 로그를 통해 Backup, Object Storage 등을 통해 일어나는 작업 이벤트 로그를 확인할 수 있습니다.



| 그림 8-5-2 | CloudTrail 서비스 로그

1 기준

식별번호	기준	내용
8.6.	**백업파일 원격 안전지역 보관**	**중요한 금융회사 전산자료는 보안이 강화된 원격 저장소에 보관하여야 한다.**

2 설명

- 중요 데이터는 원격 저장소에 안전하게 보관하여야 한다.

  - 예시

    1) 클라우드 서비스 제공자(CSP)의 DR 서비스 이용

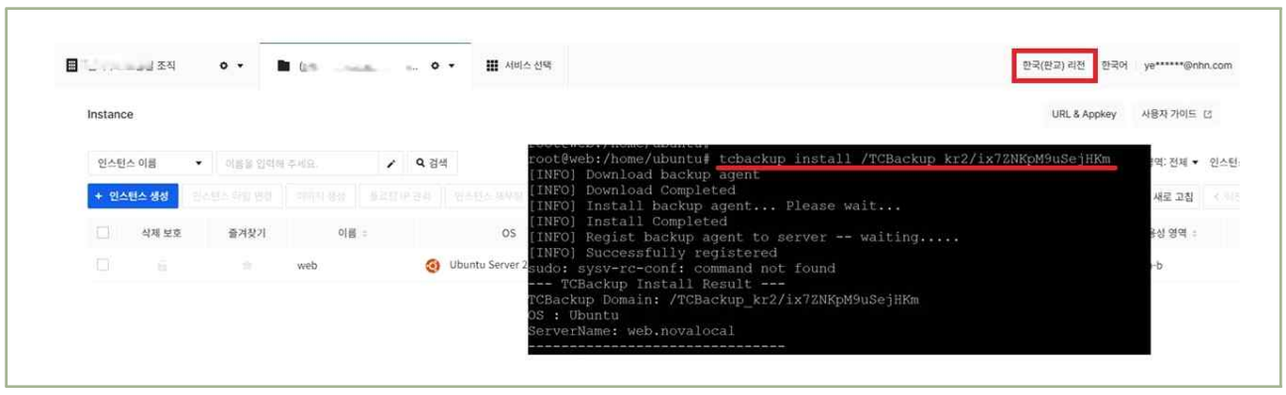
    2) 금융회사 자체 데이터센터로 소산하여 보관 등

3 우수 사례

- **(가상자원관리시스템)**

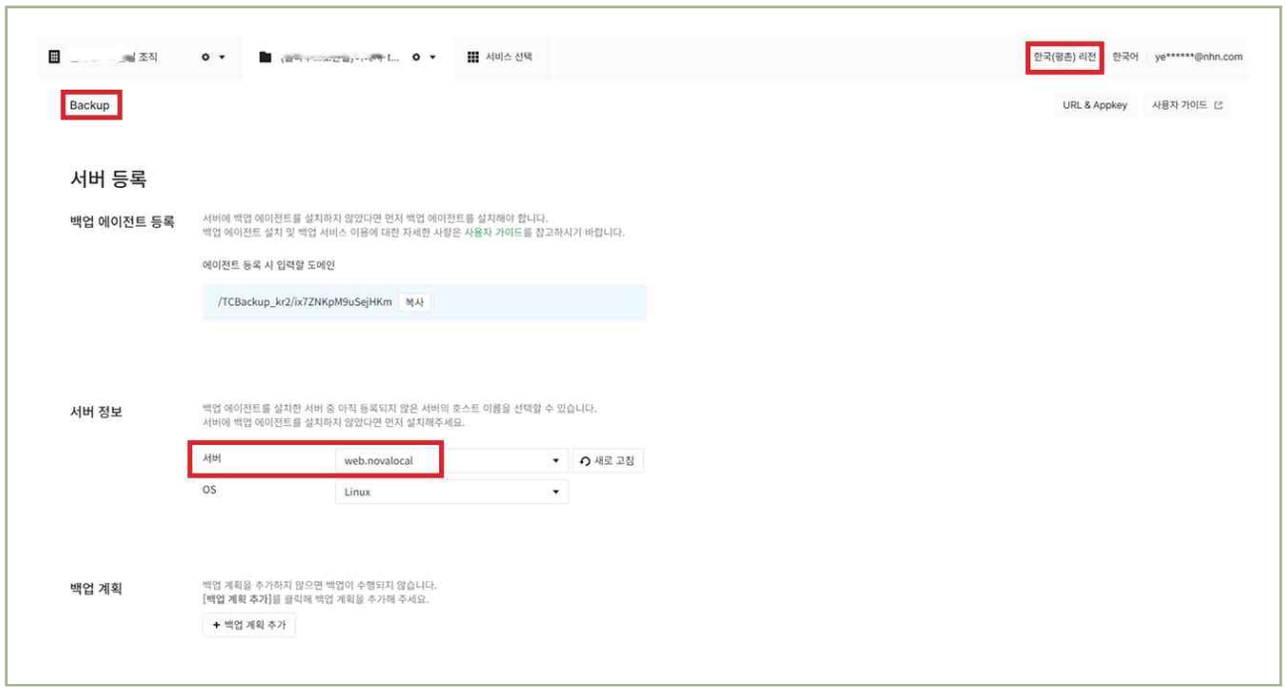
  ① NHN Cloud는 판교 리전과 평촌 리전은 상호 DR 센터 역할을 수행하고 있습니다. 이용자는 필요에 따라 리전 별로 서비스를 구성하여 트래픽을 분산시키거나 데이터 저장소를 분리 보관할 수 있습니다. 예를 들어 판교 리전의 인스턴스에 저장된 데이터를 평촌의 Backup 서비스로 데이터가 저장되도록 설정하여 데이터가 분산 보관 되도록 할 수 있습니다.

  A. 판교 리전의 인스턴스에 평촌 Backup 에이전트를 설치합니다.



| 그림 8-6-1 | 판교 리전 서버에 평촌 Backup 에이전트 설치

B. 평촌 리전의 Backup 서비스에서 백업 할 수 있도록 서버를 등록합니다.



| 그림 8-6-2 | 평촌 리전 Backup 서비스에 서버 등록

- NHN Cloud는 판교와 평촌 리전에서 IaaS, PaaS, SaaS 서비스를 제공하여 이용자가 서비스를 구축할 수 있도록 지원하는 것이며 이용자가 서비스를 구성하거나 데이터를 저장하기 위해서는 필요한 클라우드 서비스를 활성화하여 직접 구성해야 합니다.

1 기준

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

2 설명

- 인프라 구성 시 주요 전산장비를 이중화 하여 구성한다.

  - 예시

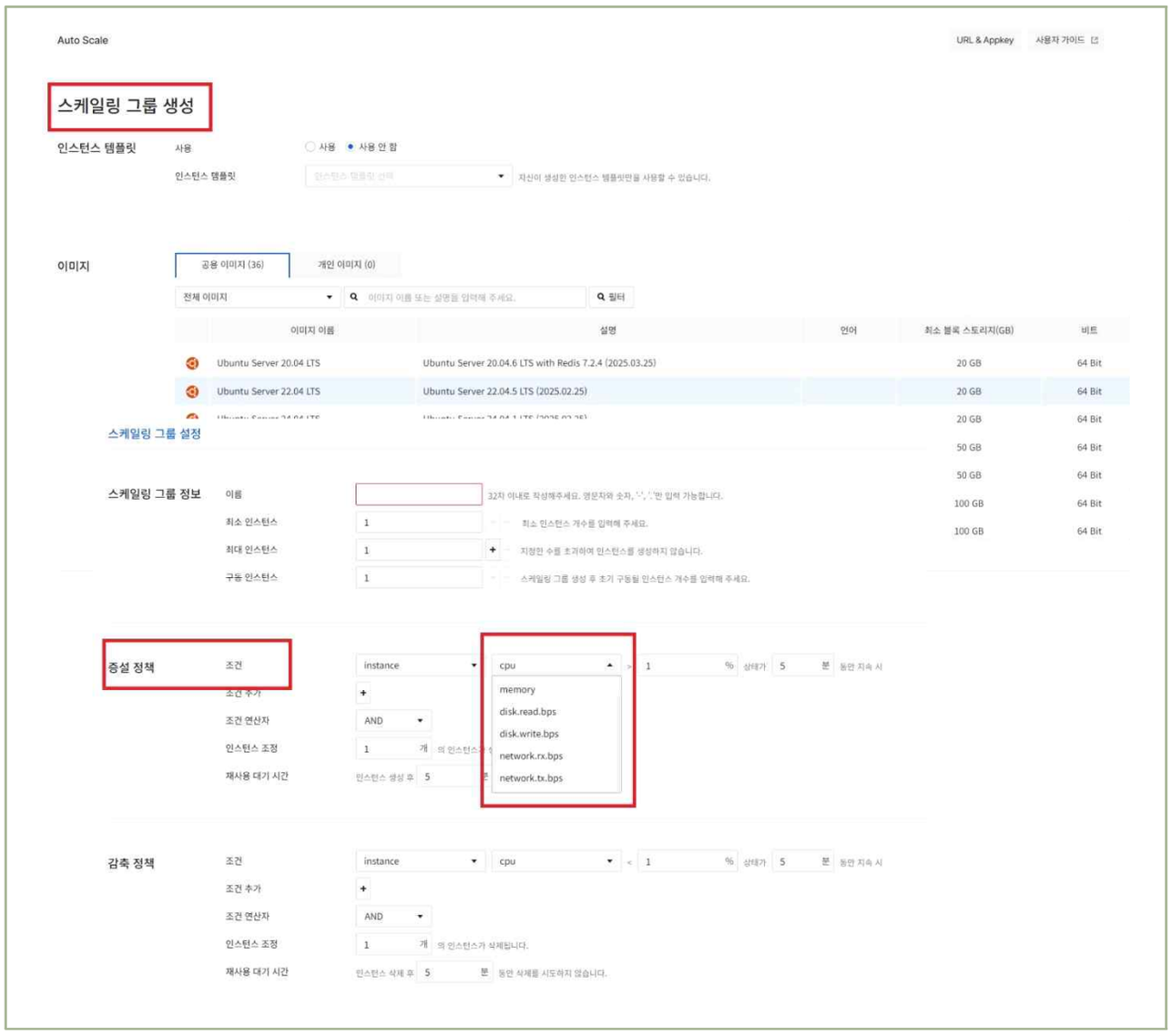
    1) 클라우드 가상화 기능을 이용하여 주요 전산장비 이중화 구성

    2) 이중화 구성 시 원격 안전지역 고려 등

3 우수 사례

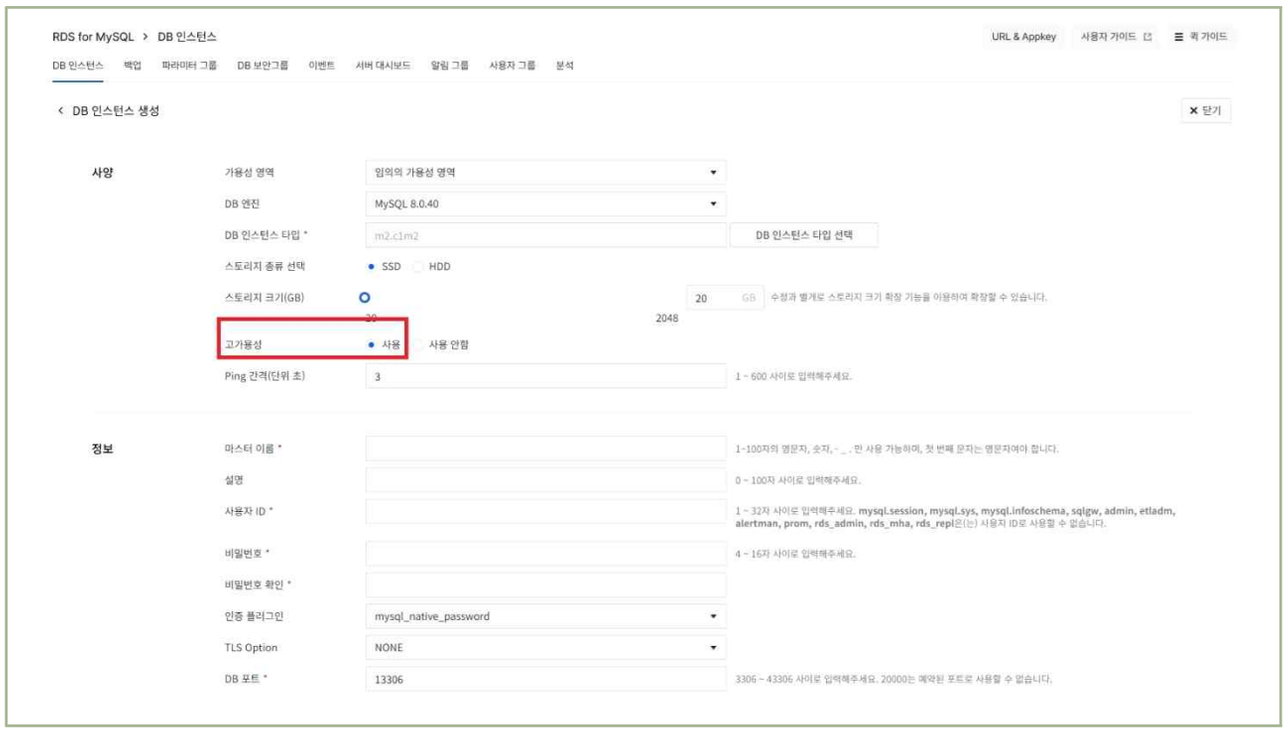
- **(가상자원관리시스템)**

  ① 오토스케일(Auto Scale) 서비스를 사용하면 인스턴스의 부하를 지속적으로 모니터링하여 필요한 경우 인스턴스를 추가로 생성하거나 삭제할 수 있습니다. 개별 인스턴스에 네트워크 단절 등의 장애가 발생하면 자동으로 새로운 인스턴스를 생성해 장애가 발생한 인스턴스를 대체할 수도 있습니다.



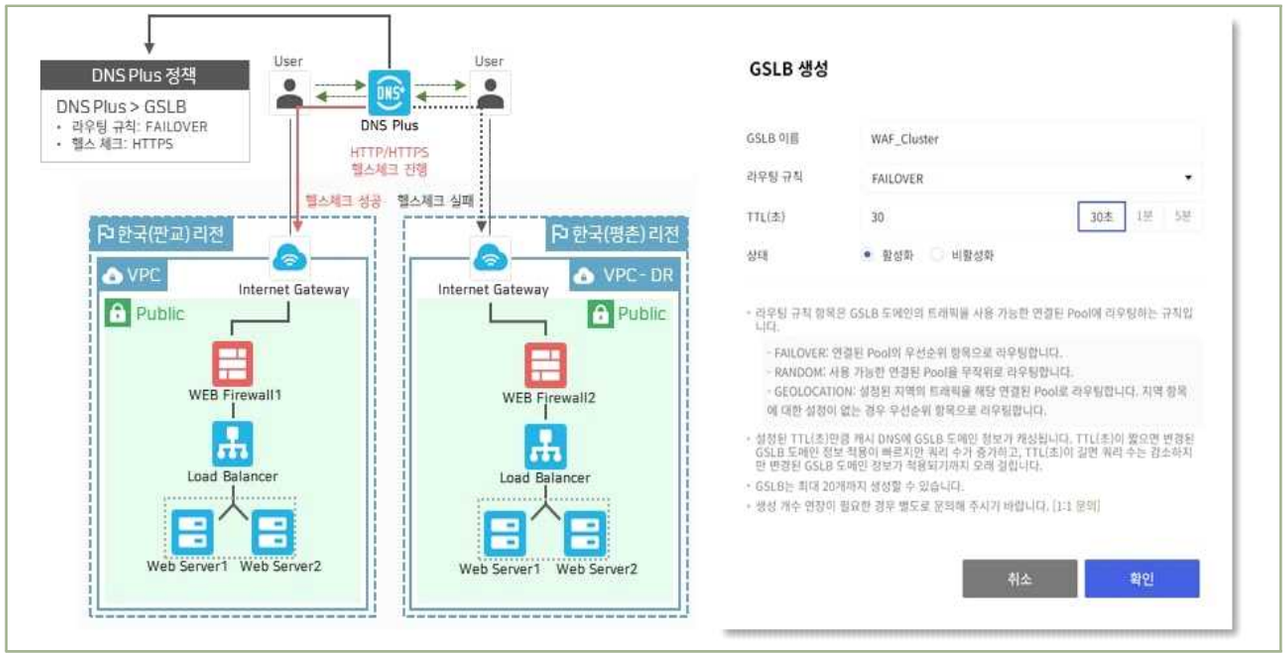
| 그림 8-7-1 | 오토스케일링 설정

② RDS 사용 시 고가용성 기능을 선택하여 마스터, 예비 마스터로 구성할 수 있습니다. 예비 마스터는 장애에 대비한 DB 인스턴스로 평소에는 사용할 수 없습니다. 고가용성 DB 인스턴스의 경우 예비 마스터에서 백업이 수행됩니다. 예비 마스터에는 장애를 감지하기 위한 프로세스가 존재하여 주기적으로 마스터의 상태를 감지합니다. 이러한 감지 주기를 Ping 간격이라고 하며 4회 연속 상태 체크에 실패할 경우 장애 조치를 수행합니다. Ping 간격이 짧을수록 장애에 민감하게 반응하며, Ping 간격이 길수록 장애에 둔감하게 반응합니다. 서비스 부하에 맞게 적절한 Ping 간격을 설정하는 것이 중요합니다.



| 그림 8-7-2 | RDS 고가용성 설정

③ 지리적으로 떨어진 판교, 평촌 리전에 이용자의 서비스를 복수 배치하여 고가용성 구성을 할 수 있습니다. 예를 들어 그림과 같이 DNS Plus의 GSLB 라우팅 규칙을 Fail over로 설정하고 WEB Firewall1이 정상일 경우는 웹 트래픽이 WEB Firewall1로 전달되고 WEB Firewall1 장애 또는 리전 장애가 발생하여 헬스 체크가 실패하면 WEB Firewall2로 트래픽이 전달 되도록 구성할 수 있습니다.



| 그림 8-7-3 | DNS Plus를 활용한 이중화 구성 예시

금융분야 상용 클라우드컴퓨팅서비스 보안 안내서 (NHN Cloud)

발 행 일	2026년 8월
발 행 인	금융보안원(원장 박상원)
공 동 발 행 인	NHN Cloud

금 융 보 안 원		NHN Cloud	
클라우드평가부	부장 유재필	**보안아키텍트팀**	책임 김덕찬
클라우드기획팀	팀장 장지현		수석 이예지
	차장 안성현		
	대리 최주섭		

발 행 처	금융보안원
	02-3495-9000
	경기도 용인시 수지구 대지로 132

〈비 매 품〉

금융분야
상용 클라우드컴퓨팅서비스
보안 안내서