업무참고 2025-클라우드대응-②-60

금융분야
상용 클라우드컴퓨팅서비스 보안 관리 참고서

NAVER Cloud

금융보안원
FINANCIAL SECURITY INSTITUTE

NAVER Cloud

CONTENTS

1. 가상자원 관리

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

1 가상자원 관리

1 기준

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

2 설명

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

  - 예시

    1) 비밀번호는 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설정

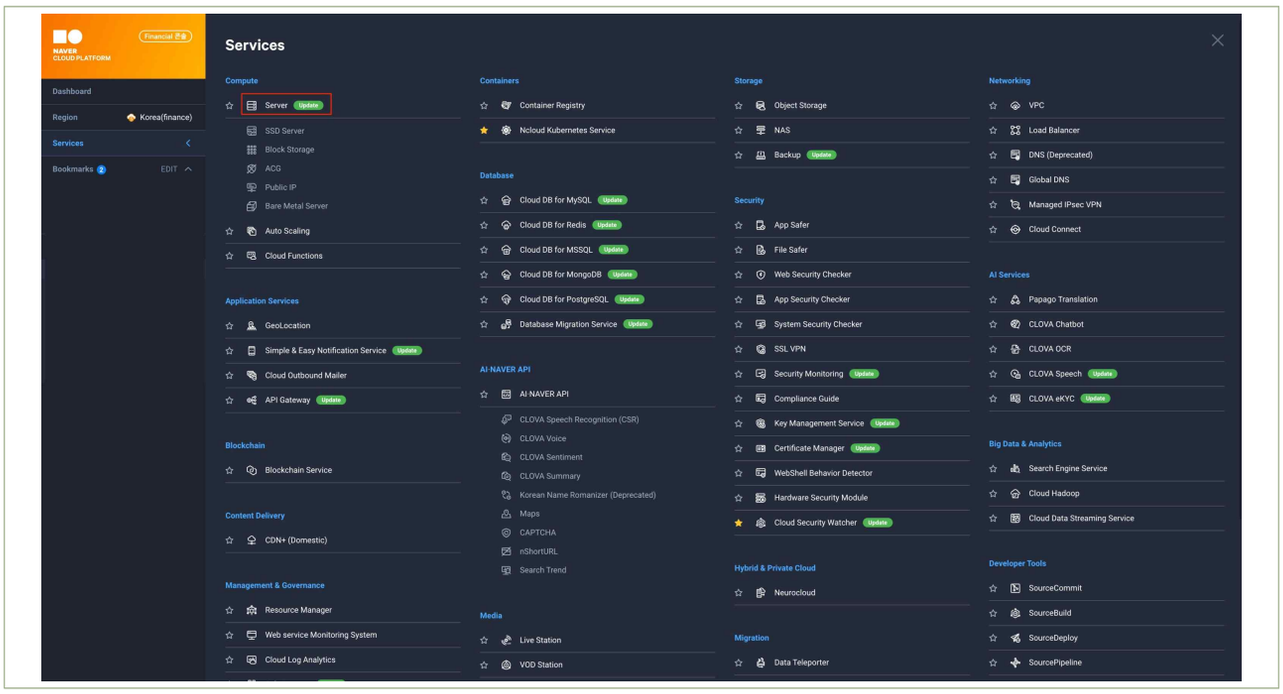
    2) 주요 가상자원의 인증키는 별도의 인증키로 설정 등

3 우수 사례

- 네이버 클라우드 플랫폼은 사용자가 가상자원(Server, Cloud DB) 생성 시 안전한 비밀번호 규칙을 준수할 수 있도록 전자금융감독규정에 따른 비밀번호 규칙이 적용되어 있습니다. 사용자는 네이버 클라우드 플랫폼의 안전한 비밀번호 규칙에 따라 Cloud DB의 비밀번호를 직접 입력하여야 합니다. 가상자원(Server)의 경우에는 관리자 계정의 비밀번호를 확인할 때 필요한 인증키를 설정하고, 해당 인증키를 통해서만 비밀번호 확인이 가능합니다. 해당 관리자 계정의 비밀번호는 안전한 비밀번호 규칙에 따라 제3자가 쉽게 유추할 수 없도록 가상자원(Server)별 비밀번호가 자동 생성됩니다.

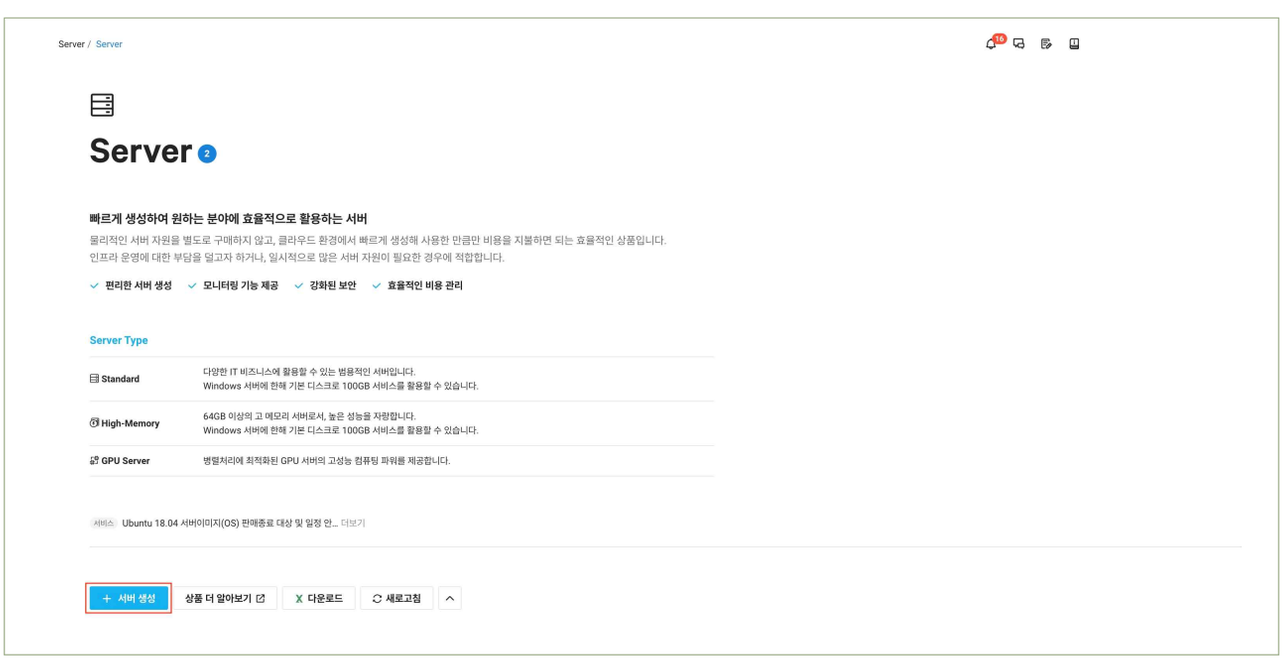
Server의 안전한 비밀번호 설정

① **(가상자원관리시스템)** ‘Services’ → ‘Server’ 상품을 선택합니다.



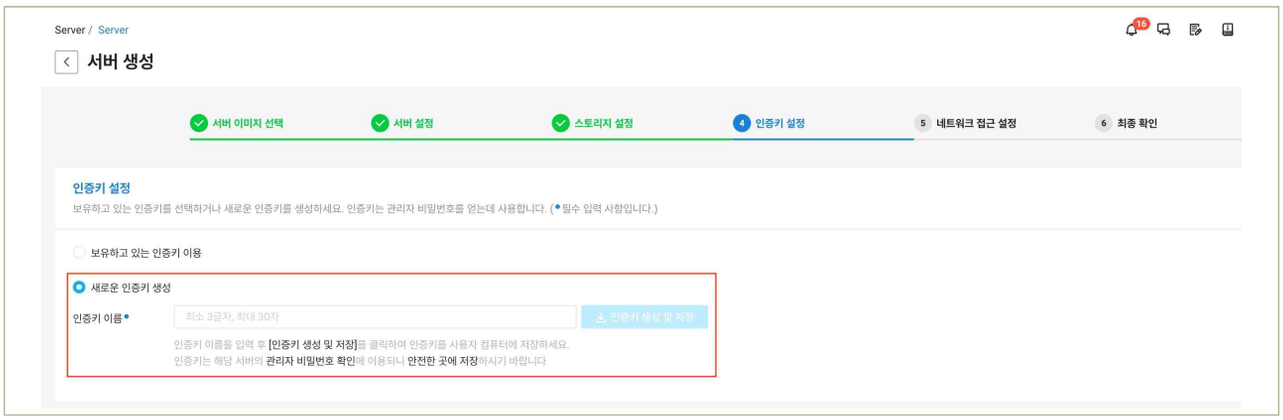
| 그림 1-1-1 | Server 상품 선택

② **(가상자원관리시스템)** ‘Server’ → ‘+ 서버 생성’을 클릭하여 가상자원(Server)를 생성합니다.



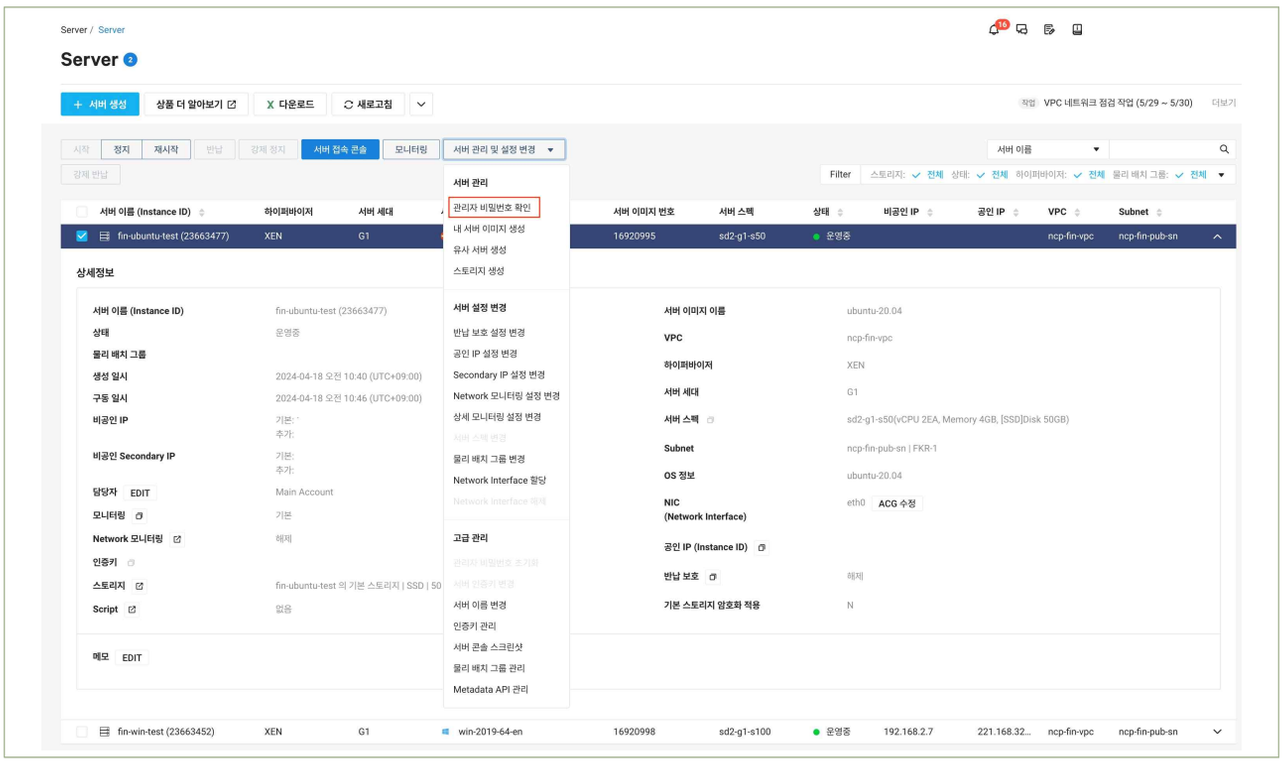
| 그림 1-1-2 | Server 생성

③ **(가상자원관리시스템)** Server 생성 단계 중, 인증키 설정단계에서 '인증키 이름' 텍스트 박스에 가상자원(Server)의 비밀번호 확인을 위한 인증키를 정의하고, 해당 인증키는 안전한 곳에 저장합니다.



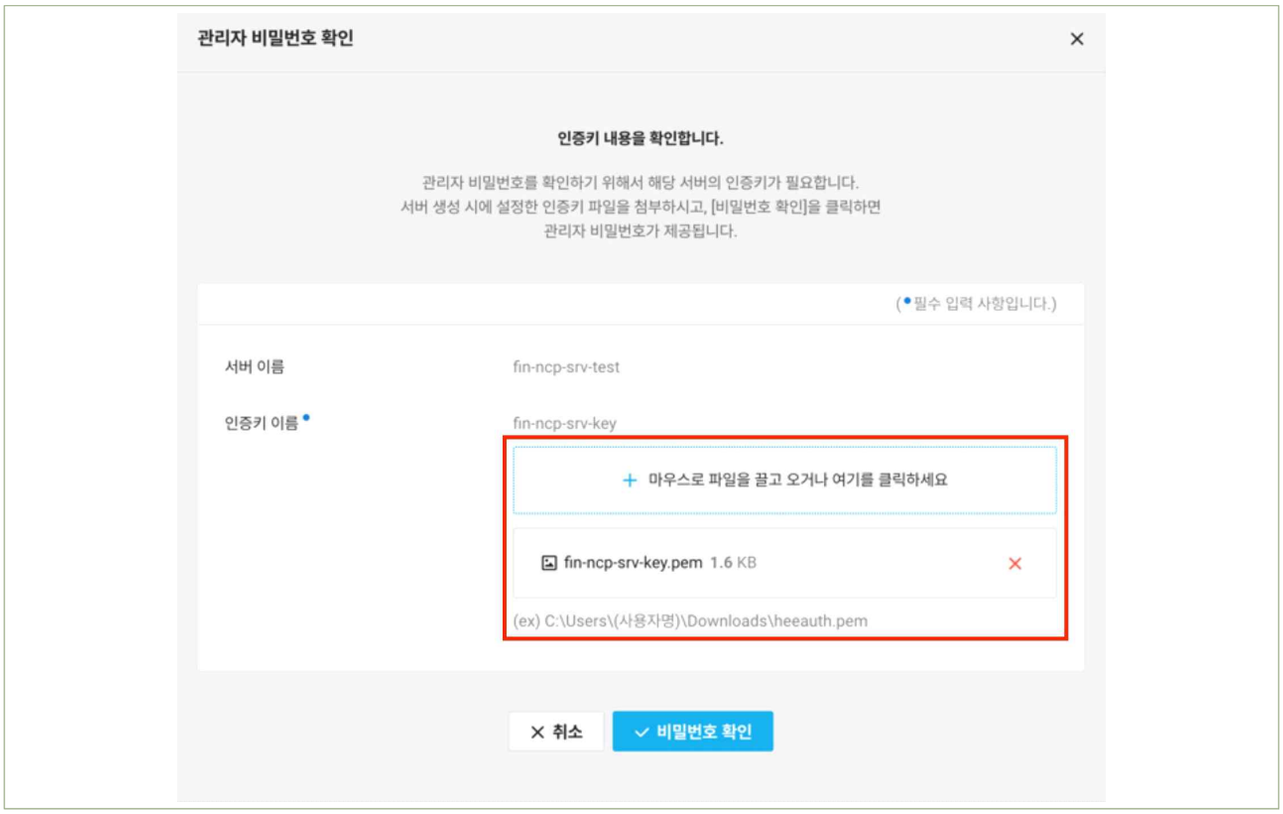
| 그림 1-1-3 | Server 인증키 정의 및 저장

④ **(가상자원관리시스템)** 가상자원(Server)의 비밀번호 확인을 위해, 'Server' → '서버 관리 및 설정 변경' → '관리자 비밀번호 확인'을 클릭합니다.



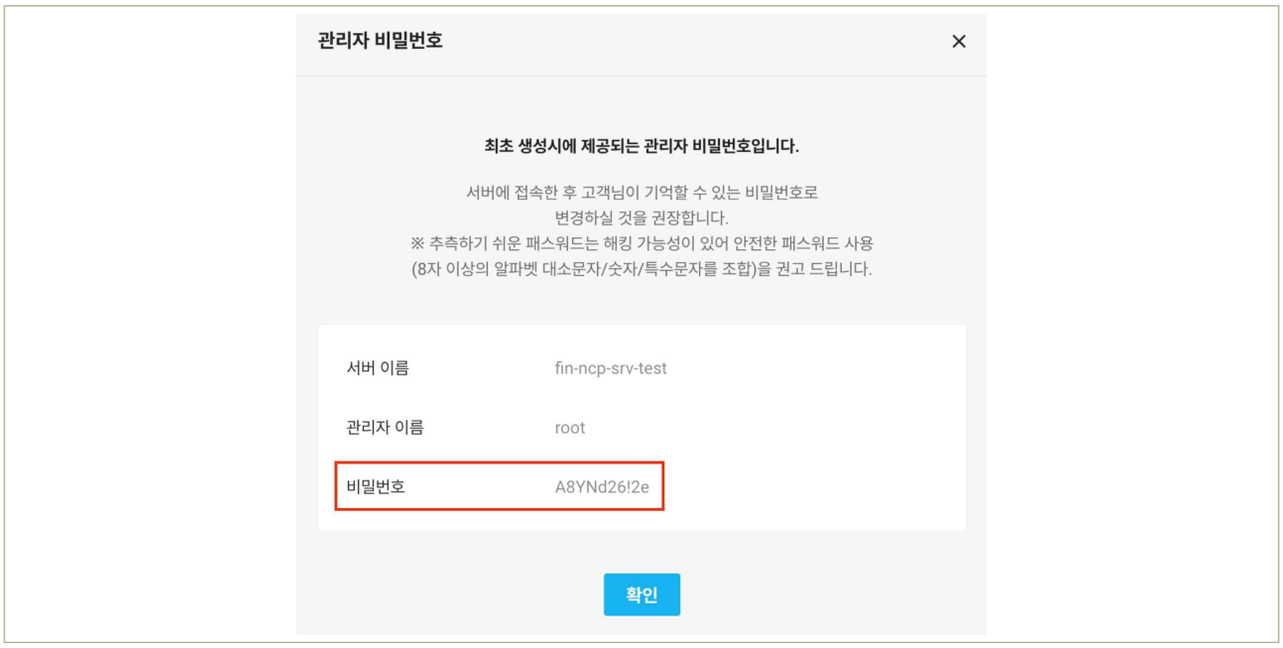
| 그림 1-1-4 | Server 관리자 비밀번호 확인

⑤ **(가상자원관리시스템)** 해당 가상자원(Server)의 인증키를 불러옵니다.



| 그림 1-1-5 | Server의 인증키 검증

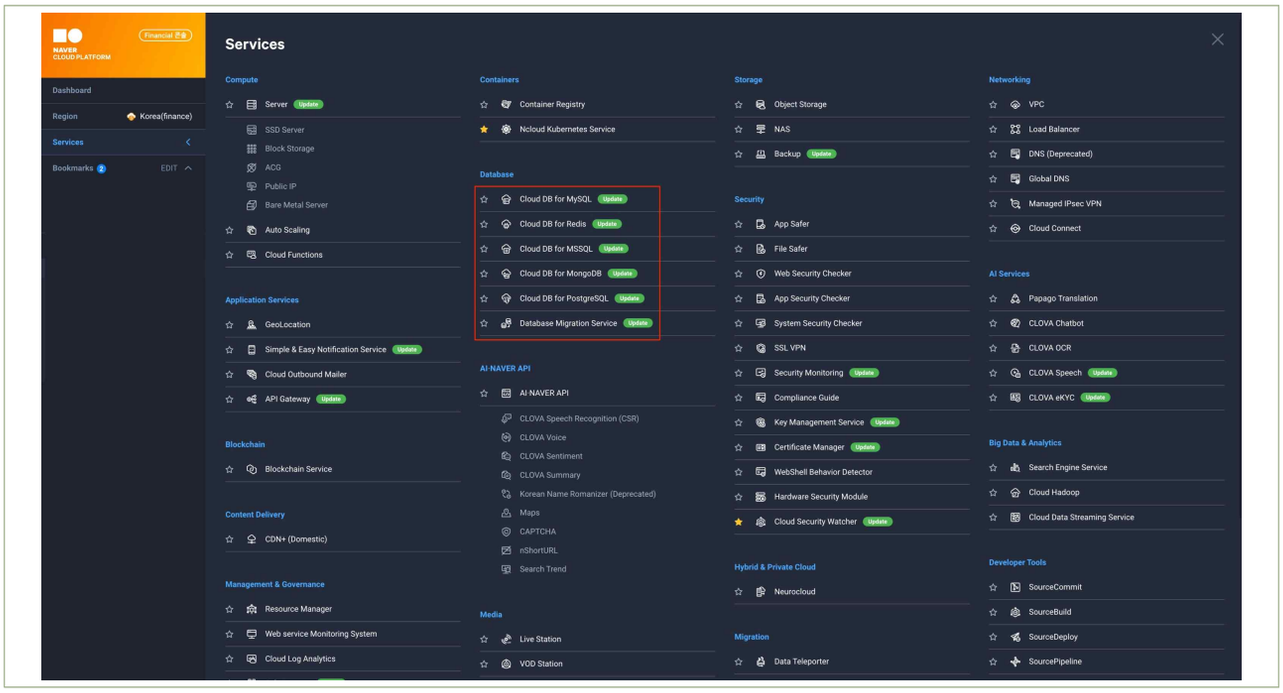
⑥ **(가상자원관리시스템)** 해당 가상자원(Server)의 관리자 비밀번호를 확인합니다.



| 그림 1-1-6 | Server의 관리자 비밀번호 확인 예시

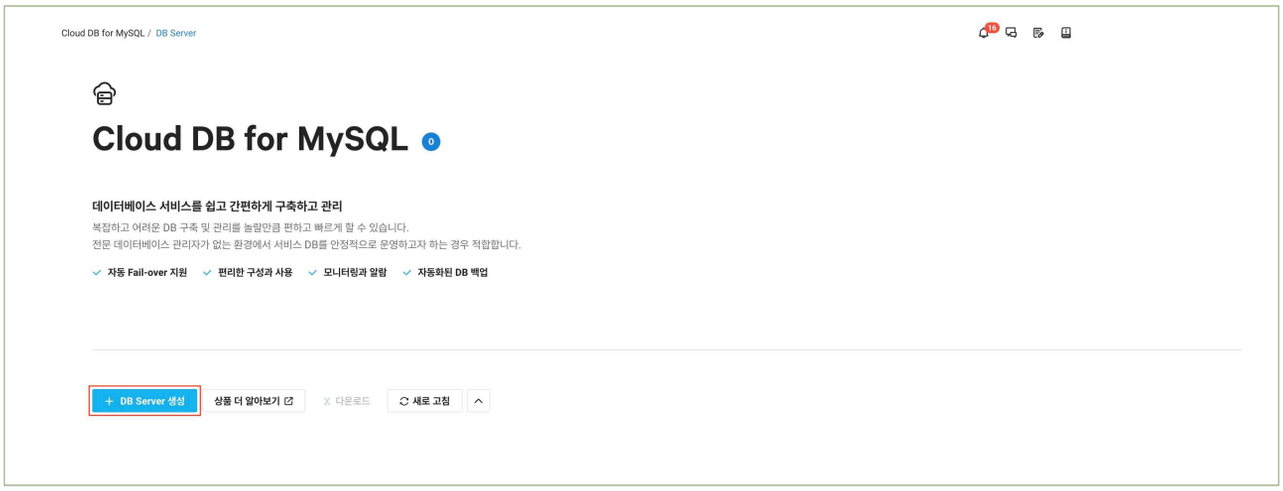
Cloud DB의 안전한 비밀번호 설정

① **(가상자원관리시스템)** ‘Services’ → ‘Cloud DB’ 상품을 선택합니다.



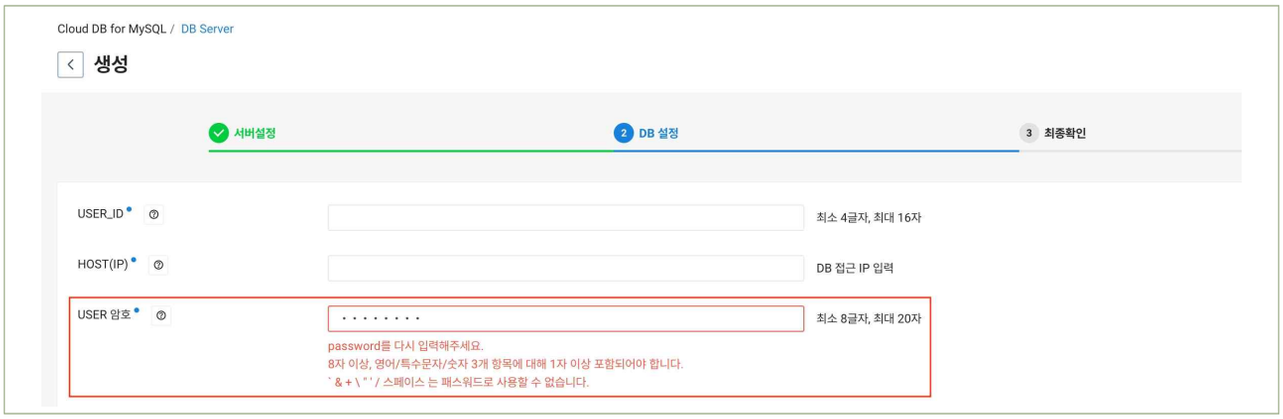
| 그림 1-1-7 | Cloud DB 상품 선택

② **(가상자원관리시스템)** ‘DB Server’ → ‘+DB Server 생성’을 클릭하여 가상자원(Cloud DB)을 생성합니다.



| 그림 1-1-8 | Cloud DB 신규 생성

③ **(가상자원관리시스템)** Cloud DB 생성 단계 중, DB 설정단계에서 'USER 암호' 텍스트 박스에 네이버 클라우드 플랫폼의 안전한 비밀번호 규칙에 따라 비밀번호를 정의합니다.



| 그림 1-1-9 | Cloud DB 계정의 비밀번호 규칙

API를 통한 가상자원(Server)의 안전한 비밀번호 설정

① **(API(CLI))** 'createLonginKey' API를 통해 인증키를 생성하고, 해당 인증키를 사용하여 가상자원(Server)을 생성합니다.

- 요청 예시

```
GET https://fin-ncloud.apigw.fin-ntruss.com/vserver/v2/createLoginKey?keyName=test-***
```

| 그림 1-1-10 | API를 통한 Server 인증키 생성

- 요청 예시

```
GET https://fin-ncloud.apigw.fin-ntruss.com/vserver/v2/createServerInstances
?regionCode=FKR
&serverImageProductCode=SW.VSVR.OS.LNX64.CNTOS.0703.B050
&vpcNo=***04
&subnetNo=***43
&serverProductCode=SVR.VSVR.STAND.C002.M004.NET.SSD.B050.G001
&feeSystemTypeCode=MTRAT
&serverCreateCount=1
&serverName=test-***
&networkInterfaceList.1.networkInterfaceOrder=0
&networkInterfaceList.1.accessControlGroupNoList.1=***63
&placementGroupNo=***61
&isProtectServerTermination=false
&initScriptNo=***44
&loginKeyName=test-***
&associateWithPublicIp=true
```

| 그림 1-1-11 | 인증키를 통한 Server 생성

② **(API(CLI))** 'getRootPassword' API를 통해 다음과 같이 가상자원(Server)의 관리자 비밀번호를 확인합니다.

- 요청 예시

```
GET https://fin-ncloud.apigw.fin-ntruss.com/vserver/v2/getRootPassword
?regionCode=FKR
&serverInstanceNo=***4299
&privateKey=-----BEGIN RSA PRIVATE
KEY-----\nMIIEpAIBAAKCAQEAzbhX0SkB+N3yAe799tP1xuYEL23uaZhqnKSup0IGOICea***\nQC/
~~~ 중 략 ~~~
xAjxtdWWUcieLv2W***\nQVy9ggBROA6vB1r4qtlMJI8AYymztJreCiOI7hBaFqezYdQHughrPA==\n-----END
RSA PRIVATE KEY-----\n
```

- 응답 예시

```
<getRootPasswordResponse>
  <requestId></requestId>
  <returnCode>0</returnCode>
  <returnMessage>success</returnMessage>
  <rootPassword>P3e7fLnd6=***</rootPassword>
</getRootPasswordResponse>
```

| 그림 1-1-12 | 인증키를 통한 Server 관리자 비밀번호 확인 예시

API를 통한 가상자원(Cloud DB)의 안전한 비밀번호 설정

① **(API(CLI))** 'createCloudMysqlInstance' API를 통해 가상자원(Cloud DB) 생성 시, 'cloudMysqlUserPassword' 파라미터를 이용하여 가상자원(Cloud DB)에 대한 안전한 비밀번호를 설정합니다. 이때, 안전하지 않은 비밀번호를 작성하는 경우에는 요청이 실패됩니다.

- 요청 예시

```
GET https://fin-ncloud.apigw.fin-ntruss.com/vmysql/v2/createCloudMysqlInstance
?regionCode=FKR
&vpcNo=****83
&cloudMysqlImageProductCode=SW.VDBAS.DBAAS.LNX64.CNTOS.0708.MYSQL.8025.B050
&cloudMysqlProductCode=SVR.VDBAS.STAND.C002.M008.NET.HDD.B050.G002
&dataStorageTypeCode=SSD
&isHa=true
&isMultiZone=true
&isStorageEncryption=true
&isBackup=true
&backupFileRetentionPeriod=10
&backupTime=02:00
&isAutomaticBackup=false
&cloudMysqlServiceName=test-****
&cloudMysqlServerNamePrefix=test-****
&cloudMysqlUserName=test-****
&cloudMysqlUserPassword=********
&hostIp=192.168.0.%
&cloudMysqlPort=13306
&cloudMysqlDatabaseName=test-****
&subnetNo=****91
&standbyMasterSubnetNo=****93
```

| 그림 1-1-13 | Cloud DB 생성 시 안전한 비밀번호 규칙 적용

4 참고 사항

- [참고1] Server 생성 시 인증키 설정 가이드
- [참고2] Cloud DB 생성 시 DB 설정 가이드
- [참고3] Server 인증키 생성 API 가이드
- [참고4] Server 관리자 비밀번호 호출 API 가이드
- [참고5] Cloud DB 생성 API 가이드

1 기준

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

2 설명

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

  - 예시

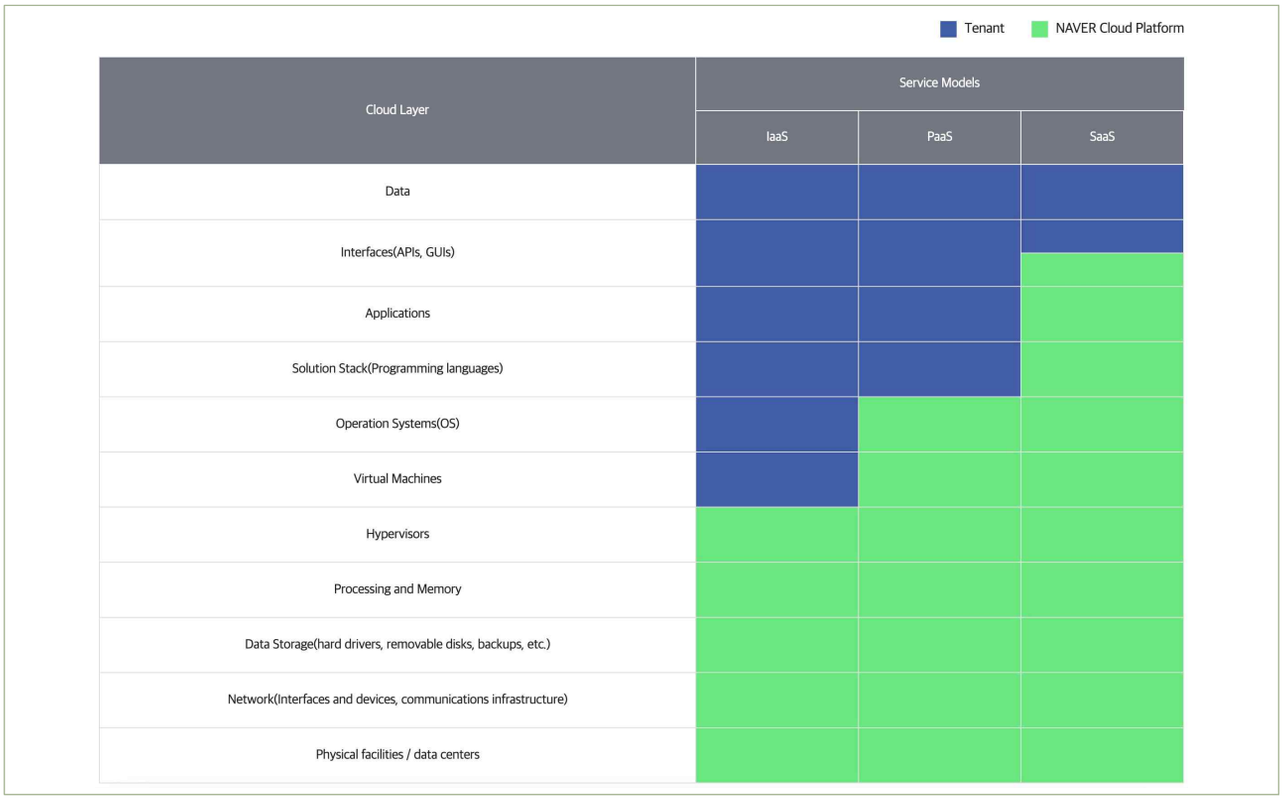
    1) OS 점검을 통한 비밀번호 임계값 설정 적용

3 우수 사례

- 네이버 클라우드 플랫폼은 클라우드 공동 책임에 따라서 사용자의 가상자원과 같은 클라우드 리소스를 안전하게 관리합니다.

  클라우드 공동 책임이란, 클라우드에 구성한 사용자의 가상자원을 안전하게 보호할 수 있도록 클라우드 서비스 제공자와 사용자가 각각 역할을 나누어 함께 책임을 다는 것을 말합니다.

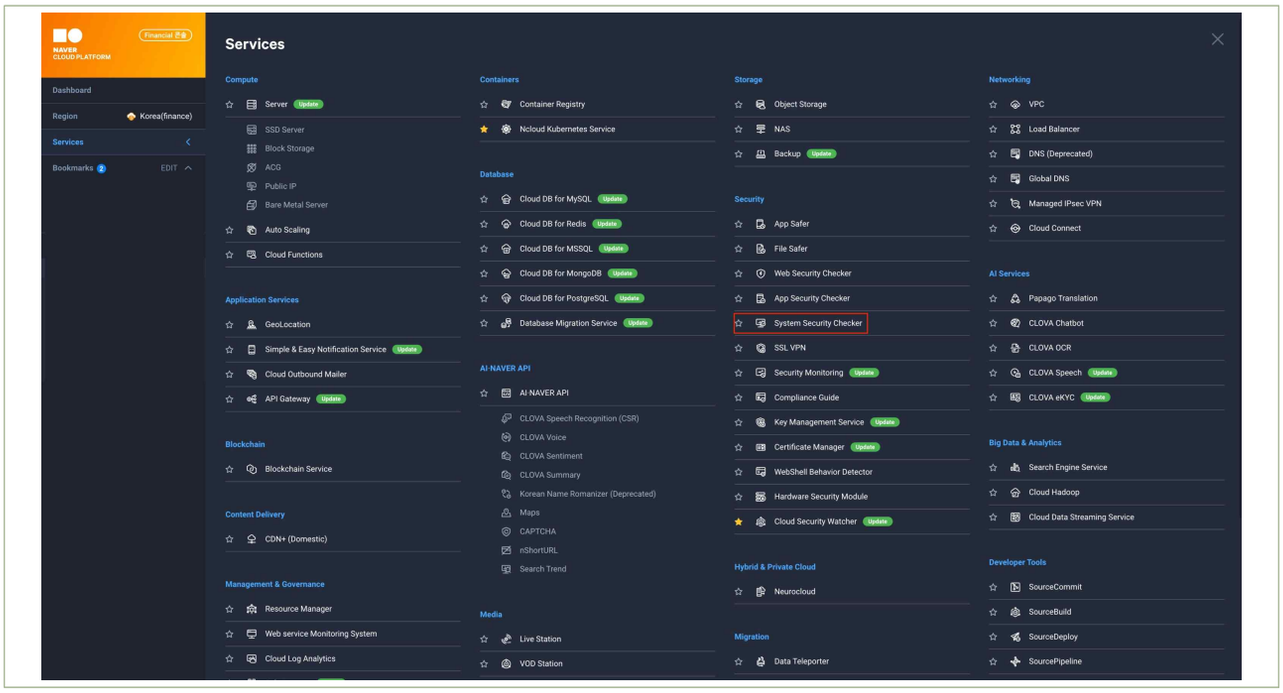
  이와 같은 클라우드 공동 책임에 따라 사용자는 IaaS(Infrastructure as a Service) 가상자원의 OS영역에 대한 무작위 대입 공격을 예방하기 위한 보안설정 적용 및 관리가 필요하며, Server의 OS에 대한 보안 설정을 점검하는 System Security Checker 상품의 OS Security Checker를 이용하여 OS 비밀번호 입력 오류에 대한 임계값 설정 여부를 검사하고 적용 방법에 대해 가이드 받을 수 있습니다.



| 그림 1-2-1 | 네이버 클라우드 플랫폼의 클라우드 공동 책임

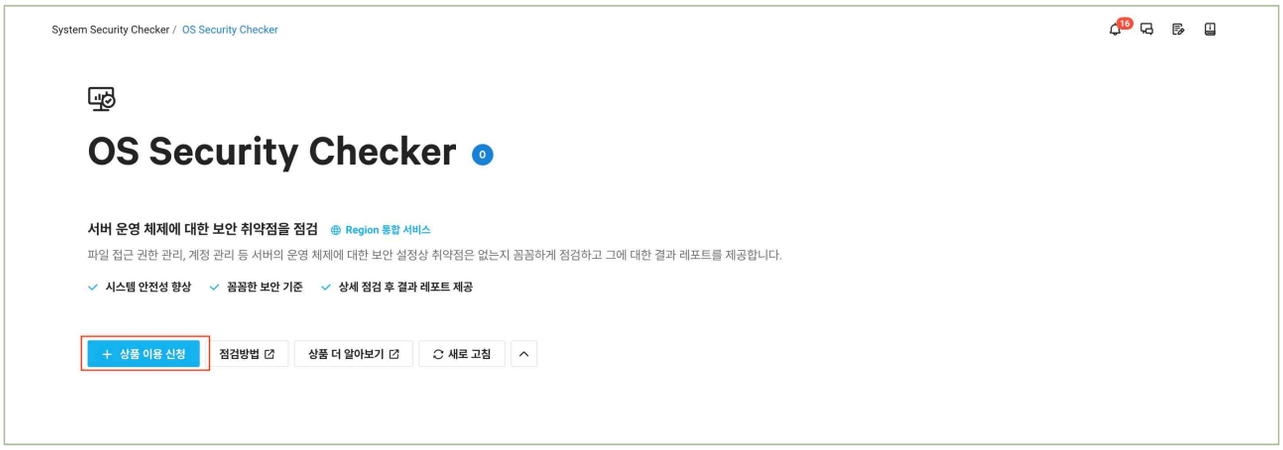
System Security Checker를 통한 비밀번호 임계값 설정 검사 및 조치

① **(가상자원관리시스템)** 'Services' → 'System Security Checker' 상품을 선택합니다.



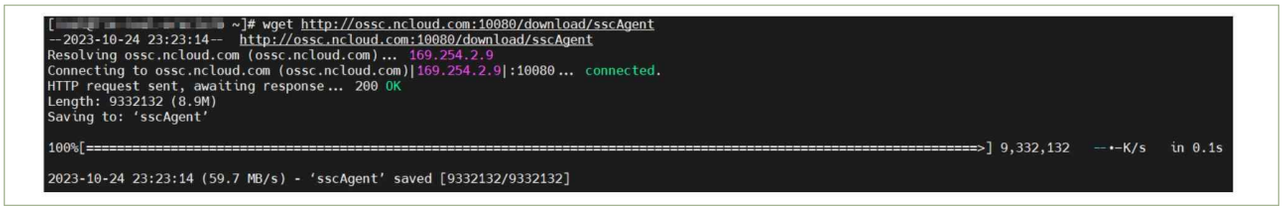
| 그림 1-2-2 | System Security Checker 상품 선택

② **(가상자원관리시스템)** ‘OS Security Checker’ → ‘+ 상품이용 신청’을 클릭하여 상품을 활성화 합니다.



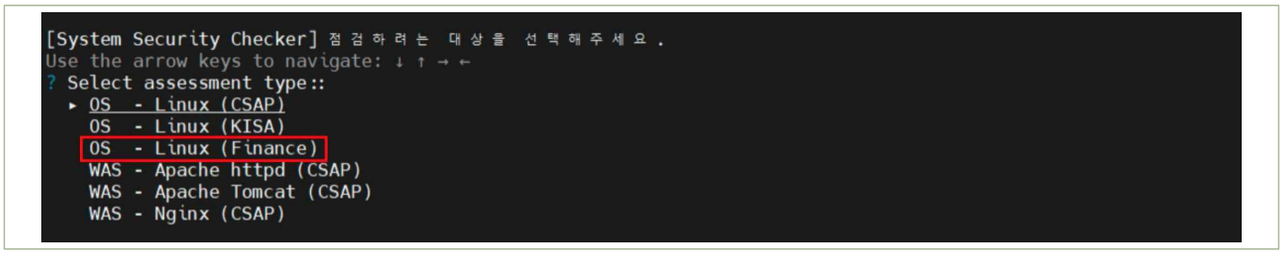
| 그림 1-2-3 | OS Security Checker 사용 신청

③ **(가상자원)** 가상자원(Server) 내에서 wget 명령어를 통해 sscAgent를 다운로드 합니다.



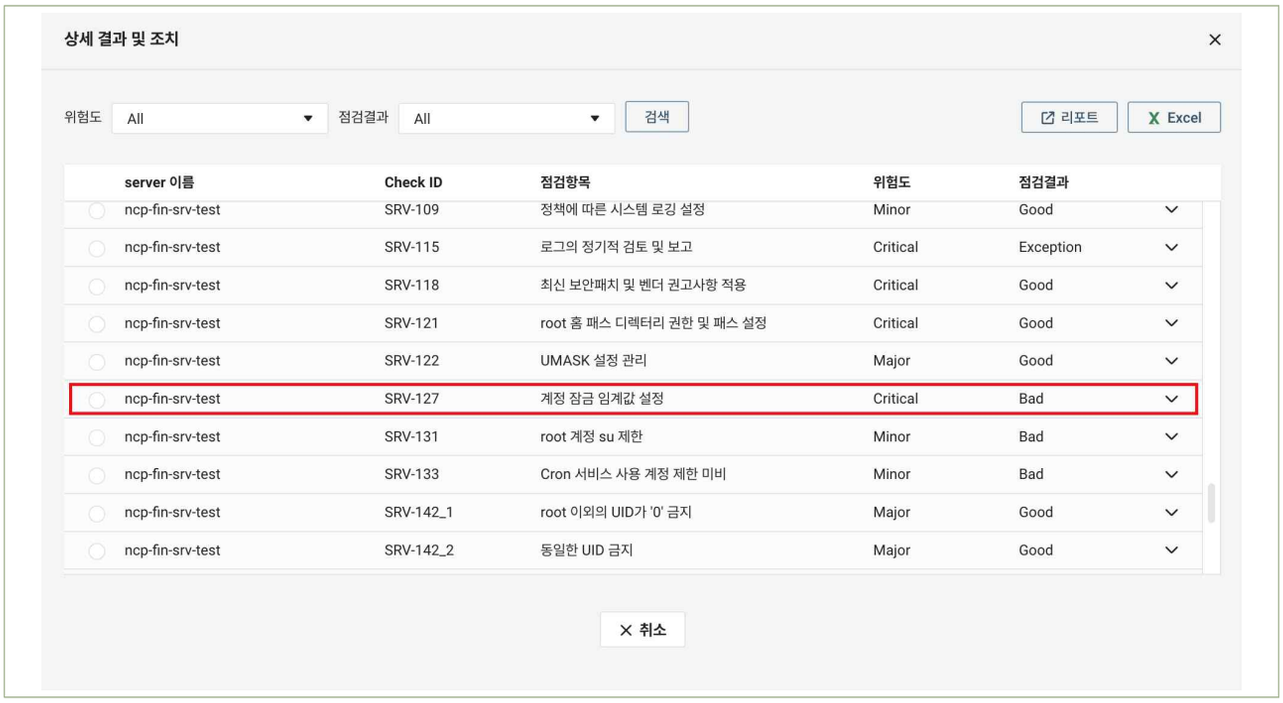
| 그림 1-2-4 | System Security Checker Agent 다운로드

④ **(가상자원)** sscAgent를 실행하여 비밀번호 임계값 설정 여부를 점검합니다.



| 그림 1-2-5 | System Security Checker를 통한 비밀번호 임계값 검사

⑤ **(가상자원관리시스템)** sscAgent를 통해 점검된 결과를 확인하고, 가이드에 따라 비밀번호 임계값을 적용합니다.



| 그림 1-2-6 | System Security Checker를 통한 비밀번호 임계값 검사 결과

4 참고 사항

- [참고1] System Security Checker 점검 항목 (금융보안원 전자금융기반시설 기준)
- [참고2] System Security Checker Agent 실행 가이드
- [참고3] 네이버 클라우드 플랫폼 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

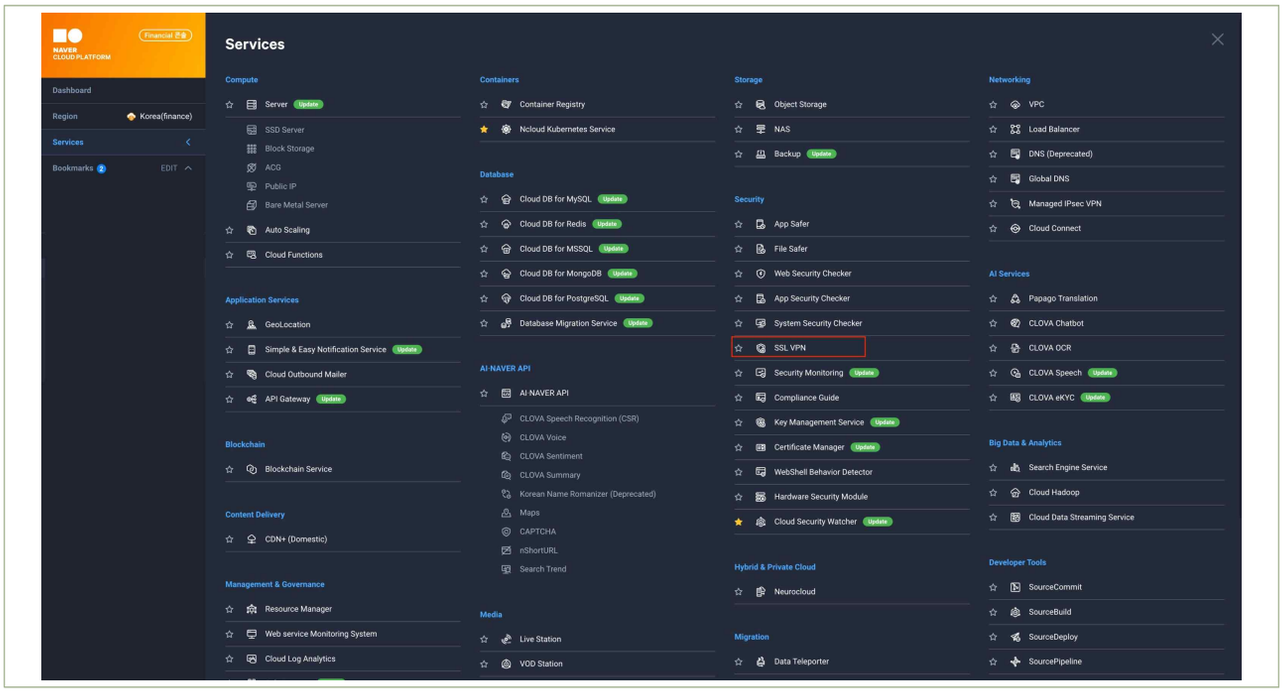
    1) 이메일 인증
    2) SMS 인증
    3) 별도 인증도구 활용 등

3 우수 사례

- 네이버 클라우드 플랫폼은 사용자의 안전한 가상자원(Server) 접근을 위해 SSL VPN 보안상품의 사용을 권장하고 있습니다. SSL VPN 상품은 로그인 단계에서 사용자의 ID/Password 인증 외에도 SMS, Email 인증과 같은 추가 인증 수단을 통해 인증이 적용되어 있어 사용자는 가상자원(Server)에 안전한 인증 절차를 통해 접근하도록 구성할 수 있습니다.

가상자원 루트 계정 접근 시 추가인증 수단 확보

① **(가상자원관리시스템)** ‘Services’ → ‘SSL VPN’ 상품을 선택합니다.

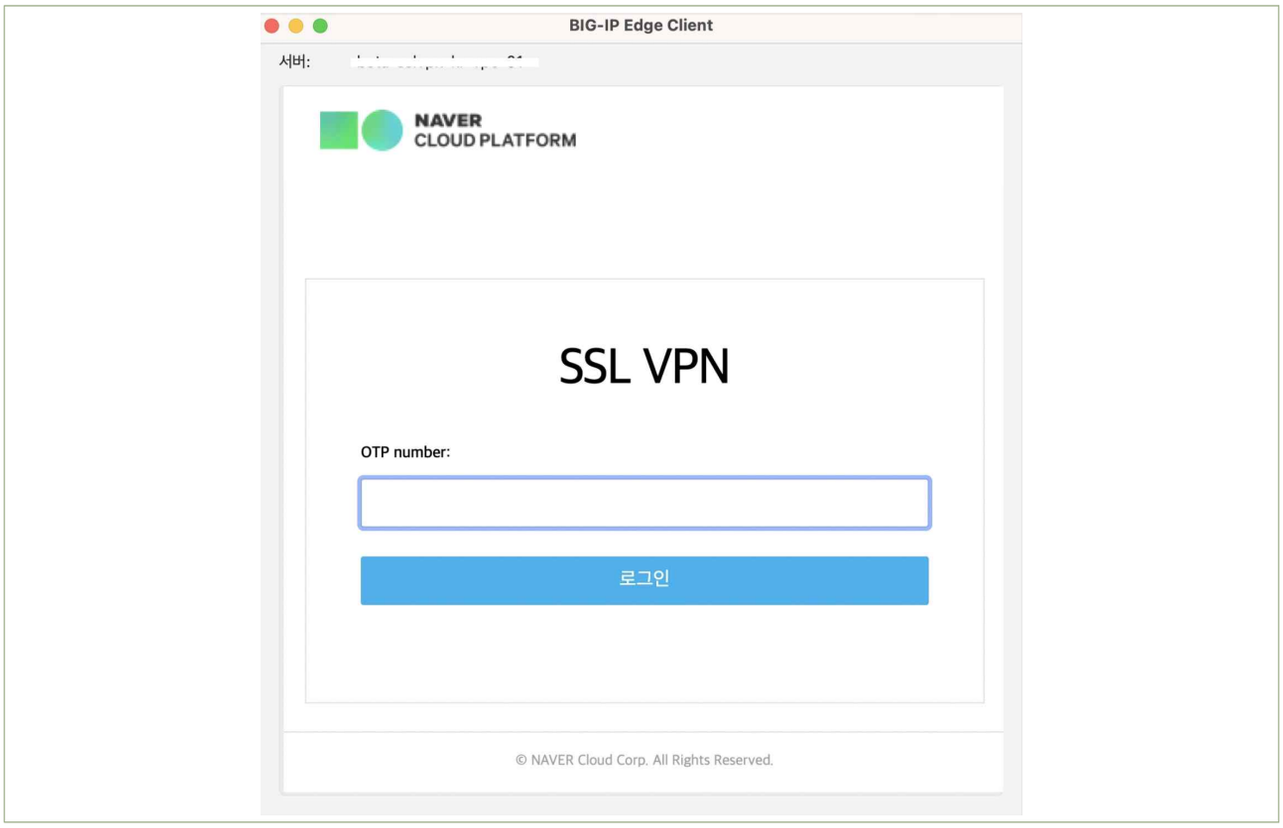


| 그림 1-3-1 | SSL VPN 상품 선택

② **(가상자원관리시스템)** ‘+ SSL VPN 생성’ 버튼을 클릭하여 SSL VPN 상품을 활성화 합니다.

| 그림 1-3-2 | SSL VPN 상품 활성화

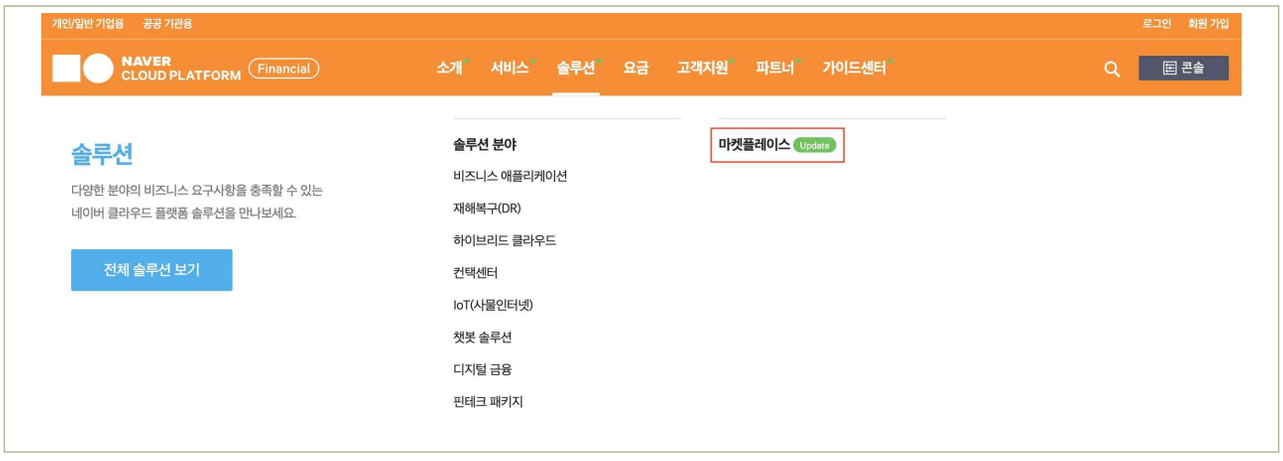
③ **(PC)** SSL VPN Agent 다운로드(링크) 및 설치를 통해 가상자원(Server) 접근 시 ID/Password 인증과 추가 인증수단(SMS, Email)을 통해 접근합니다.



| 그림 1-3-3 | SSL VPN을 통한 추가 인증 수단 적용

- **마켓플레이스 보안 솔루션을 통한 루트 계정 접근 시 추가인증 수단 확보**

① **(네이버 클라우드 플랫폼 포털)** '솔루션' → '마켓플레이스'를 클릭합니다.



| 그림 1-3-4 | NCP 마켓플레이스

② **(네이버 클라우드 플랫폼 포털)** '검색창'에 서버접근통제, 서버보안 등의 3rd Party 보안 솔루션을 검색합니다.

| 그림 1-3-5 | 3rd Party 보안 솔루션 검색

③ **(네이버 클라우드 플랫폼 포털)** 적합한 3rd Party 보안 솔루션의 선택 및 이용 신청을 통해 VPC내에 보안 솔루션을 구성하여 가상자원 루트 계정 접속 시 추가 인증 수단을 적용합니다.

| 그림 1-3-6 | 3rd Party 보안솔루션 이용신청

※ 3rd Party 보안 솔루션 구성에 대한 보다 자세한 사항 및 문의는 마켓플레이스 기술 지원 탭에 안내된 연락처를 통해 문의하여 주시기 바랍니다.

4 참고 사항

- [참고1] SSL VPN Agent 설치 및 접속 가이드
- [참고2] SSL VPN Agent 다운로드
- [참고3] 네이버 클라우드 플랫폼 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 IP대역에서만 접근할 수 있도록 설정하여야 한다.

  - 예시

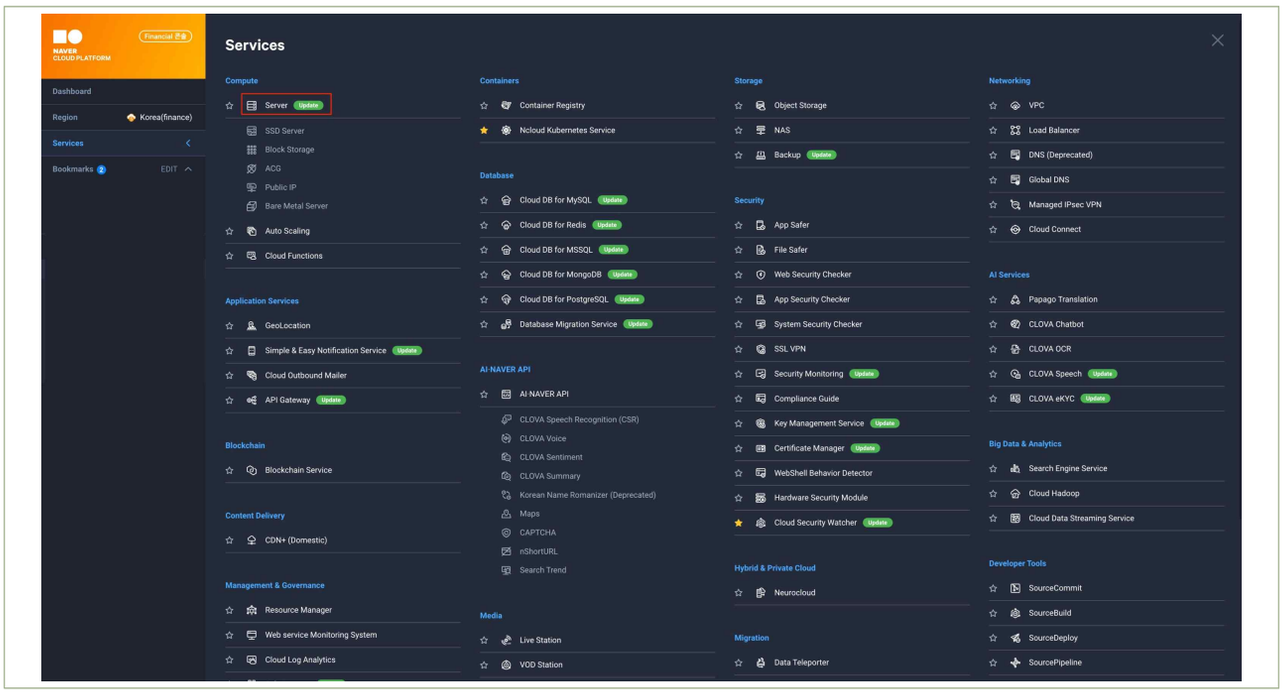
    1) 가상자원 접속 가능한 공인IP(외부)대역 점검 및 제거
    2) 접근가능한 IP 또는 IP 대역대 설정
    3) VPC 및 보안그룹을 통한 내부 네트워크 대역 접근 설정

3 우수 사례

- 네이버 클라우드 플랫폼은 가상자원(Server, Cloud DB 등)의 접근제어를 위하여 ACG(Access Control Group)의 Inbound 규칙을 사용할 수 있습니다.
  ACG는 Whitelist 기반의 접근제어를 제공하므로 추가된 허용 규칙 외의 접근은 모두 차단됩니다. 사용자는 이러한 ACG를 통해 가상자원에 대한 외부 접근을 제한하고 접근 가능한 최소한의 IP를 정의하여 안전한 네트워크를 구성하여야 합니다.

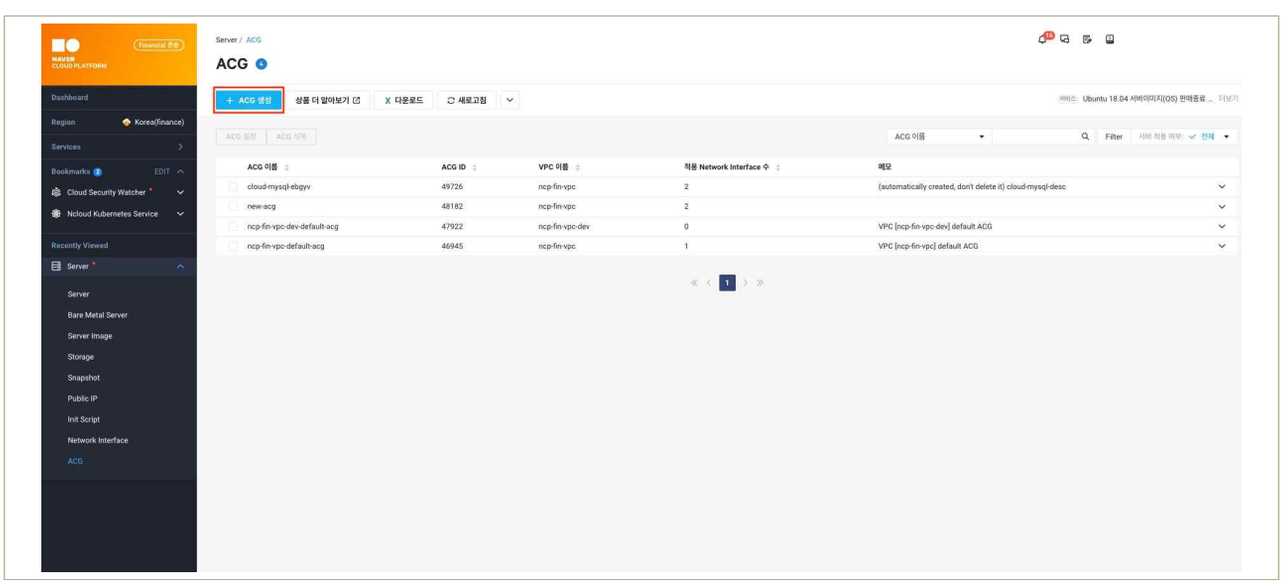
Server에 대한 IP 접근제어

① **(가상자원관리시스템)** ‘Services’ → ‘Server’ 상품을 선택합니다.



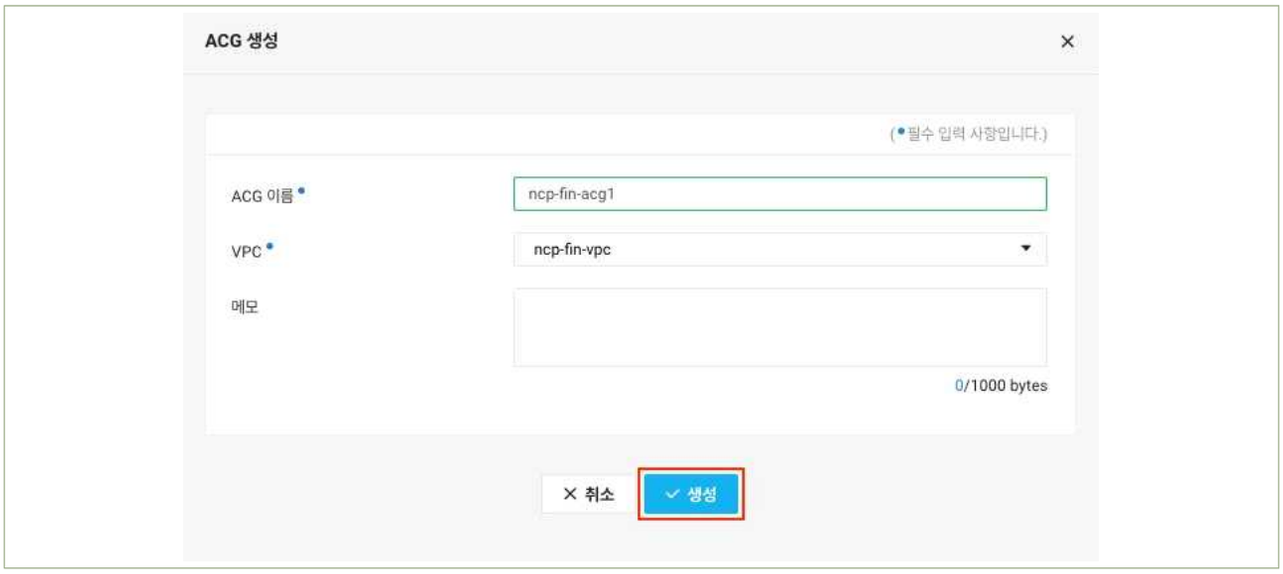
| 그림 1-4-1 | Server 상품 선택

② **(가상자원관리시스템)** ‘ACG’ → ‘+ ACG 생성’을 클릭합니다.



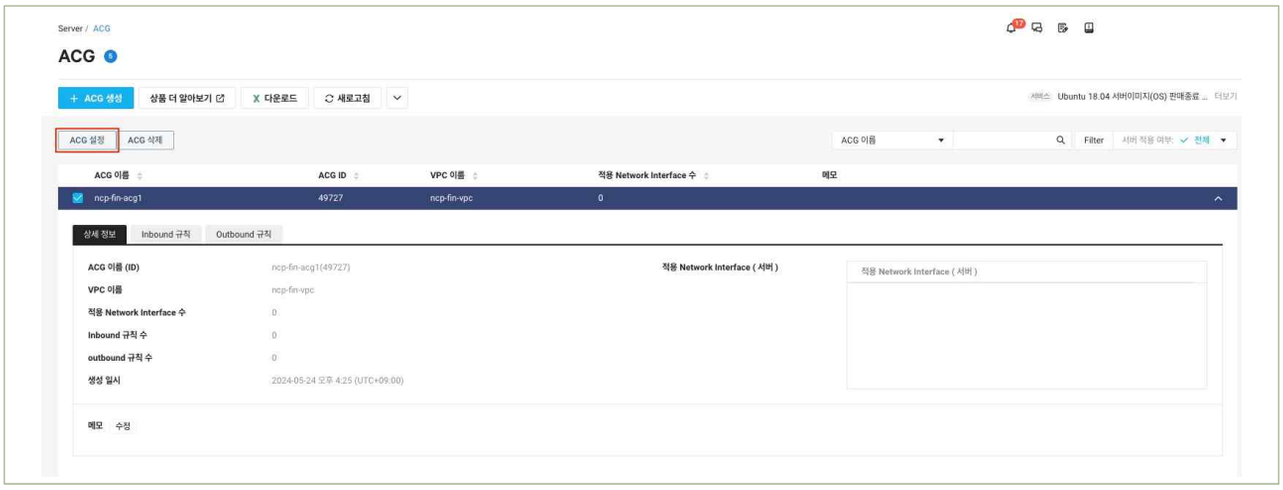
| 그림 1-4-2 | Server의 ACG 생성

③ **(가상자원관리시스템)** ACG 생성을 위해 'ACG 이름'과 '대상 VPC'를 선택하고 '생성'버튼을 클릭합니다.



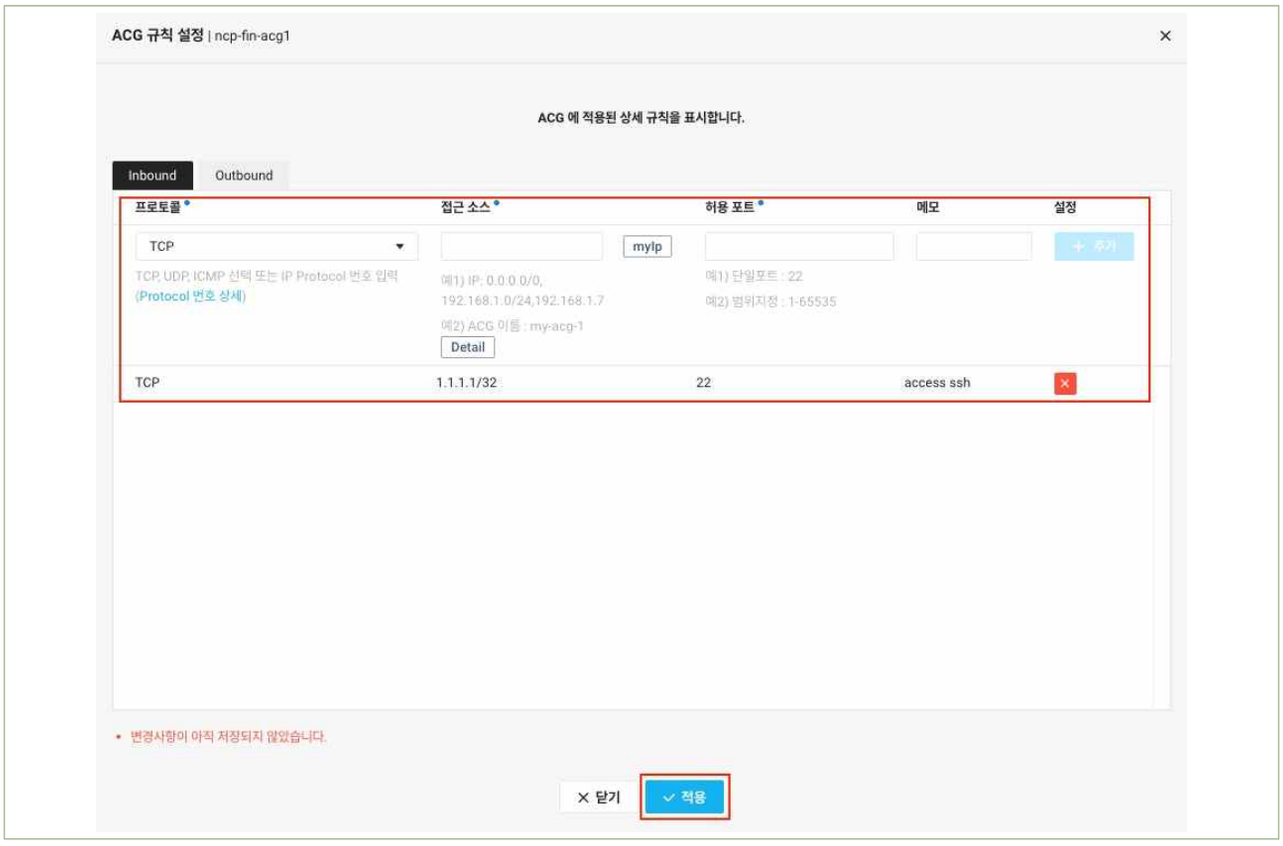
| 그림 1-4-3 | ACG 생성 대상 VPC 선택

④ **(가상자원관리시스템)** 신규 생성된 ACG를 선택하고 'ACG 설정' 버튼을 클릭합니다.



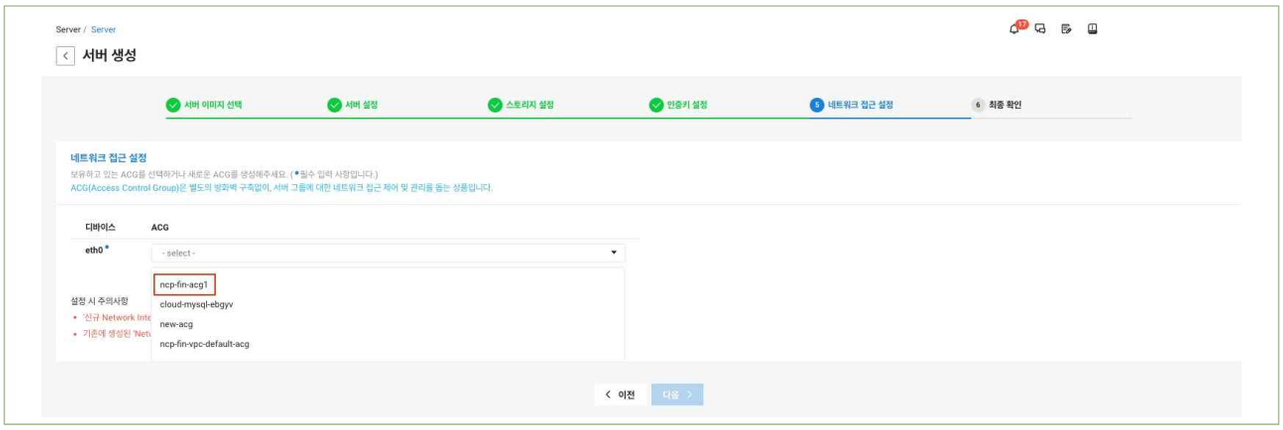
| 그림 1-4-4 | ACG 설정

⑤ **(가상자원관리시스템)** ‘프로토콜’, ‘접근 소스’, ‘허용 포트’ 등을 입력 후, ‘+ 추가’ 버튼을 클릭하여 Inbound 규칙을 정의하고, ‘적용’버튼을 클릭하여 ACG 설정을 완료합니다.



| 그림 1-4-5 | ACG Inbound 규칙 정의 및 적용

⑥ **(가상자원관리시스템)** ‘Services’ → ‘Server’ → ‘Server’ → ‘+ 서버 생성’을 통해 서버를 생성하는 단계 중, ‘네트워크 접근 설정’ 단계에서 사전에 정의한 ACG를 선택하여 가상자원(Server)에 대해 접근제어를 적용합니다.

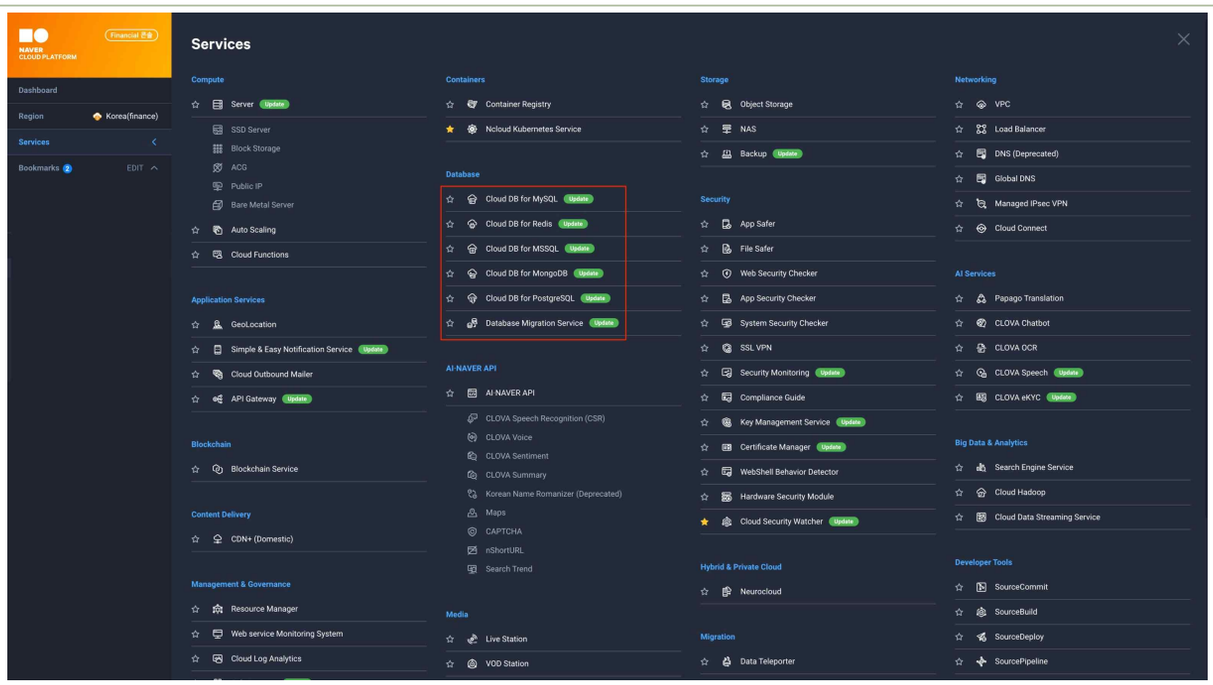


| 그림 1-4-6 | 가상자원(Server)의 접근제어 적용

※ 만약, 공인 IP가 할당된 가상자원(Server) 생성하는 경우, 네이버 클라우드 플랫폼은 다음과 같이 가상자원의 안전한 관리를 위한 외부 직접 접속 허용규칙 적용에 대해 안내하고 있습니다.

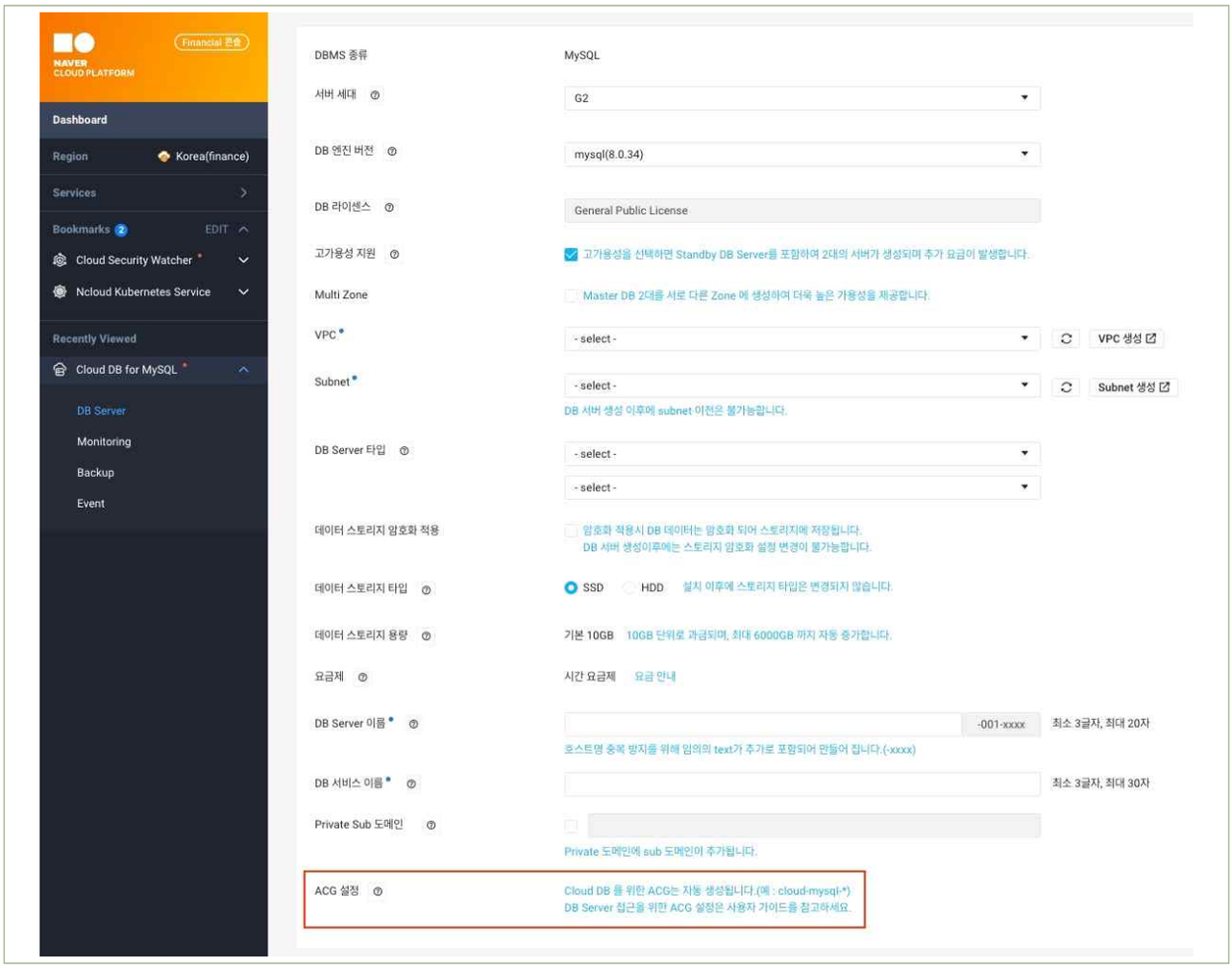
Cloud DB에 대한 IP 접근제어

① **(가상자원관리시스템)** 'Services' → 'Cloud DB' 상품을 선택합니다.



| 그림 1-4-7 | Cloud DB 상품 선택

② **(가상자원관리시스템)** 'DB Server' → '+ DB Server 생성'을 통해 Cloud DB를 생성하는 단계에서 Cloud DB에 대한 ACG는 자동으로 생성됩니다.



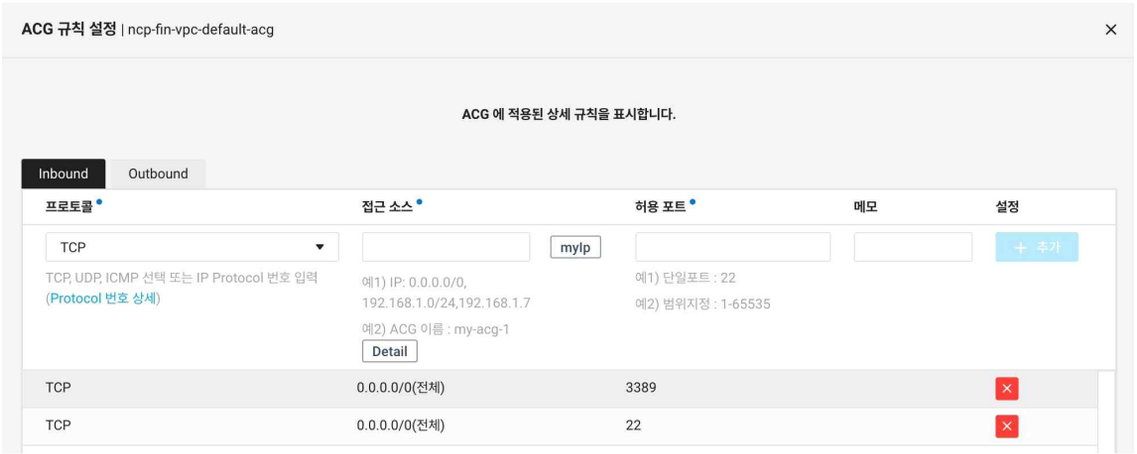
| 그림 1-4-8 | Cloud DB의 ACG 생성

③ **(가상자원관리시스템)** '대상 Cloud DB' → '규칙 보기'를 통해 자동으로 생성된 Cloud DB의 ACG Inbound 규칙을 확인합니다.

| 그림 1-4-9 | Cloud DB 접속 허용 IP대여 확인

※ 자동 생성된 Cloud DB의 ACG는 기본적으로 로컬호스트 외의 접근이 불가하도록 안전한 Inbound 규칙으로 생성됩니다.

불필요한 IP대역의 삭제 등 Cloud DB의 ACG 수정이 필요한 경우, ‘Services’ → ‘Server’ → ‘ACG’ → ‘대상 ACG’ → ‘ACG 설정’을 통해 Cloud DB에대한 Inbound 허용 규칙을 수정할 수 있습니다.



[ACG Inbound 규칙 수정]

API를 통한 가상자원(Server, Cloud DB)의 접근제어 설정

① **(API(CLI))** ‘createServerInstances’ API를 통해 가상자원(Server) 생성 시 ‘accessControlGroupNoList’ 파라미터에 사전에 정의된 ACG ID를 연결하여 안전한 네트워크 접근제어를 적용합니다.

- 요청 예시

```
GET https://fin-ncloud.apigw.fin-ntruss.com/vserver/v2/createServerInstances
?regionCode=FKR
&serverImageProductCode=SW.VSVR.OS.LNX64.CNTOS.0703.B050
&vpcNo=***04
&subnetNo=***43
&serverProductCode=SVR.VSVR.STAND.C002.M004.NET.SSD.B050.G001
&feeSystemTypeCode=MTRAT
&serverCreateCount=1
&serverName=test-***
&networkInterfaceList.1.networkInterfaceOrder=0
&networkInterfaceList.1.accessControlGroupNoList.1=***34
&networkInterfaceList.1.accessControlGroupNoList.2=***45
&placementGroupNo=***61
&isProtectServerTermination=false
&initScriptNo=***44
&loginKeyName=test-***
&associateWithPublicIp=true
```

| 그림 1-4-10 | Server 생성 시 안전한 ACG 적용

② **(API(CLI))** 'getAccessControlGroupRuleList' API을 통해 확인 대상 ACG ID에 대한 Inbound 세부 규칙을 확인할 수 있습니다.

- 요청 예시

```
GET https://fin-ncloud.apigw.fin-ntruss.com/vserver/v2/getAccessControlGroupRuleList
?regionCode=FKR
```

- 응답 예시

```
<getAccessControlGroupRuleListResponse>
<requestId>a6fe4c12-b592-41c6-acf9-dff0369f09b0</requestId>
<returnCode>0</returnCode>
<returnMessage>success</returnMessage>
<totalRows>2</totalRows>
<accessControlGroupRuleList>
    <accessControlGroupRule>
      <accessControlGroupNo>***63</accessControlGroupNo>
      <protocolType>
        <code>TCP</code>
        <codeName>tcp</codeName>
        <number>6</number>
      </protocolType>
      <ipBlock>***.***.0.0/0</ipBlock>
      <accessControlGroupSequence></accessControlGroupSequence>
      <portRange>22</portRange>
      <accessControlGroupRuleType>
        <code>INBND</code>
        <codeName>Inbound</codeName>
      </accessControlGroupRuleType>
   <accessControlGroupRuleDescription></accessControlGroupRuleDescription>
    </accessControlGroupRule>
    <accessControlGroupRule>
      <accessControlGroupNo>***63</accessControlGroupNo>
      <protocolType>
        <code>TCP</code>
        <codeName>tcp</codeName>
        <number>6</number>
      </protocolType>
      <ipBlock>***.***.0.0/0</ipBlock>
      <accessControlGroupSequence></accessControlGroupSequence>
      <portRange>22</portRange>
      <accessControlGroupRuleType>
        <code>OTBND</code>
        <codeName>Outbound</codeName>
      </accessControlGroupRuleType>
   <accessControlGroupRuleDescription></accessControlGroupRuleDescription>
    </accessControlGroupRule>
</accessControlGroupRuleList>
</getAccessControlGroupRuleListResponse>
```

| 그림 1-4-11 | ACG의 Inbound 세부 규칙 확인

③ **(API(CLI))** ‘removeAccessControlGroupInboundRule’ API를 통해 안전하지 않은 Inbound 규칙을 제거하고, ‘addAccessControlGroupInboundR`ule’ API를 통해 안전한 Inbound 규칙을 적용할 수 있습니다.

- 요청 예시 (규칙 제거)

```
GET  https://fin-ncloud.apigw.fin-ntruss.com/vserver/v2/removeAccessControlGroupInboundRule
?regionCode=FKR
&vpcNo=***04
&accessControlGroupNo=***63
&accessControlGroupRuleList.1.protocolTypeCode=TCP
&accessControlGroupRuleList.1.ipBlock=***.***.0.0/0
&accessControlGroupRuleList.1.portRange=22
```

- 요청 예시 (규칙 생성)

```
GET https://fin-ncloud.apigw.fin-ntruss.com/vserver/v2/addAccessControlGroupInboundRule
?regionCode=FKR
&vpcNo=***04
&accessControlGroupNo=***63
&accessControlGroupRuleList.1.protocolTypeCode=TCP
&accessControlGroupRuleList.1.ipBlock=***.***.10.1/32
&accessControlGroupRuleList.1.portRange=22
```

| 그림 1-4-12 | ACG 규칙의 제거 및 생성

4 참고 사항

- [참고1] ACG 사용 가이드
- [참고2] ACG 규칙 확인 API 가이드
- [참고3] ACG 규칙 삭제 API 가이드
- [참고4] ACG 규칙 생성 API 가이드
- [참고5] Server 생성 API 가이드

1 기준

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

2 설명

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

  - 예시

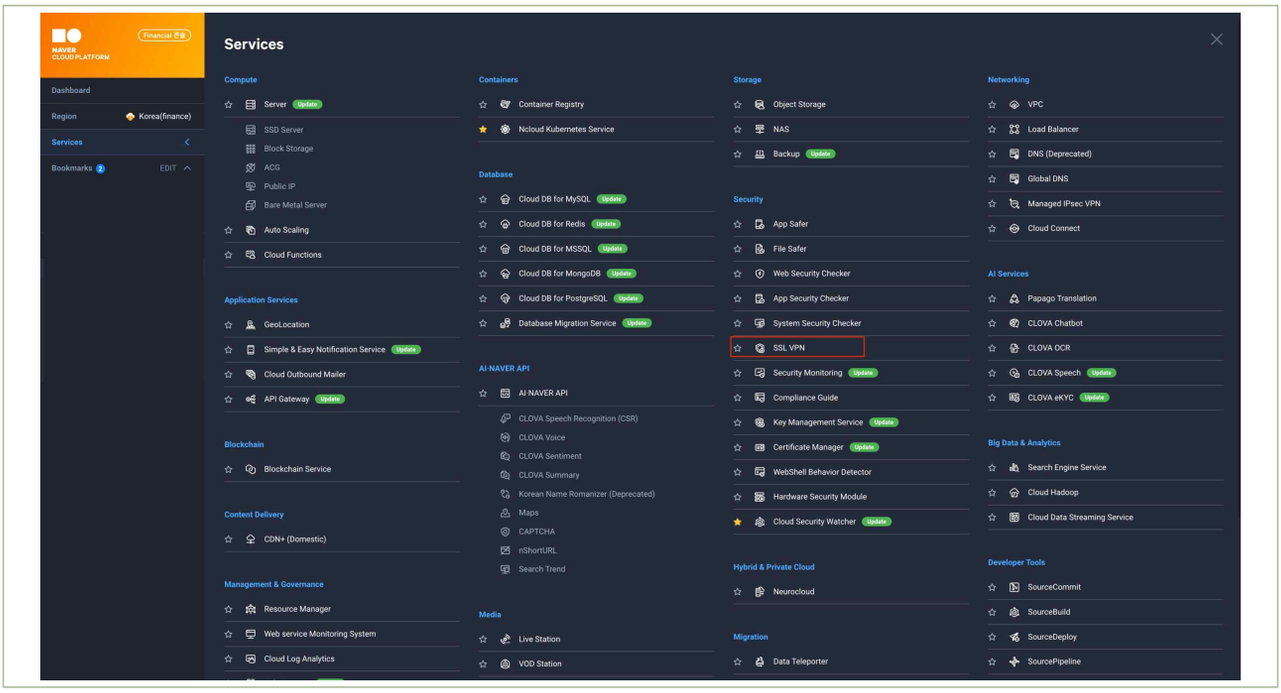
    1) SSH를 통한 접속 시 안전한 인증절차 적용
    2) 클라우드 웹 콘솔에서 직접 실행 시 안전한 인증 방식 적용(해당 인스턴스를 호출할 수 있는 권한을 지닌 이용자인지 검증 등)

3 우수 사례

- 네이버 클라우드 플랫폼은 사용자의 안전한 가상자원(Server) 접근을 위해 SSL VPN 보안상품의 사용을 권장하고 있습니다. 사용자는 SSL VPN상품을 이용하여 안전한 인증수단을 적용하고 안전한 통신수단을 통해 가상자원(Server, Cloud DB)에 접근할 수 있습니다.

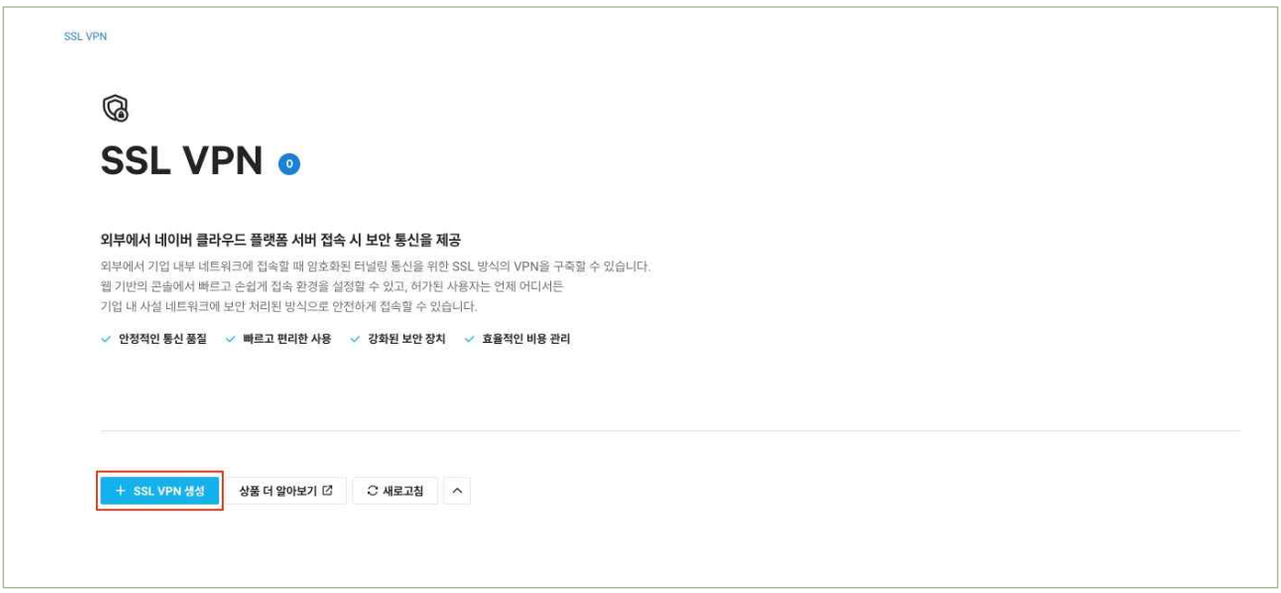
가상자원 루트 계정 접근 시 추가인증 수단 확보

① **(가상자원관리시스템)** ‘Services’ → ‘SSL VPN’ 상품을 선택합니다.



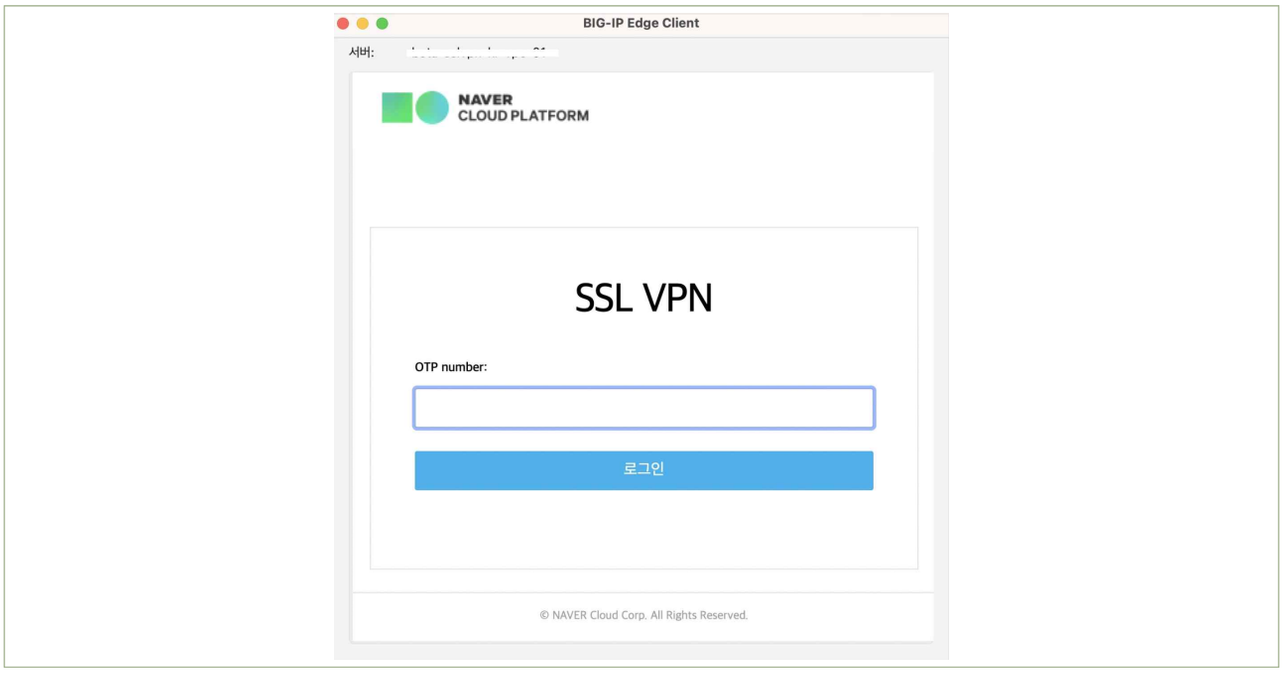
| 그림 1-5-1 | SSL VPN 상품 선택

② **(가상자원관리시스템)** ‘+ SSL VPN 생성’ 버튼을 클릭하여 SSL VPN 상품을 활성화합니다.



| 그림 1-5-2 | SSL VPN 상품 활성화

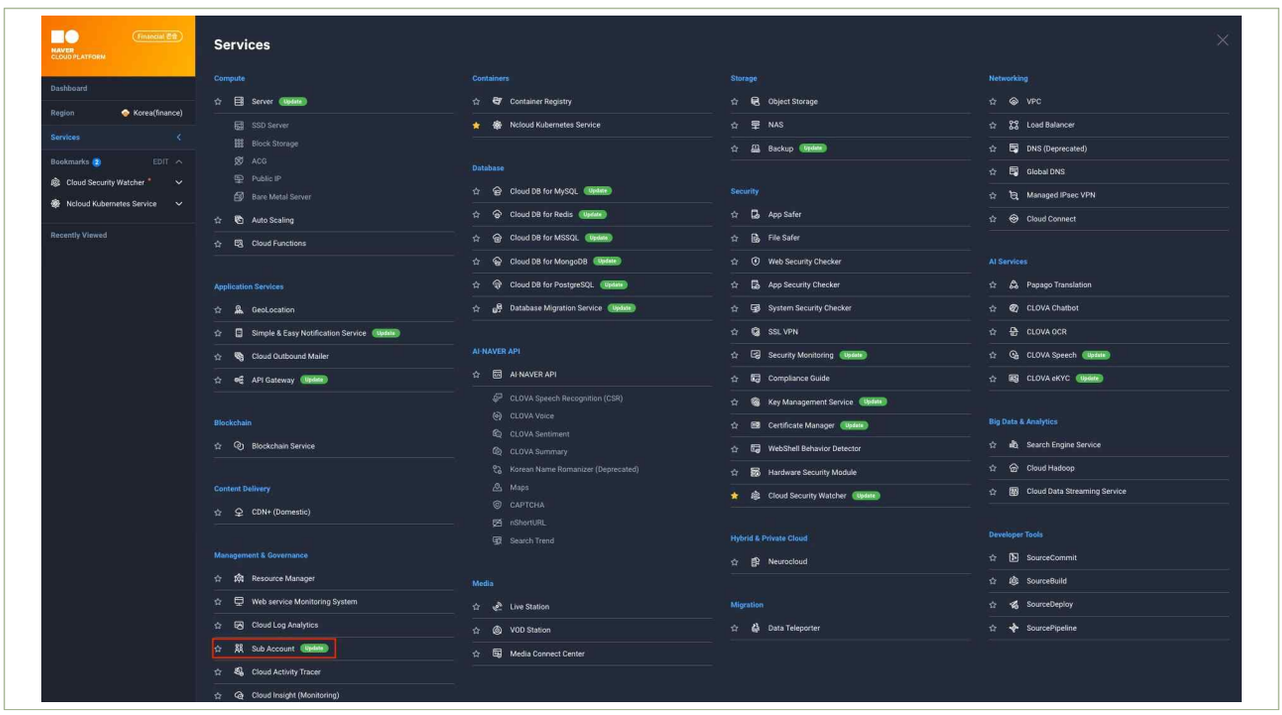
③ **(PC)** SSL VPN Agent 다운로드(링크) 및 설치를 통해 가상자원(Server) 접근 시 ID/Password 인증과 추가 인증수단(SMS, Email)을 통해 접근합니다.



| 그림 1-5-3 | SSL VPN을 통한 추가 인증 수단 적용

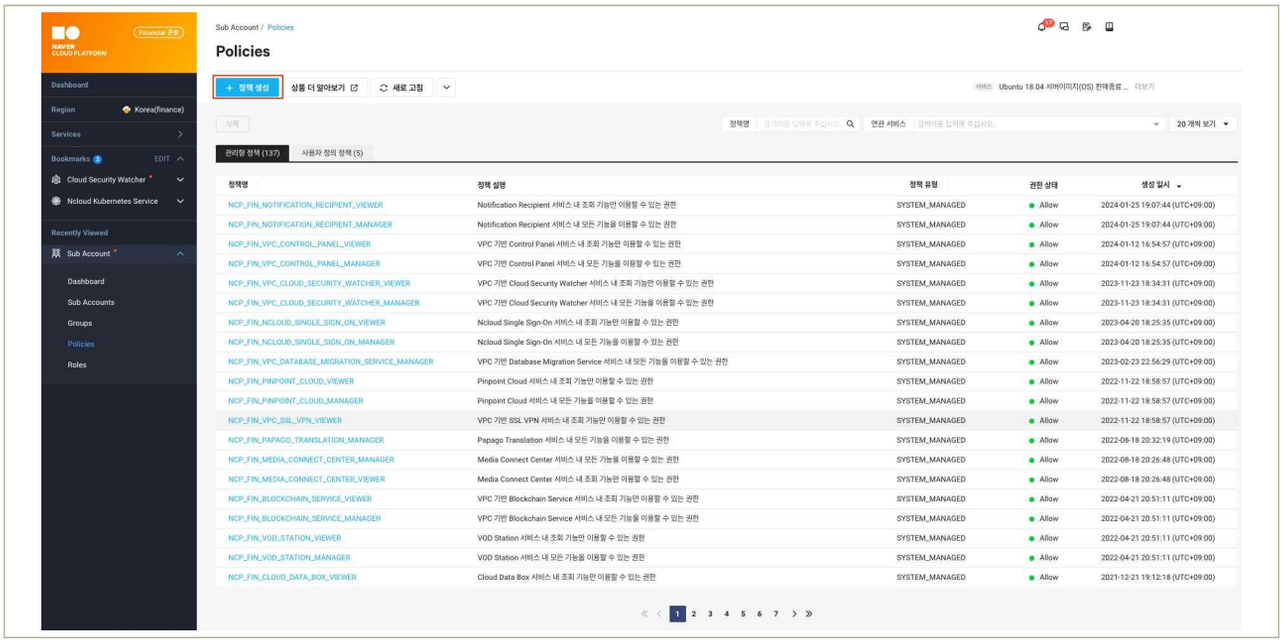
◎ 사용자 정의 정책을 통한 서버 접속 콘솔 사용 제한

① **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ 상품을 선택합니다.



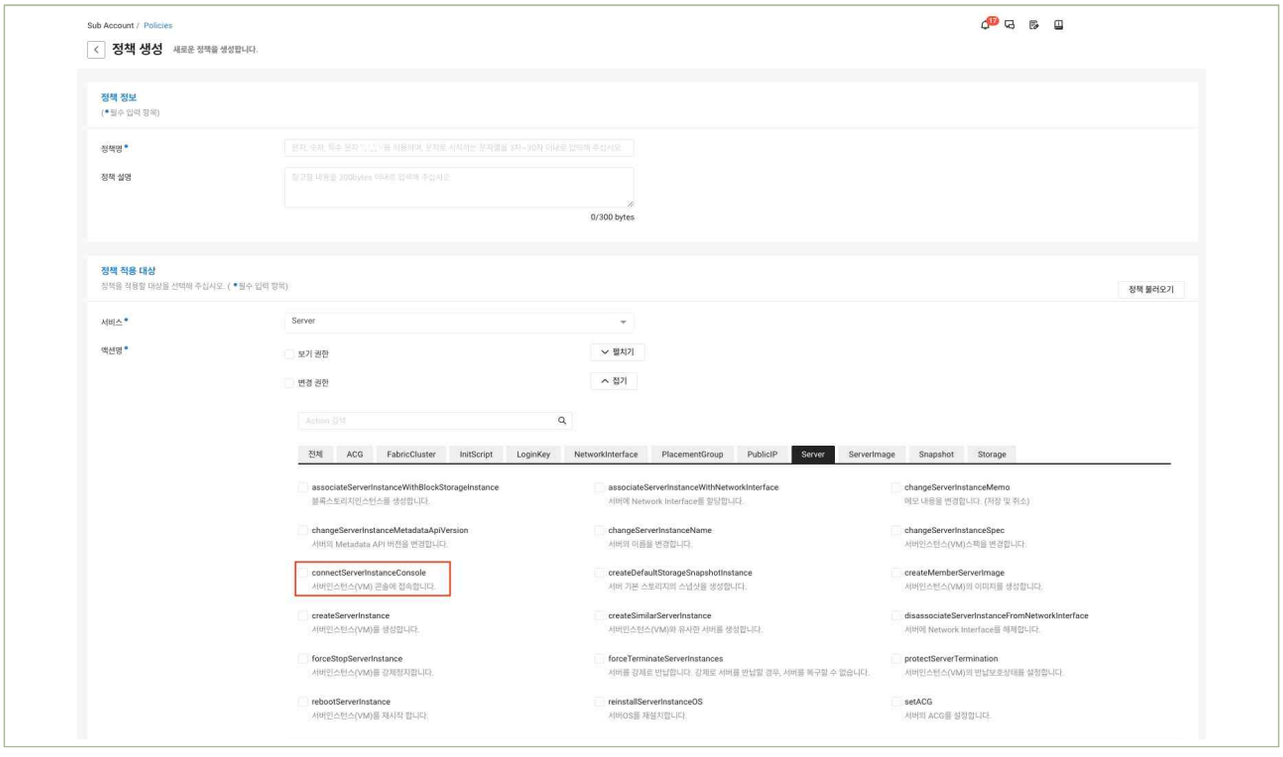
| 그림 1-5-4 | Sub Account 상품 선택

② **(가상자원관리시스템)** 사용자 정의 정책 생성을 위해 'Policies' → '+ 정책 생성'버튼을 클릭합니다.



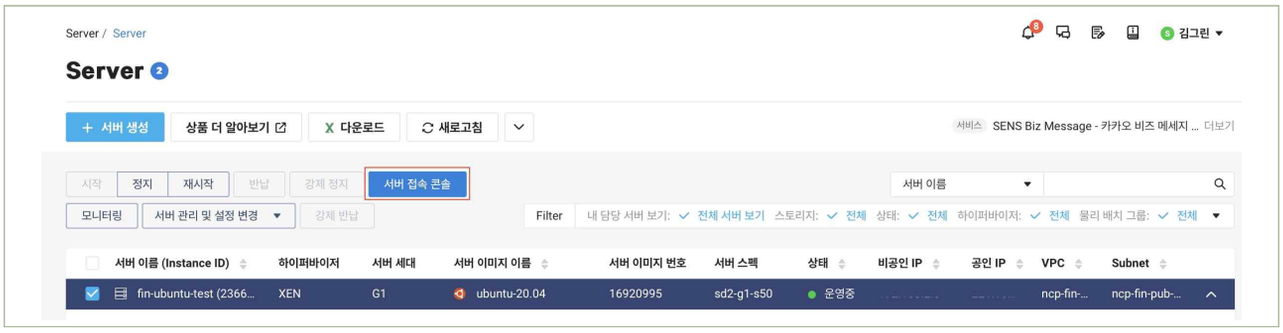
| 그림 1-5-5 | 사용자 정의 정책 생성

③ **(가상자원관리시스템)** 'Policies' → '+ 정책 생성'를 통해 사용자 정의 정책을 생성하고, 웹 콘솔 접근을 제한할 서브 계정에 사용자 정의 정책을 연결합니다.



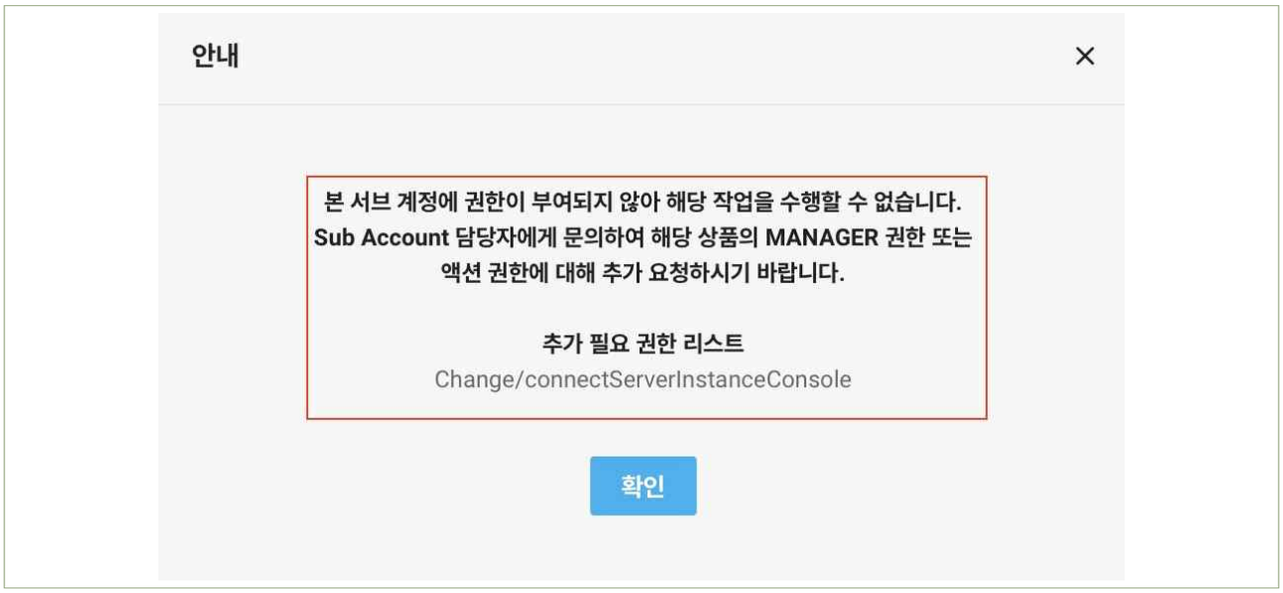
| 그림 1-5-6 | 사용자 정의 정책 생성

④ **(가상자원관리시스템)** ‘Services’ → ‘Server’ → ‘서버 접속 콘솔’ 버튼을 통해 서버 접속 콘솔에 접근합니다.



| 그림 1-5-7 | 서버 접속 콘솔 접근 시도

⑤ **(가상자원관리시스템)**’ 서버 접속 콘솔에 대한 권한이 존재하지 않은 서브 계정은 다음과 같이 접근이 차단됩니다.



| 그림 1-5-8 | 서버 접속 콘솔 접근 차단 예시

4 참고 사항

- [참고1] SSL VPN Agent 설치 및 접속 가이드
- [참고2] SSL VPN Agent 다운로드
- [참고3] 사용자 정의 정책 생성 가이드

1 기준

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

2 설명

- 이용자 직무 및 권한에 따른 가상자원 별 접근통제 방안(권한 설정 등)을 수립하여야 한다.

  - 예시

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

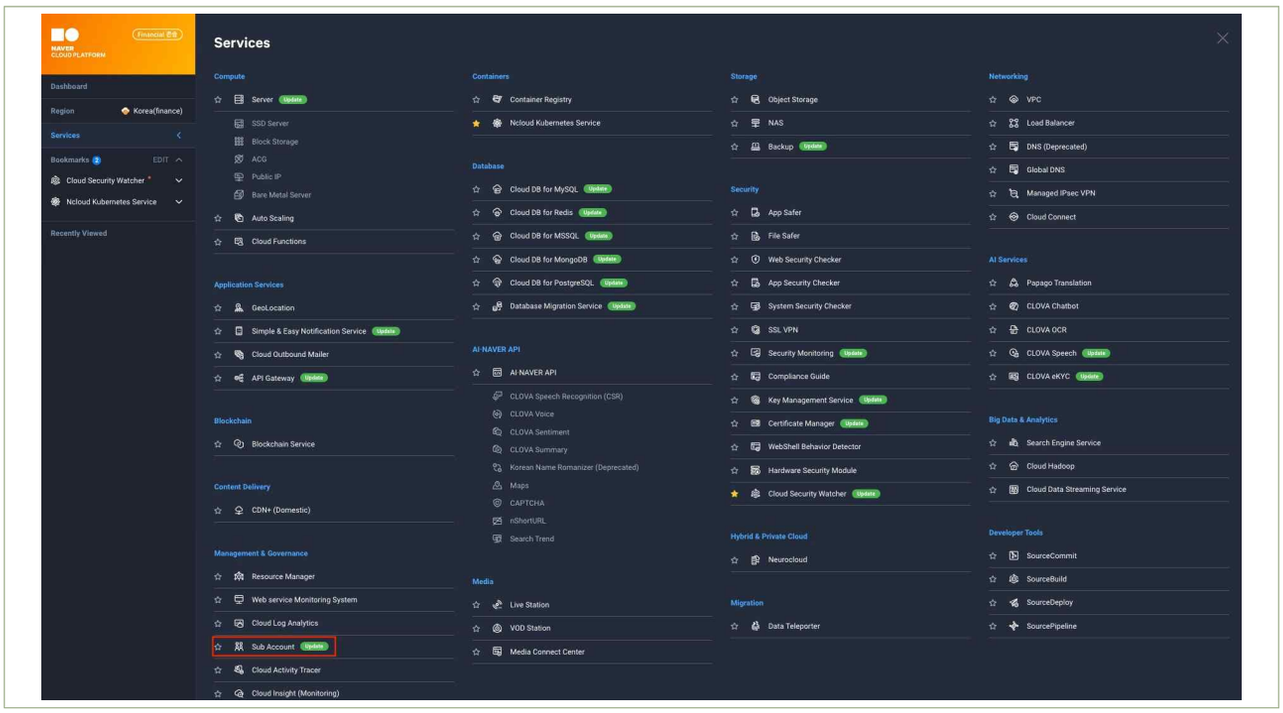
       - 모든 가상자원에 접근 가능한 Role에 대해서는 최소 인원에 대해서만 부여

3 우수 사례

- 네이버 클라우드 플랫폼은 이용자 직무 및 권한을 고려한 권한체계를 적용할 수 있도록 Sub Account 상품을 통해 사용자 정의 정책 부여할 수 있습니다. 사용자 정의 정책을 사용하면 이용자(서브 계정) 별 가상자원에 대한 세부 권한을 제어하고 관리할 수 있습니다.

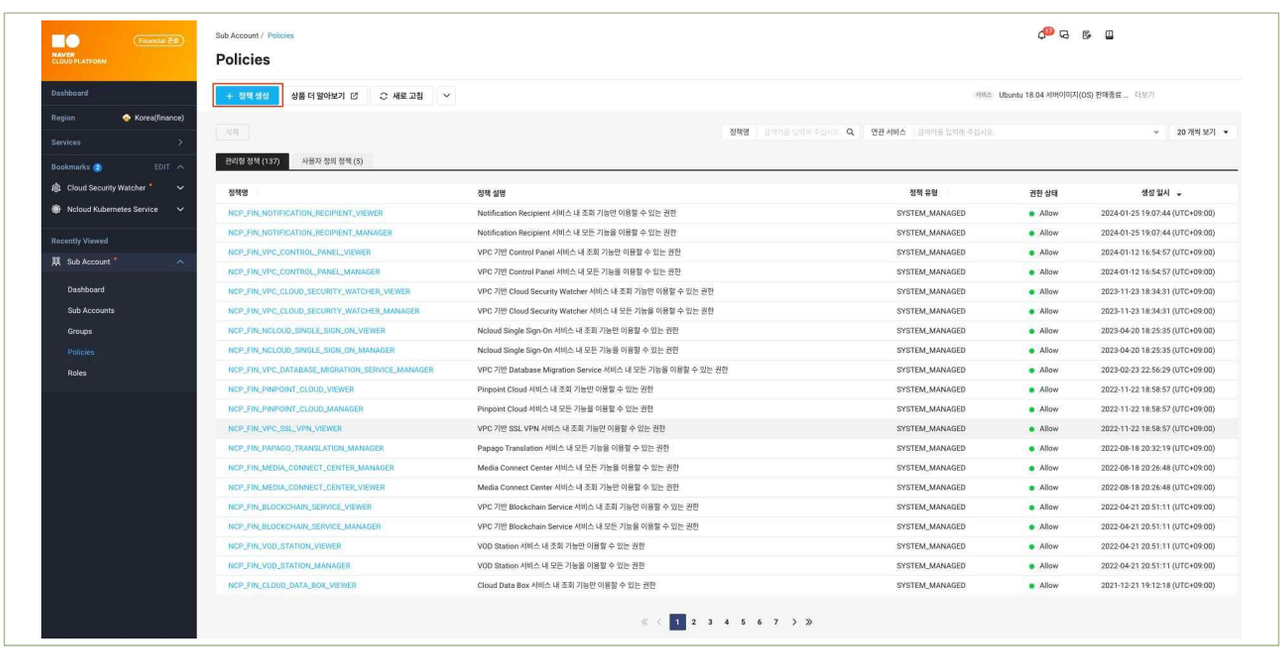
서브 계정 별 특정 가상자원에 대한 접근권한 부여

① **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ 상품을 선택합니다.



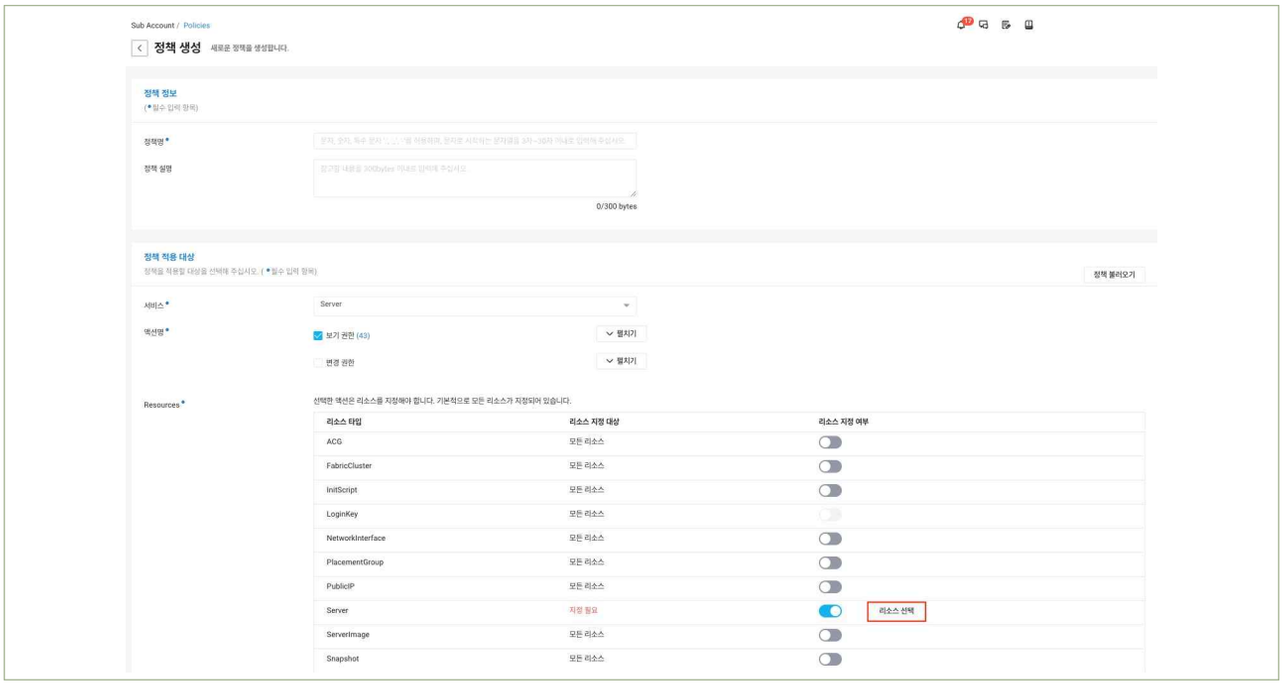
| 그림 1-6-1 | Sub Account 상품 선택

② **(가상자원관리시스템)** 사용자 정의 정책 생성을 위해 ‘Policies’ → ‘+ 정책 생성’버튼을 클릭합니다.



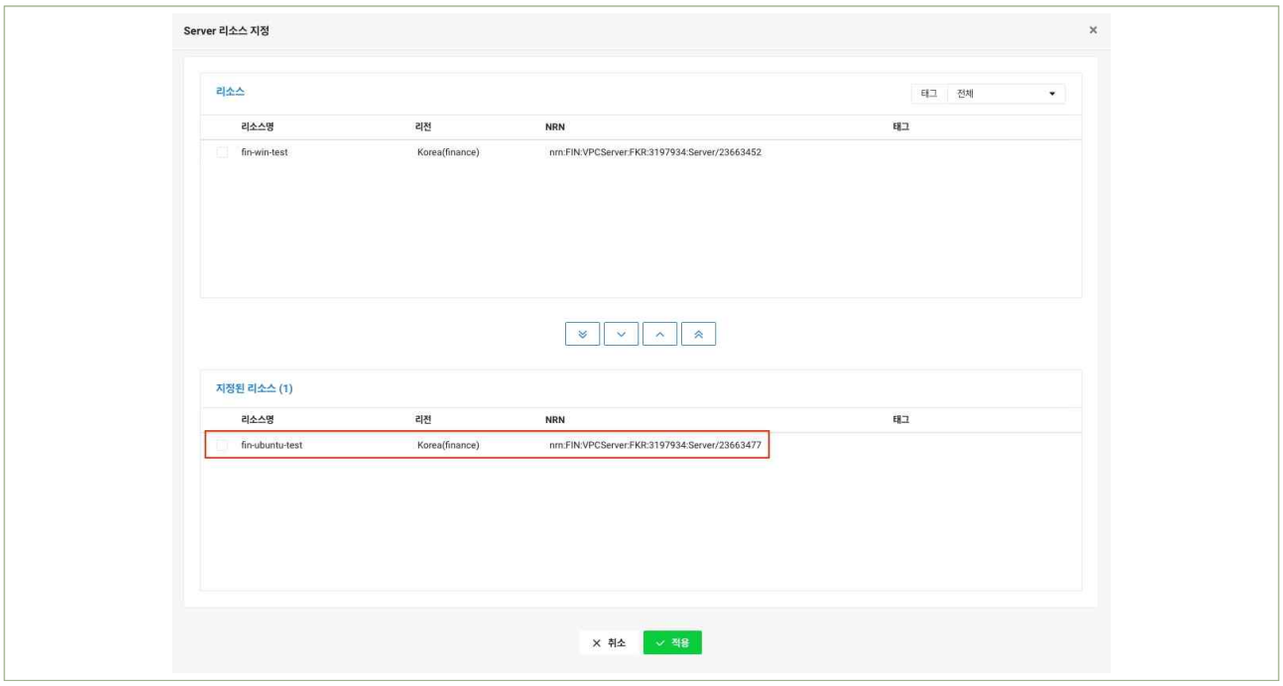
| 그림 1-6-2 | 사용자 정의 정책 생성

③ **(가상자원관리시스템)** 정책 생성 단계에서 특정 가상자원에 대한 접근권한 부여 정책 생성을 위해 리소스 지정 여부 토글을 활성화하고 '리소스 선택' 버튼을 클릭합니다.



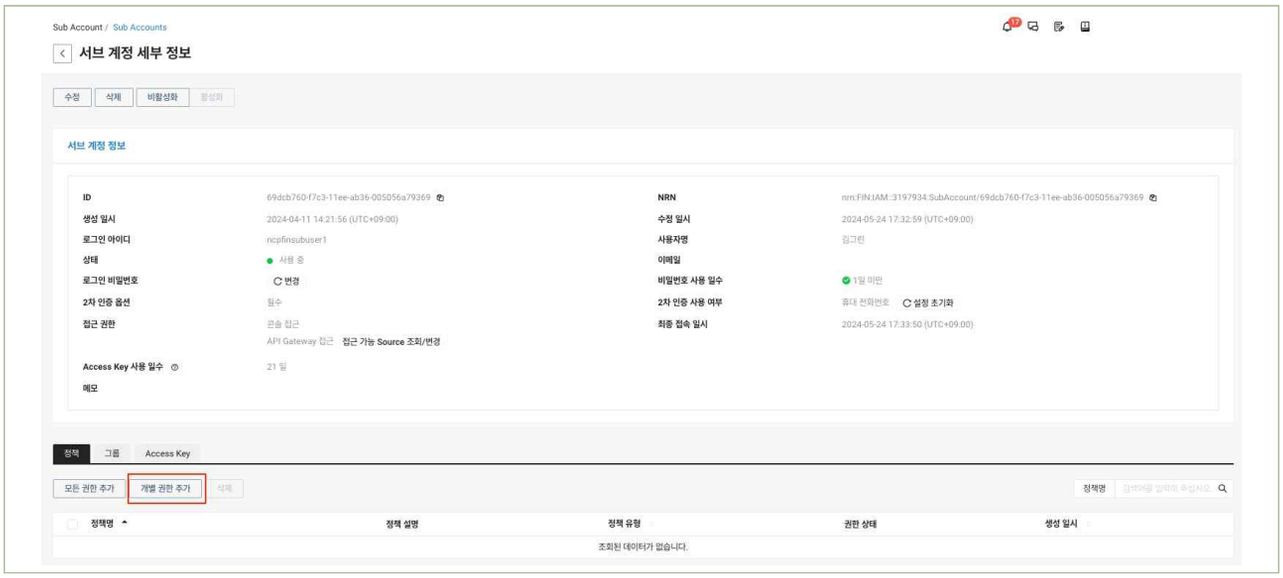
| 그림 1-6-3 | 리소스 지정 여부 활성화

④ **(가상자원관리시스템)** 리소스 지정 단계에서 접근권한을 부여할 가상자원을 선택하고 '적용'버튼을 클릭하여 정책생성을 완료합니다.



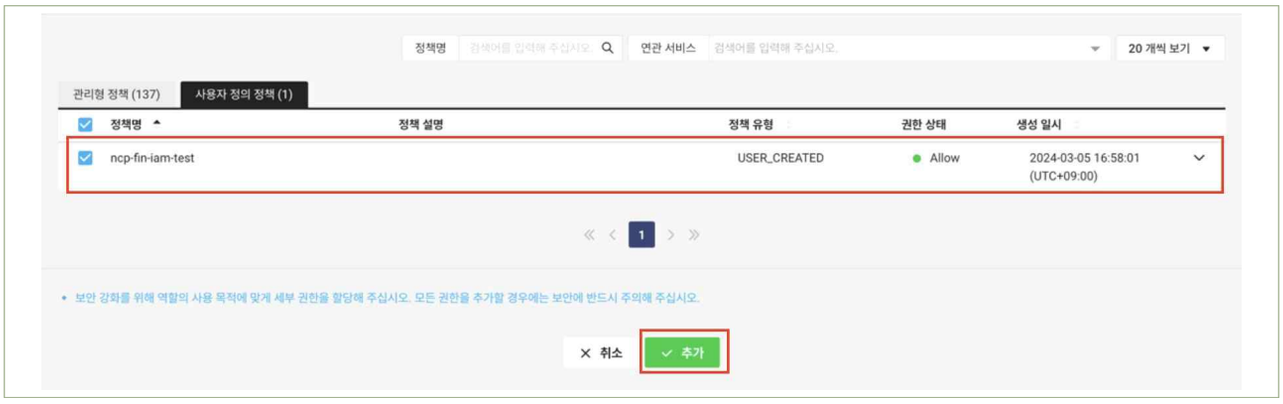
| 그림 1-6-4 | 가상자원 리소스 지정

⑤ **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ → ‘Sub Accounts’에서 사용자 정의 정책을 부여할 서브 계정을 선택하고, ‘개별 권한 추가’를 클릭합니다.



| 그림 1-6-5 | 서브 계정 별 개별 권한 추가

⑥ **(가상자원관리시스템)** 정책 추가 단계에서 사전에 정의한 ‘사용자 정의 정책’을 서브 계정에게 연결합니다.



| 그림 1-6-6 | 사용자 정의 정책 부여 예시

4 참고 사항

- [참고1] 사용자 정의 정책 생성 가이드

1 기준

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

2 설명

- 이용자 가상자원 내 악성코드 통제방안을 수립하여야 한다.

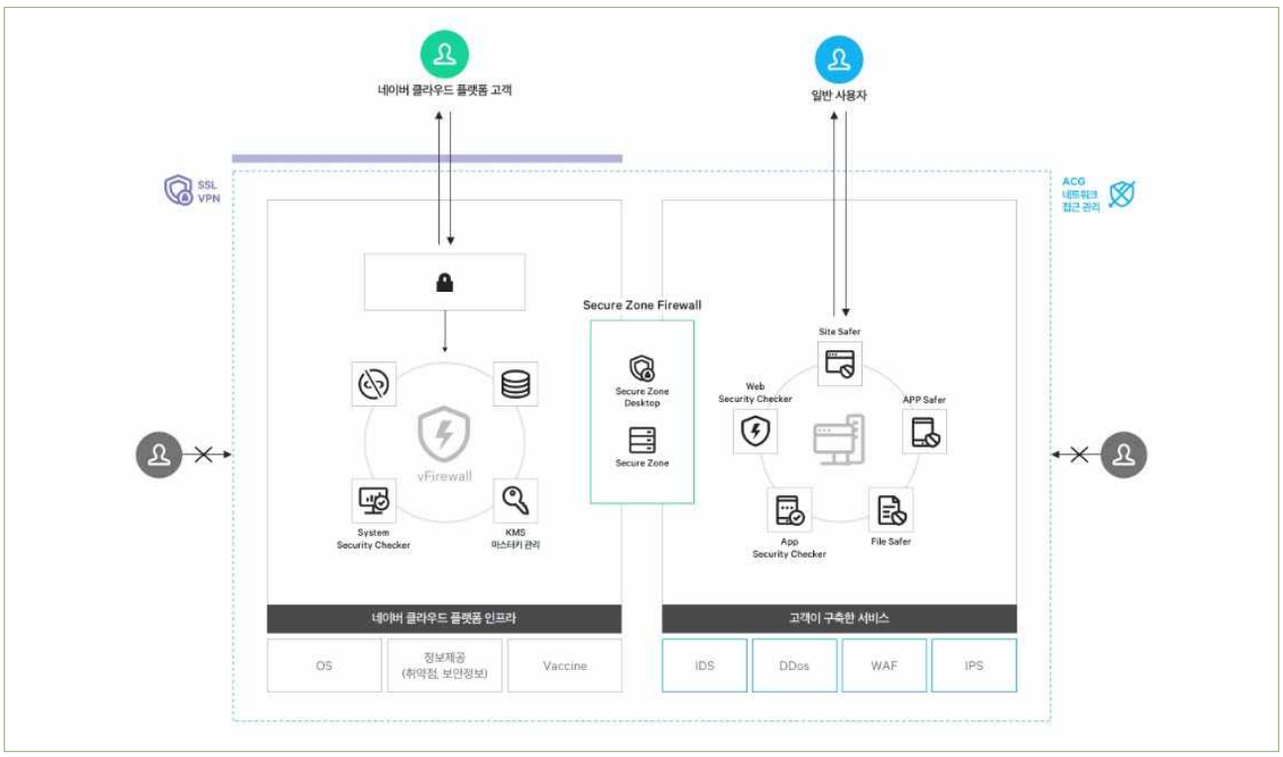
  - 예시

    1) 이용자가 보유하고 있는 악성코드 통제방안 수립(백신 등)

    2) 클라우드 사업자가 악성코드 통제방안 제공(백신 등)

3 우수 사례

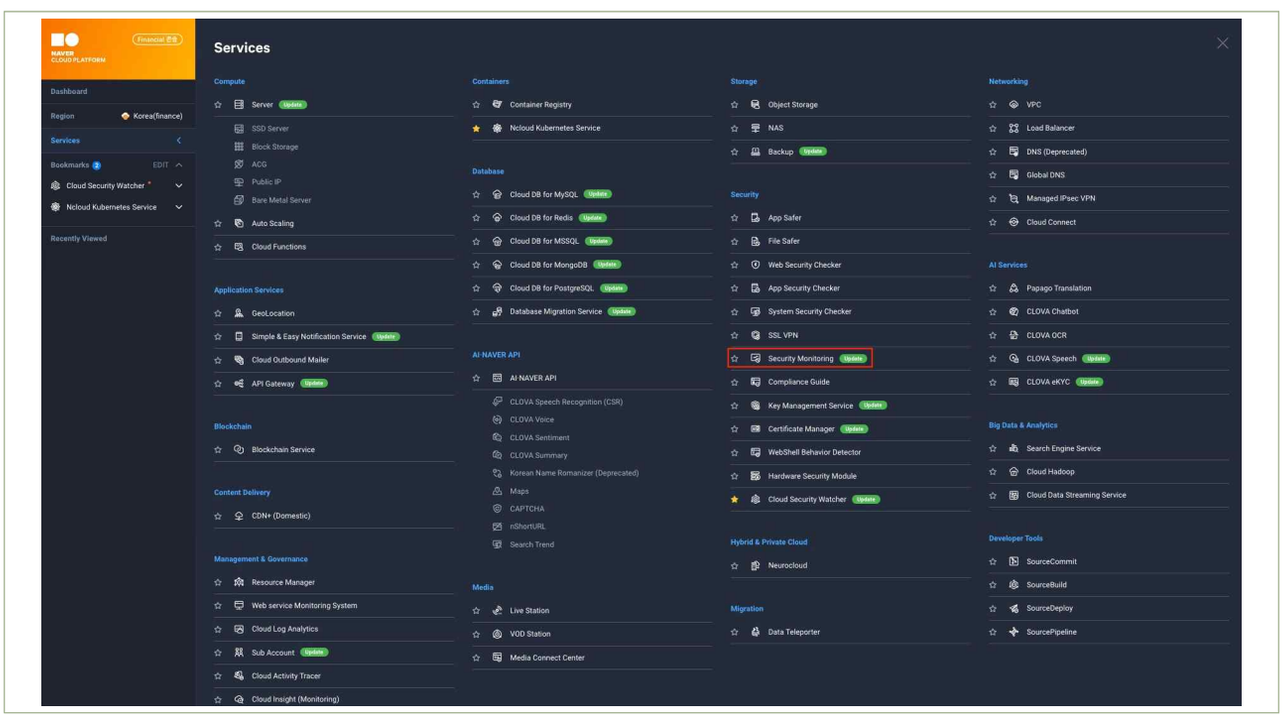
- 네이버 클라우드 플랫폼은 사용자의 가상자원을 안전하게 보호하기 위하여 Anti-Virus, IDS, IPS, WAS, Anti-DDoS 구성 및 보안전문 인력이 24시간 365일 보안관제 서비스를 수행하는 Security Monitoring 상품을 제공하고 있습니다. 사용자는 Security Monitoring 상품의 Anti-Virus 통해 가상자원(Server)의 Linux 및 Windows OS에 대한 악성코드를 탐지하고 방어할 수 있습니다.



| 그림 1-7-1 | Security Monitoring 아키텍처

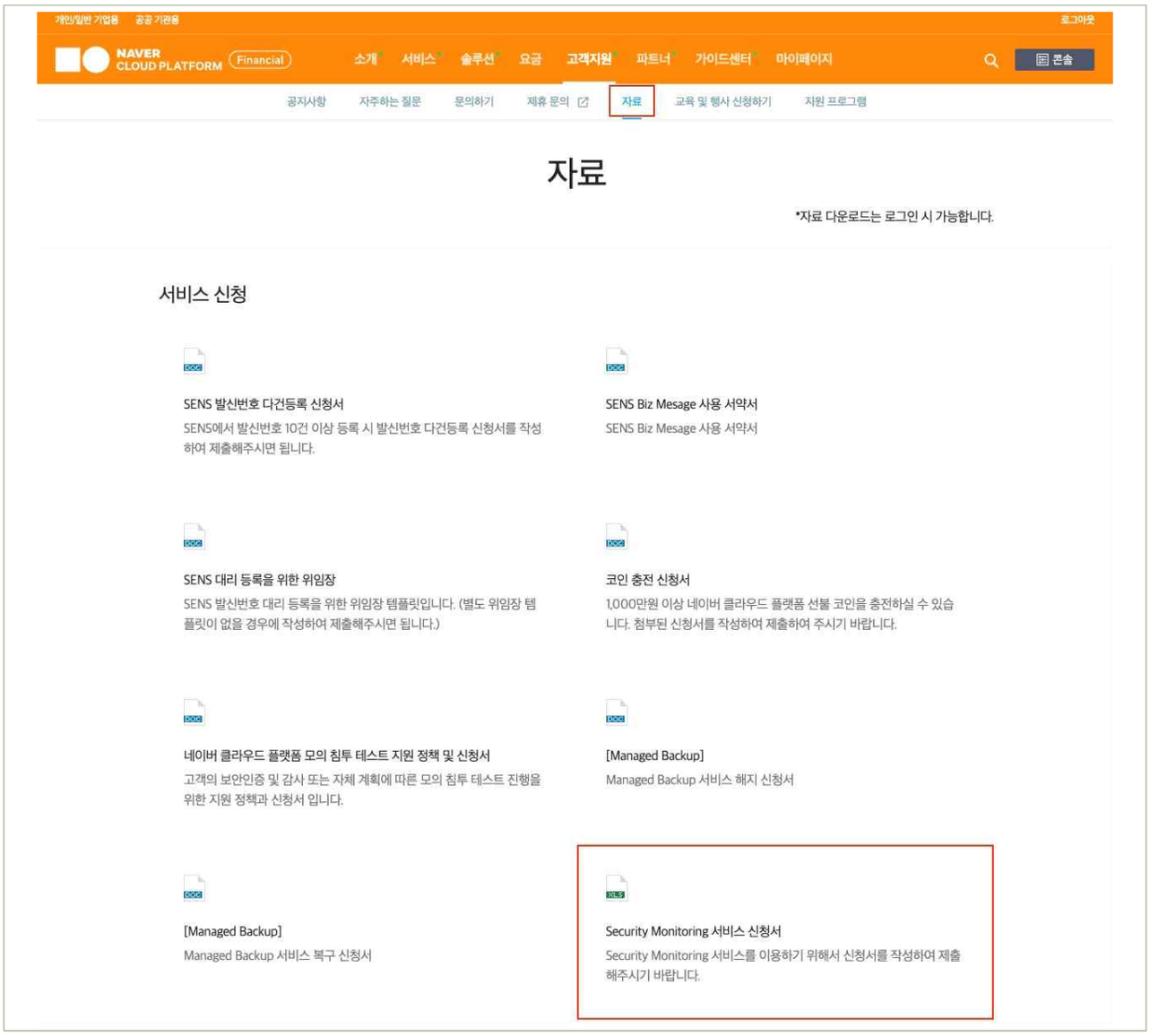
◦ 네이버 클라우드 플랫폼의 Anti-Virus 상품 이용

① **(가상자원관리시스템)** 'Services' → 'Security Monitoring' 상품을 선택하고, '+ 상품 이용 신청'을 통해 상품을 활성화 합니다.



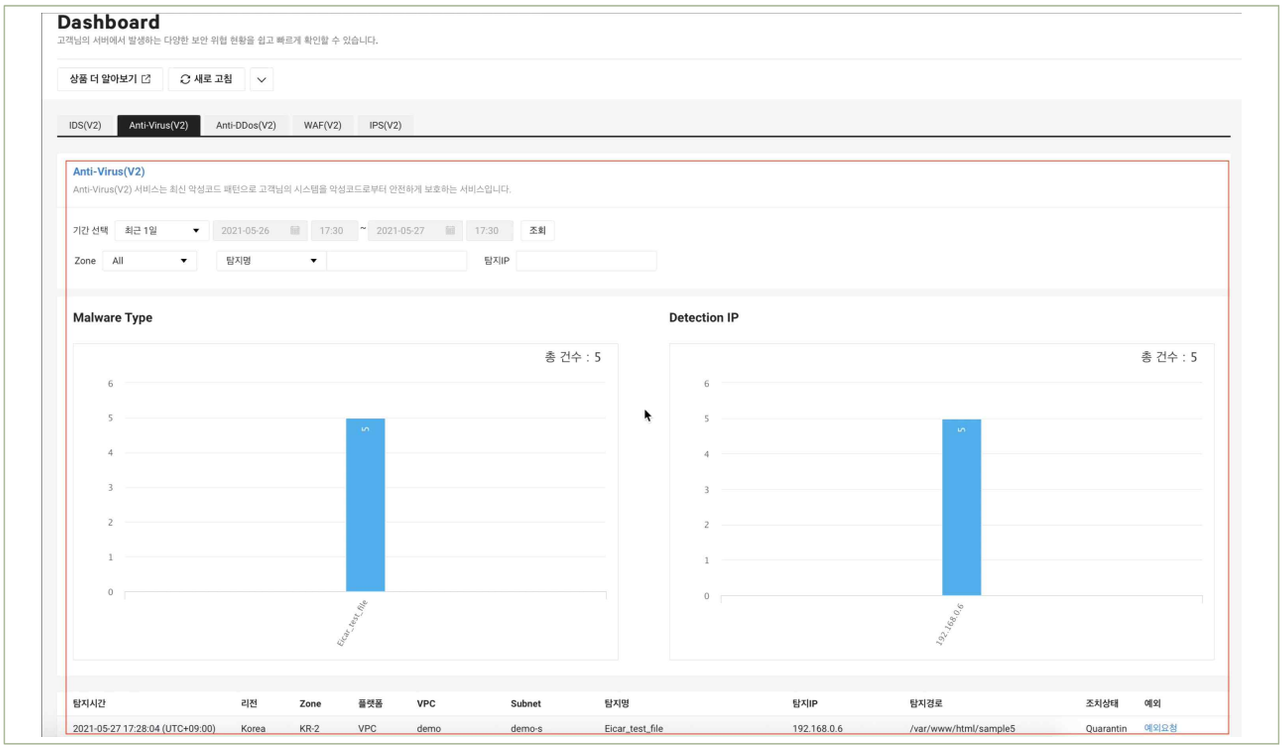
| 그림 1-7-2 | Security Monitoring 상품 선택

② **(네이버 클라우드 플랫폼 포털)** 상세 서비스 신청을 위해 '고객지원' → '자료' → 'Security Monitoring 서비스 신청서'를 다운받아 신청서를 작성합니다. 작성이 완료된 신청서는 네이버 클라우드 플랫폼 포털의 '고객지원' → '문의하기'를 통해 제출합니다.



| 그림 1-7-3 | Security Monitoring 상세 서비스 신청

③ **(가상자원관리시스템)** 신청서를 통해 지정한 가상자원(Server)에 대해 Anti-Virus 설치 완료 이후 '가상자원관리시스템'의 Security Monitoring 콘솔에서 Anti-Virus 상품 현황을 확인합니다.



| 그림 1-7-4 | Anti-Virus 현황 예시

4 참고 사항

- [참고1] Anti-Virus Agent 설치 및 운영 가이드
- [참고2] Security Monitoring 사용 가이드
- [참고3] Security Monitoring 상품 사용 신청서

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

3 우수 사례

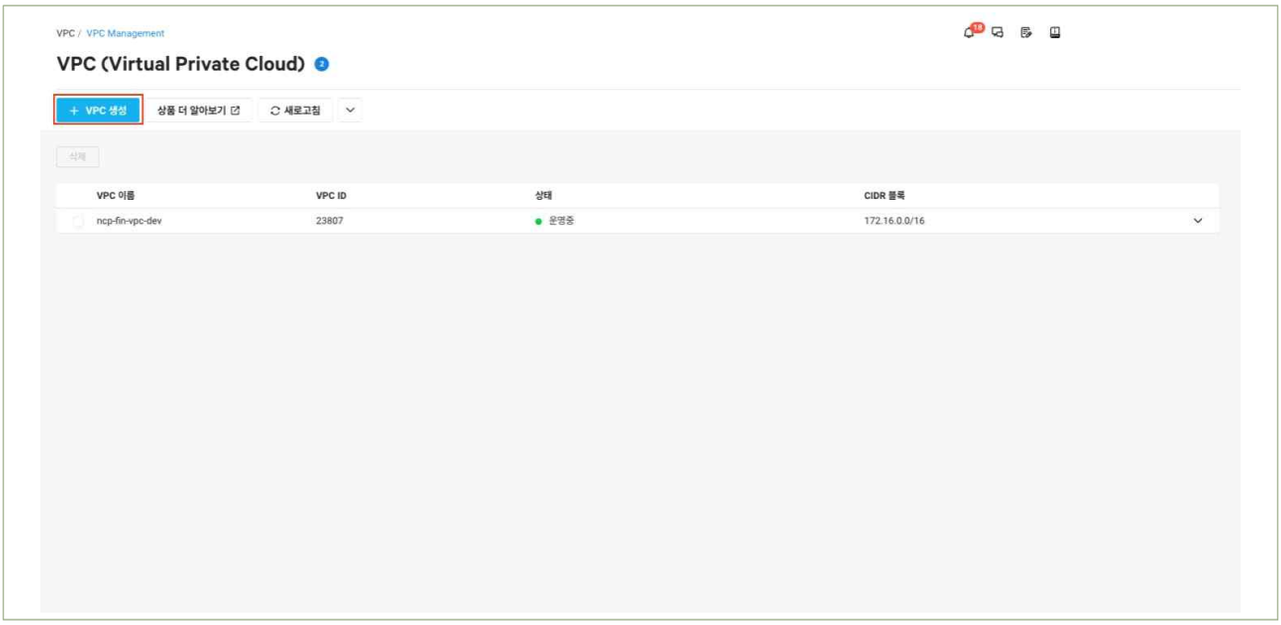
- 네이버 클라우드 플랫폼 환경에서 개발, 운영, 업무 등 업무 목적에 따른 네트워크 분리는 메인계정 분리, 계정 내 VPC 분리 등과 같이 여러가지 방안이 존재하며, 사용자는 정보처리시스템의 형태를 고려하여 적절한 네트워크 구성 방안을 선택하여야 합니다. 계정 내 VPC 분리를 통해 개발, 운영, 업무용도의 VPC를 분리하는 경우, VPC는 다른 VPC 네트워크와 논리적으로 분리되어 있으므로 안전한 네트워크를 구현할 수 있습니다.

VPC 분리를 통한 네트워크 구성

① **(가상자원관리시스템)** ‘Services’ → ‘VPC’ 상품을 선택합니다.

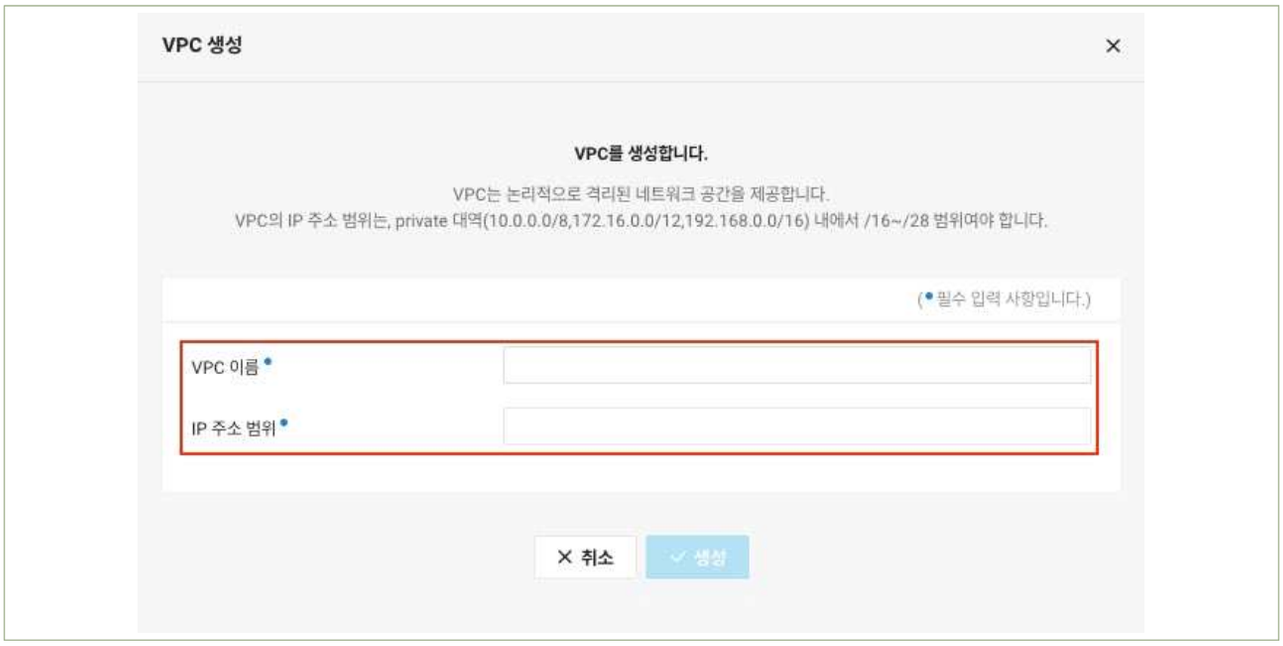
| 그림 2-1-1 | VPC 상품 선택

② **(가상자원관리시스템)** ‘VPC Management’ → ‘+ VPC 생성’을 클릭합니다.



| 그림 2-1-2 | VPC 관리 콘솔

③ **(가상자원관리시스템)** ‘VPC 이름’, ‘IP 주소 범위’를 입력하고 생성 버튼을 클릭하여 신규 VPC를 생성합니다.



| 그림 2-1-3 | 신규 VPC 생성

④ **(가상자원관리시스템)** 위 ①~③의 절차를 반복하여 다음과 같이 운영, 개발 네트워크 분리를 위한 VPC를 구성합니다.

| 그림 2-1-4 | 운영 및 개발 VPC 분리 예시

API를 통한 네트워크 분리 구성

① **(API(CLI))** ‘createVpc’ API를 통해 운영, 개발 VPC를 각각 생성하여 네트워크 분리 및 접근통제를 강화합니다.

- 요청 예시

```
GET  https://fin-ncloud.apigw.fin-ntruss.com/vpc/v2/createVpc
?regionCode=FKR
&vpcName=test-***
&ipv4CidrBlock=***.***.0.0/16
```

- 응답 예시

```
<createVpcResponse>
<requestId>21a29c59-3139-4c23-9f92-10c1fddafef6</requestId>
<returnCode>0</returnCode>
<returnMessage>success</returnMessage>
<totalRows>1</totalRows>
<vpcList>
    <vpc>
      <vpcNo>***04</vpcNo>
      <vpcName>test-***</vpcName>
      <ipv4CidrBlock>***.***.0.0/16</ipv4CidrBlock>
      <vpcStatus>
        <code>INIT</code>
        <codeName>init</codeName>
      </vpcStatus>
      <regionCode>FKR</regionCode>
      <createDate>2020-07-27T17:17:05+0900</createDate>
    </vpc>
</vpcList>
</createVpcResponse>
```

| 그림 2-1-5 | 운영 및 개발 VPC 분리 예시

4 참고 사항

- [참고1] VPC 사용 가이드
- [참고2] VPC 생성 API 가이드

1 기준

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

2 설명

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

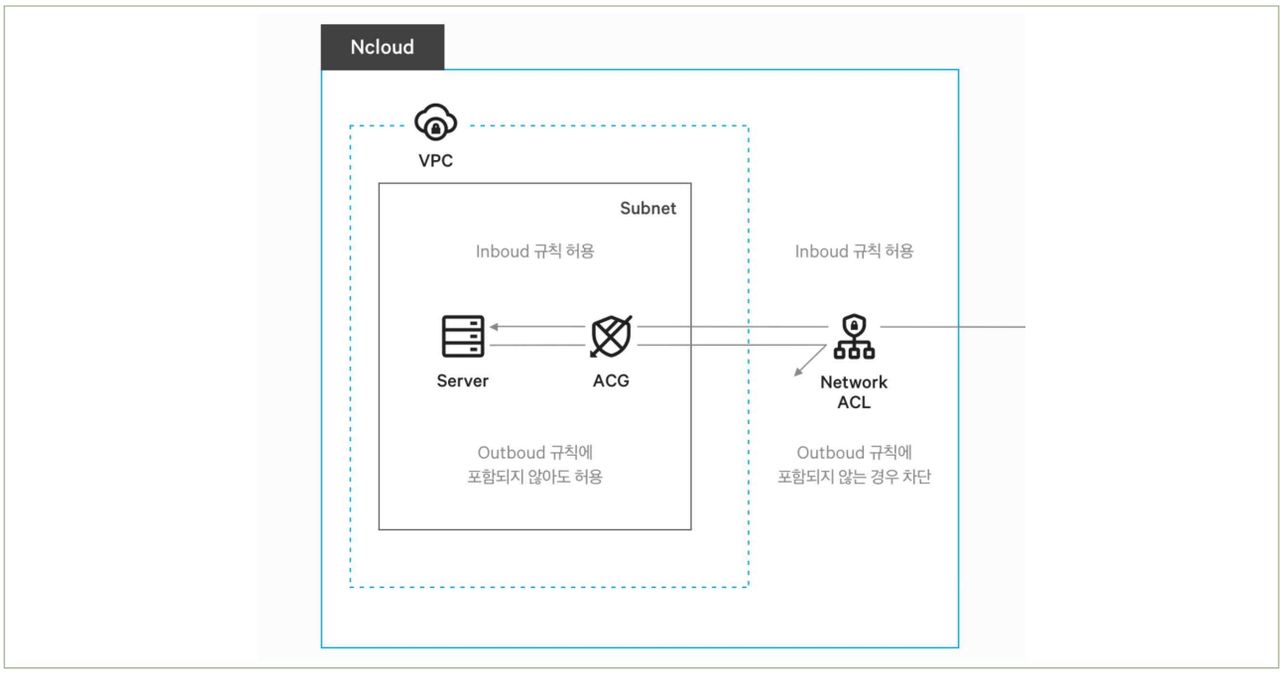
- 네이버 클라우드 플랫폼의 Server, Cloud DB 등과 같은 중요 가상자원에 대해 외부로부터의 침입, 비인가 접근 등을 제한하기 위해서 가상자원을 Private Subnet과 같이 인터넷과 연결되지 않은 안전한 네트워크 내부에 위치하도록 생성하여야 합니다.

  Server, Cloud DB를 Private Subnet에 생성하면 기본적으로 공인IP(Public IP) 등을 할당할 수 없으므로, 외부로 부터의 직접적인 접근을 제한할 수 있습니다.

  그 다음, ACG(Access Control Group)와 Network ACL을 사용하여 VPC 내부 네트워크에 대한 접근제어 규칙을 정의하여 가상자원에 대한 접근통제를 구성하여야 합니다.

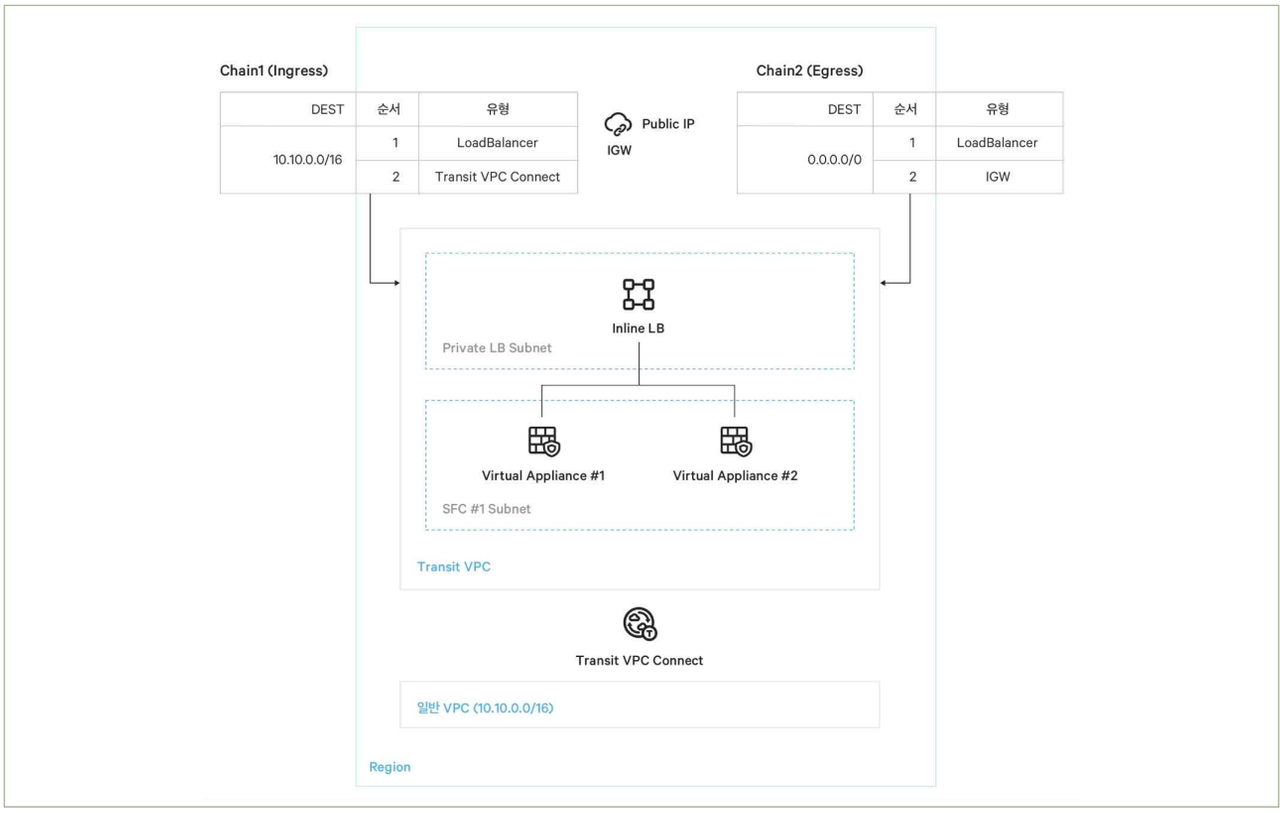
  ACG는 Inbound 및 Outbound 트래픽에 허용 규칙을 설정하여 서버의 트래픽을 제어하며, Network ACL은 Subnet 레벨에서 Inbound 및 Outbound 트래픽에 대하여 허용 또는 차단 규칙을 적용할 수 있습니다. Network ACL을 이용하여 각 Subnet을 독립적인 네트워크로 구분 짓고, Subnet 내 통신의 보안은 ACG로 제어함으로써 강력한 네트워크 보안체계를 구성할 수 있습니다.

ACG는 “stateful”, Network ACL은 “Stateless” 방식으로 각각 동작합니다. Stateful은 트래픽 상태를 저장한다는 의미로 Inbound 규칙에 의해 허용된 트래픽은 Outbound 규칙에 상관없이 응답할 수 있습니다. 반면에 Stateless 방식은 트래픽 상태를 저장하고 있지 않으므로 Inbound 규칙에 의해 허용된 트래픽의 응답도 Outbound 규칙에 의해 필터링됩니다. 따라서, Network ACL 규칙 설정은 각별한 주의와 충분한 검증 테스트가 요구됩니다.



| 그림 2-2-1 | 네트워크 보호를 위한 ACG와 Network ACL의 예시

위와 같이 ACG 및 Network ACL을 통한 방법 외에도 VPC 상품의 Service Function Chain을 통해 네트워크 또는 보안 장비 전문 업체가 제작한 가상 어플라이언스 이미지(IPS, NGFW, TMS(통합보안관리) 등)를 Transit VPC에 네트워크 인라인 형태로 구성하여 보다 강력한 네트워크 보안 통제를 구현할 수 있습니다. 또한, 다수의 VPC를 운영중인 경우에도 Service Function Chain을 활용하면 복수의 VPC에 대하여 중앙화된 접근제어 관리체계를 구성할 수도 있습니다.



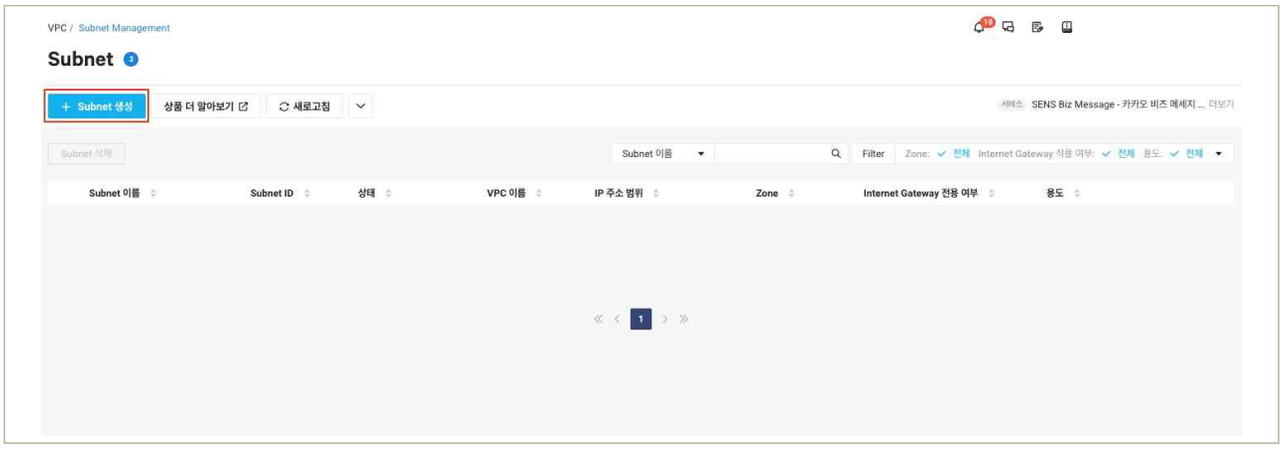
| 그림 2-2-2 | Service Function Chain 구성 예시

Private Subnet 구성을 통한 인터넷망 접근 제한

① **(가상자원관리시스템)** 'Services' → 'VPC' 상품을 선택합니다.

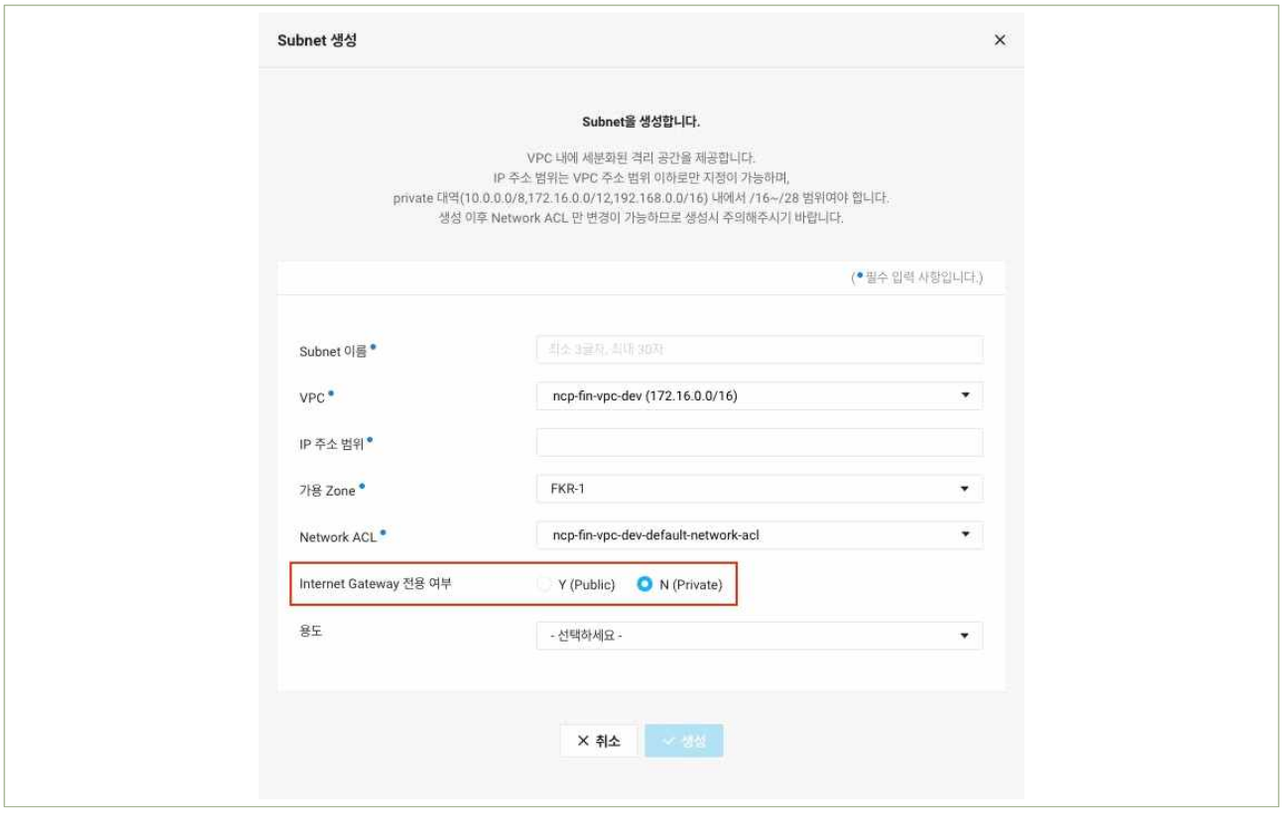
| 그림 2-2-3 | VPC 상품 선택

② **(가상자원관리시스템)** ‘Subnet Management’ → ‘+ Subnet 생성’을 클릭합니다.



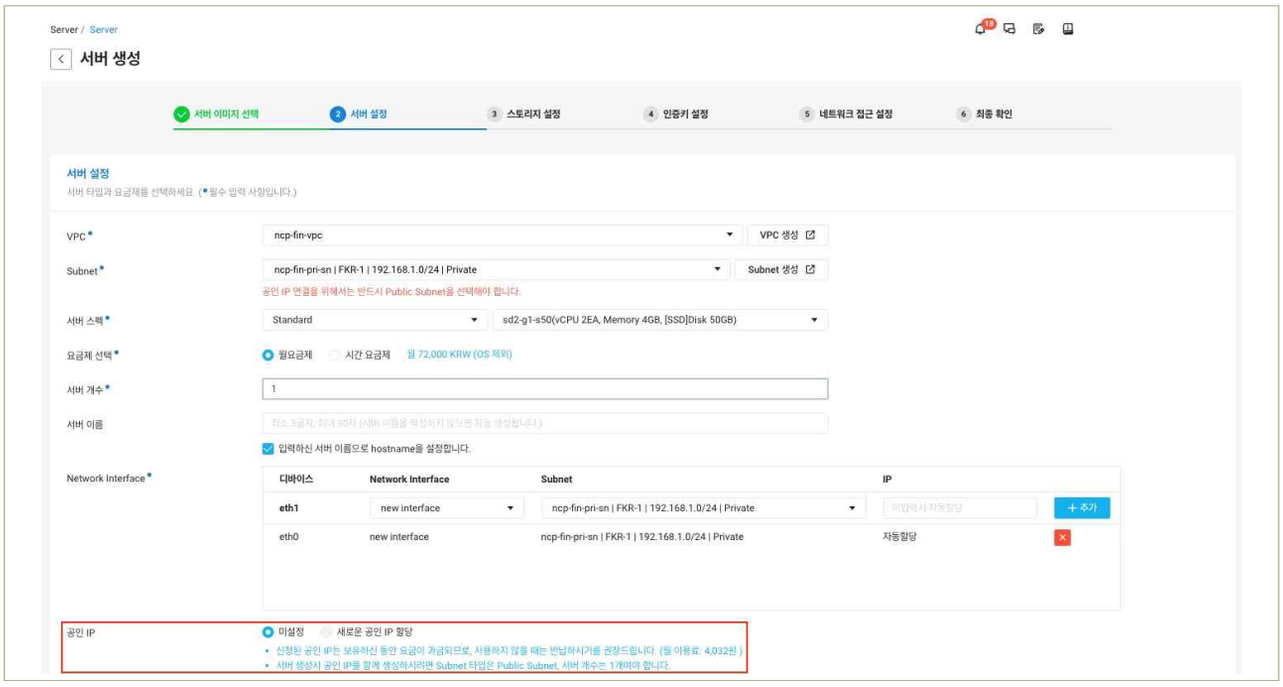
| 그림 2-2-4 | Subnet 관리 콘솔

③ **(가상자원관리시스템)** ‘Internet Gateway 전용 여부’ 라디오 버튼에서 ‘N (Private)’을 클릭하여 Private Subnet을 생성합니다.

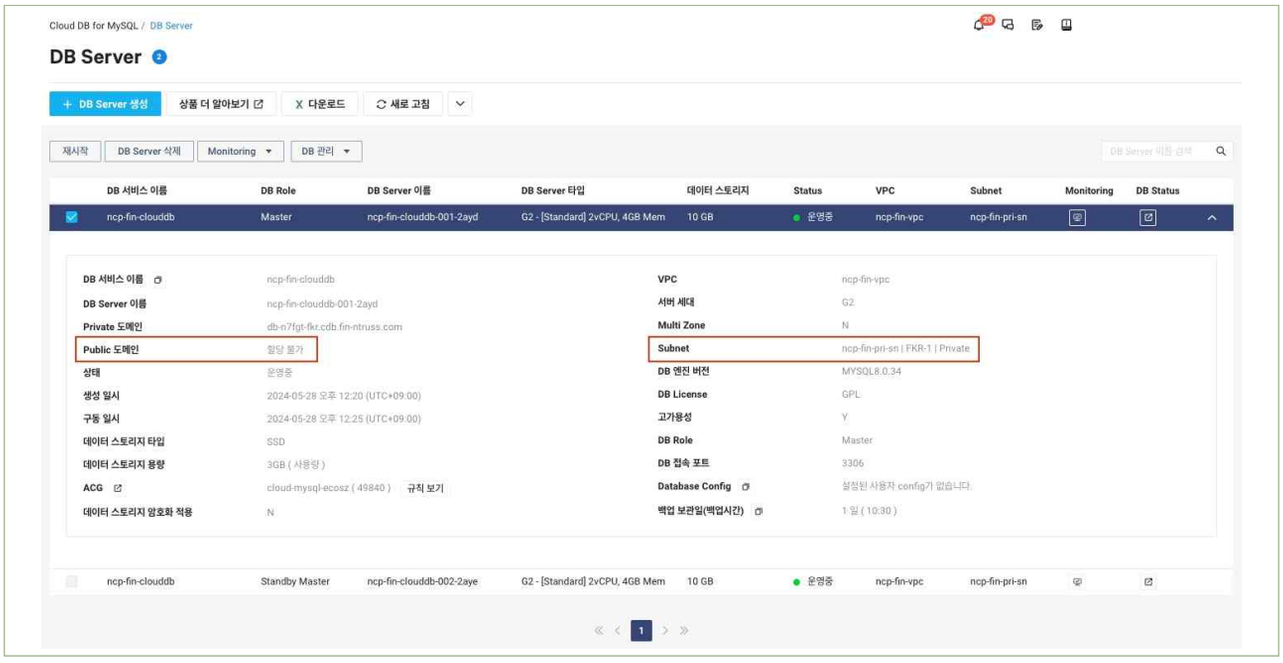


| 그림 2-2-5 | Private Subnet 생성

④ **(가상자원관리시스템)** 'Internet Gateway 전용 여부' 라디오 버튼에서 'N (Private)'을 클릭하여 Private Subnet을 생성합니다. 가상자원(Server, Cloud DB 등)을 Private Subnet에 생성하게 되면, 다음과 같이 가상자원에 공인 IP 설정이 불가합니다.



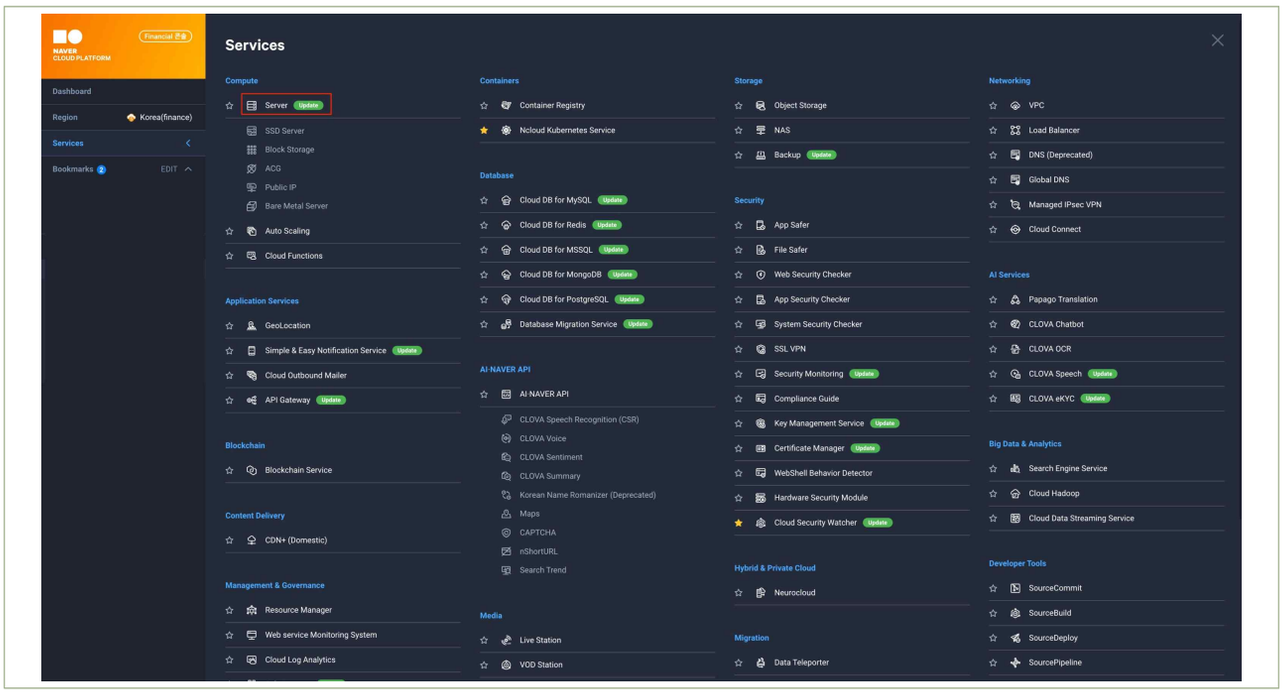
| 그림 2-2-6 | Server의 공인 IP 할당불가 예시



| 그림 2-2-7 | Cloud DB의 공인 IP 할당불가 예시

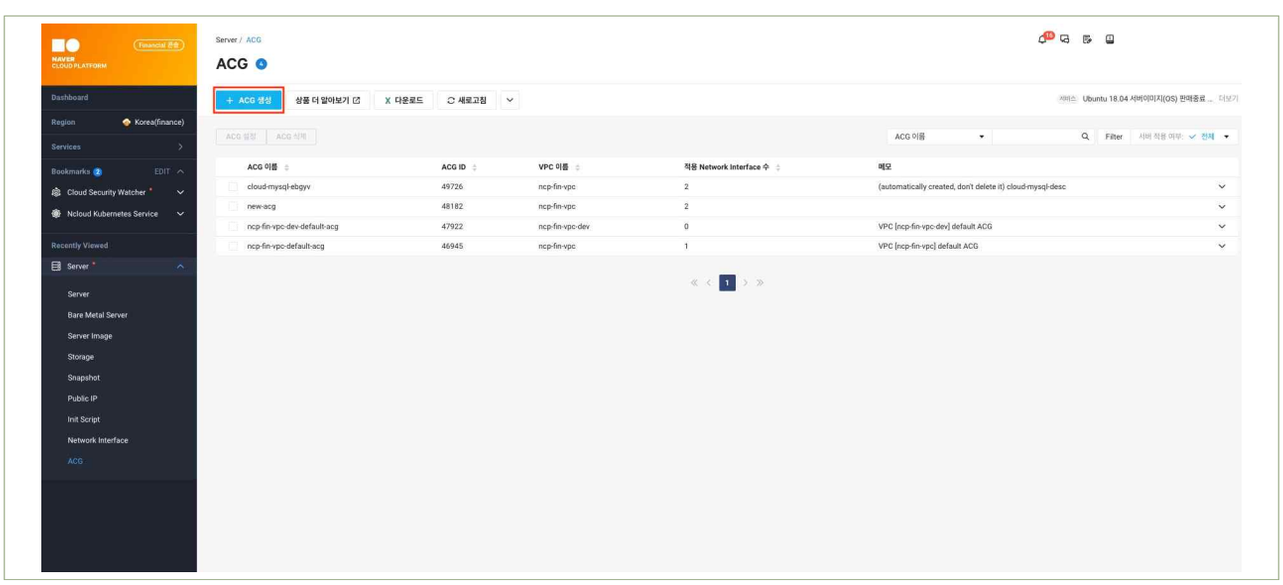
ACG(Access Control Group)을 통한 접근 통제

① **(가상자원관리시스템)** ‘Services’ → ‘Server’ 상품을 선택합니다.



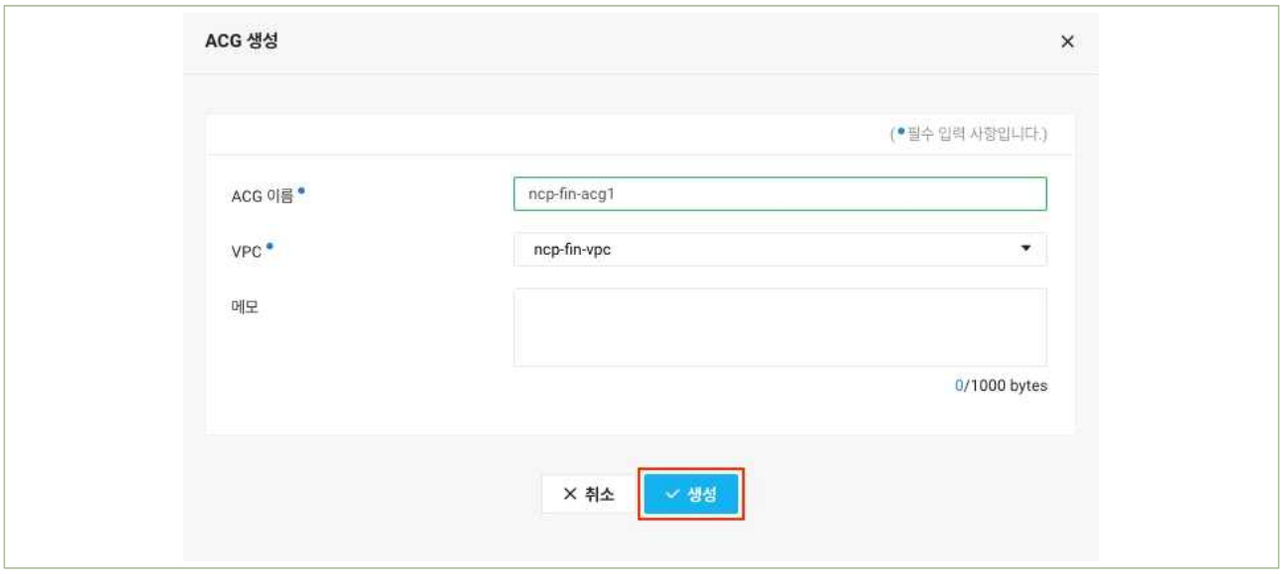
| 그림 2-2-8 | Server 상품 선택

② **(가상자원관리시스템)** ‘ACG’ → ‘+ ACG 생성’을 클릭합니다.



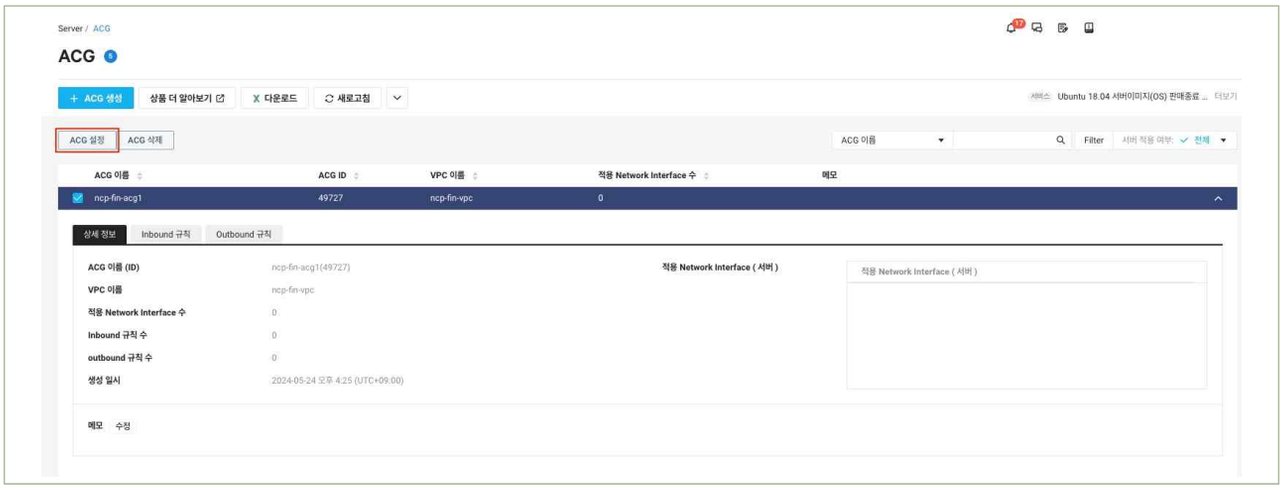
| 그림 2-2-9 | Server의 ACG 생성

③ **(가상자원관리시스템)** ACG 생성을 위해 'ACG 이름'과 '대상 VPC'를 선택하고 '생성'버튼을 클릭합니다.



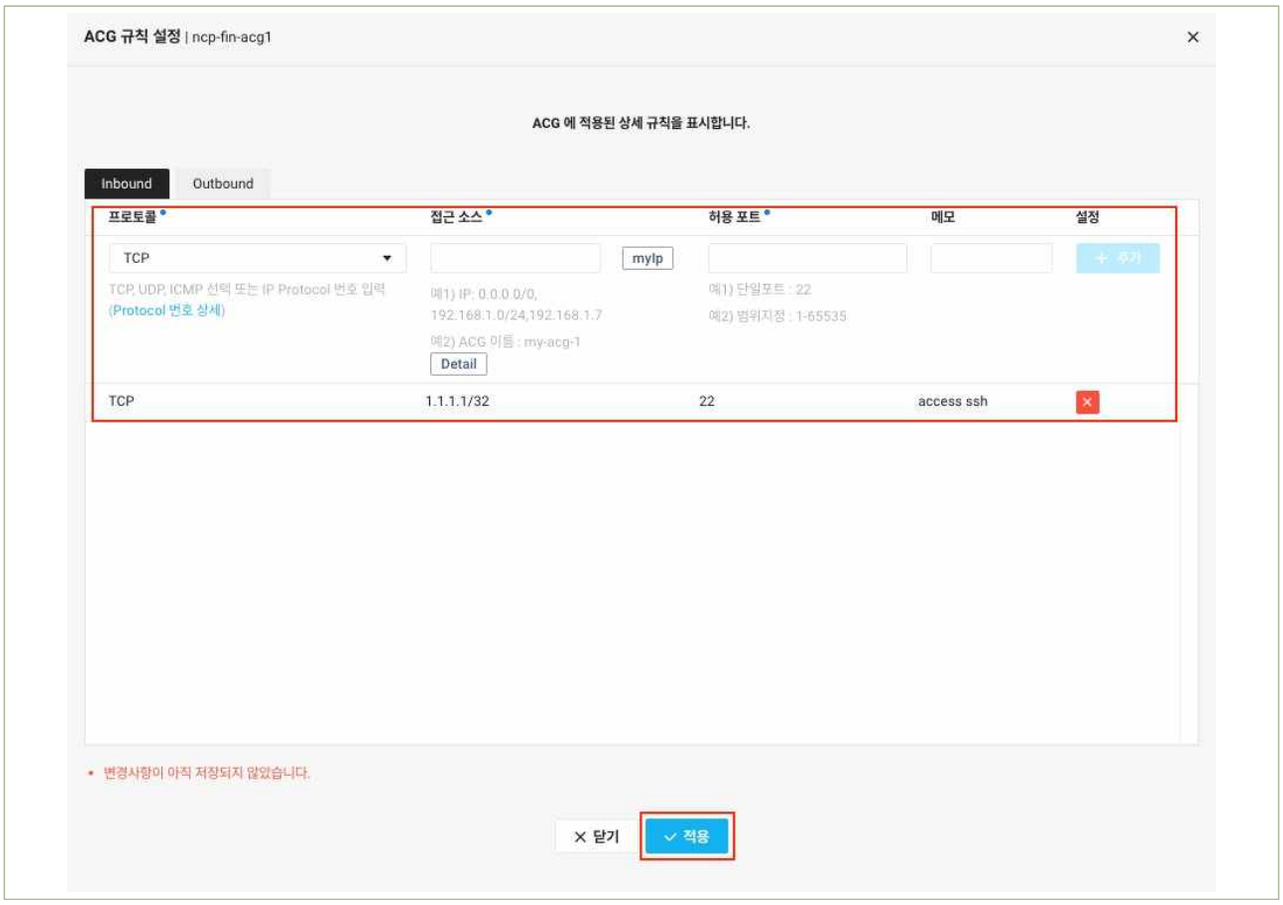
| 그림 2-2-10 | ACG 생성 대상 VPC 선택

④ **(가상자원관리시스템)** 신규 생성된 ACG를 선택하고 'ACG 설정' 버튼을 클릭합니다.



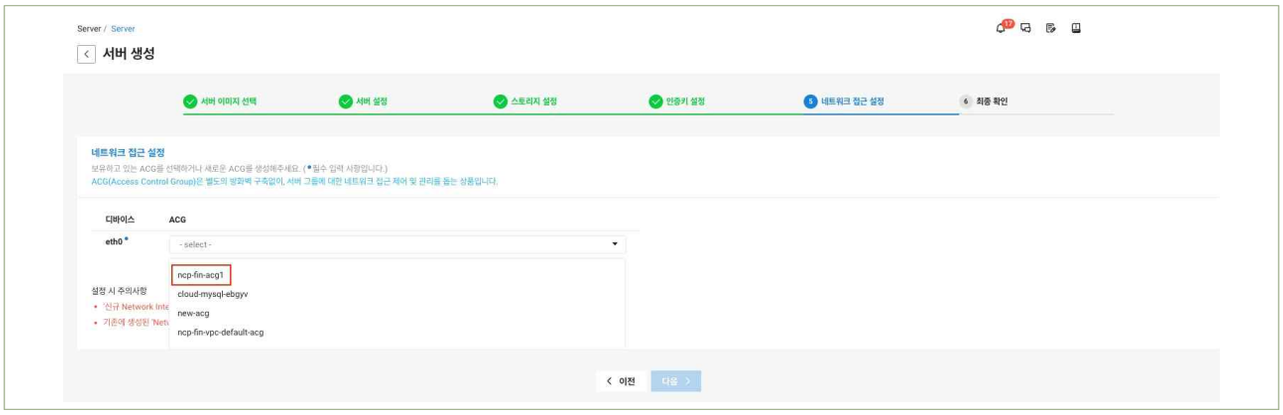
| 그림 2-2-11 | ACG 설정

⑤ **(가상자원관리시스템)** ‘프로토콜’, ‘접근 소스’, ‘허용 포트’ 등을 입력 후, ‘+ 추가’ 버튼을 클릭하여 Inbound 규칙을 정의하고, ‘적용’버튼을 클릭하여 ACG 설정을 완료합니다.



| 그림 2-2-12 | ACG Inbound 규칙 정의 및 적용

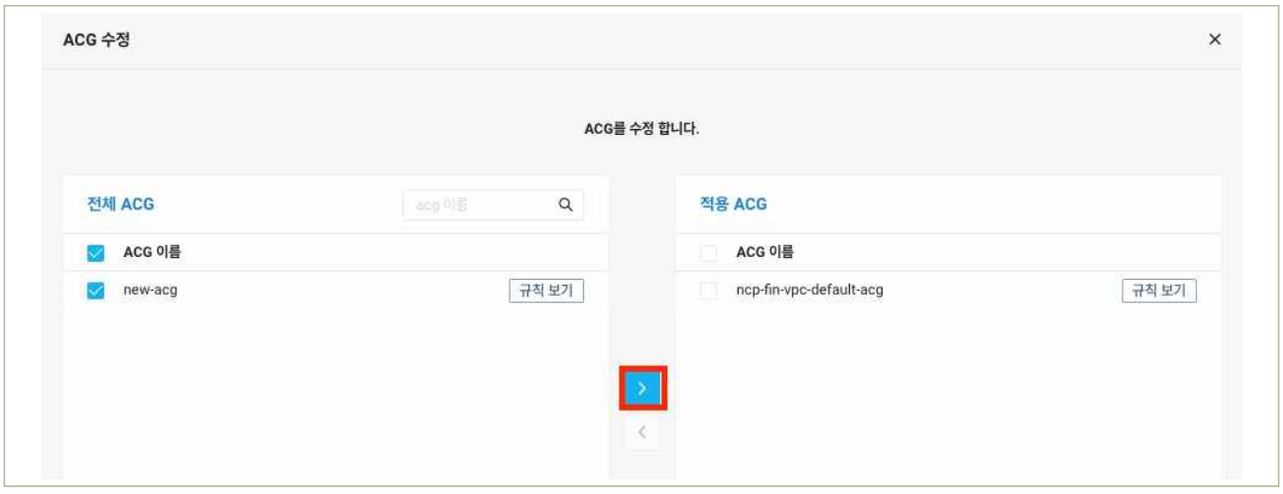
⑥ **(가상자원관리시스템)** ‘Services’ → ‘Server’ → ‘Server’ → ‘+ 서버 생성’을 통해 서버를 생성하는 단계 중, ‘네트워크 접근 설정’ 단계에서 사전에 정의한 ACG를 선택하여 가상자원(Server)에 대해 접근제어를 적용합니다.



| 그림 2-2-13 | 가상자원(Server)의 접근제어 적용

⑦ **(가상자원관리시스템)** ‘Services’ → ‘Server’ → ‘대상 Server 선택’ → ‘ACG 수정’을 통해 운영중인 Server 인스턴스에 대해서도 ACG 변경 또는 추가로 ACG를 연결할 수 있습니다.

| 그림 2-2-14 | ACG 수정/변경 예시 1



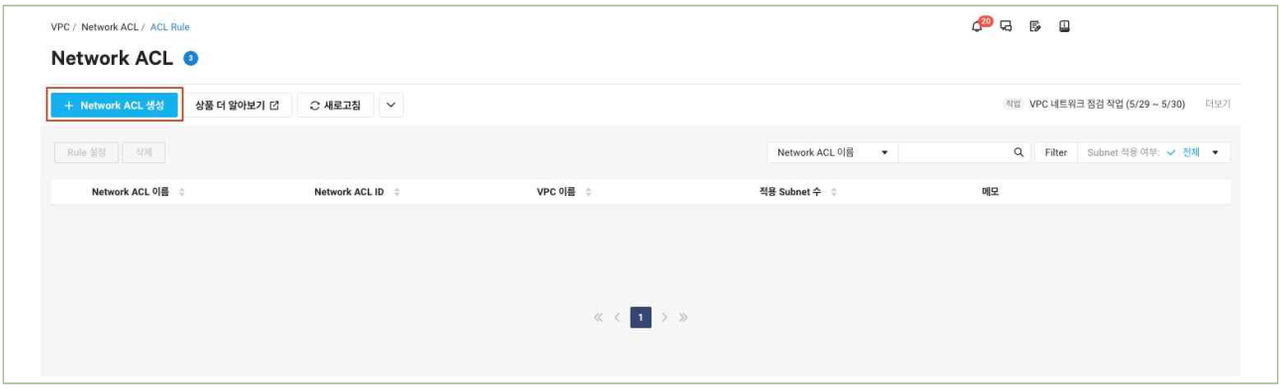
| 그림 2-2-15 | ACG 수정/변경 예시 2

NACL(Network Access Control List)을 통한 접근 통제

① **(가상자원관리시스템)** ‘Services’ → ‘VPC’ 상품을 선택합니다.

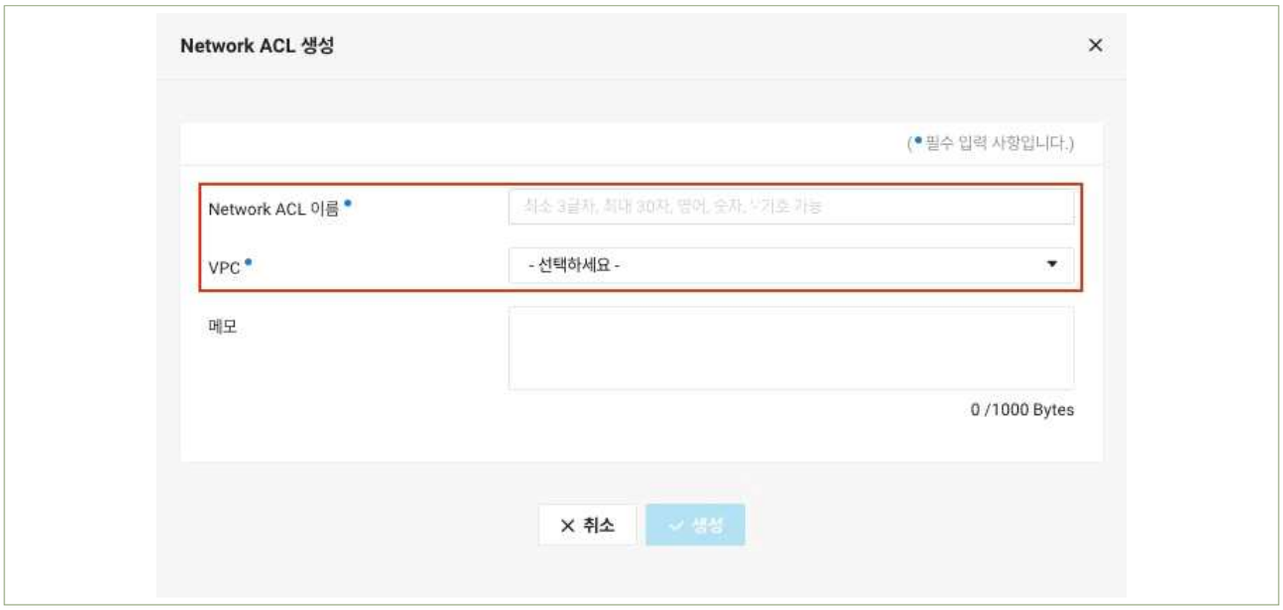
| 그림 2-2-16 | VPC 상품 선택

② **(가상자원관리시스템)** ‘Network ACL’ → ‘ACL Rule’ → ‘+ Network ACL 생성’을 클릭합니다.



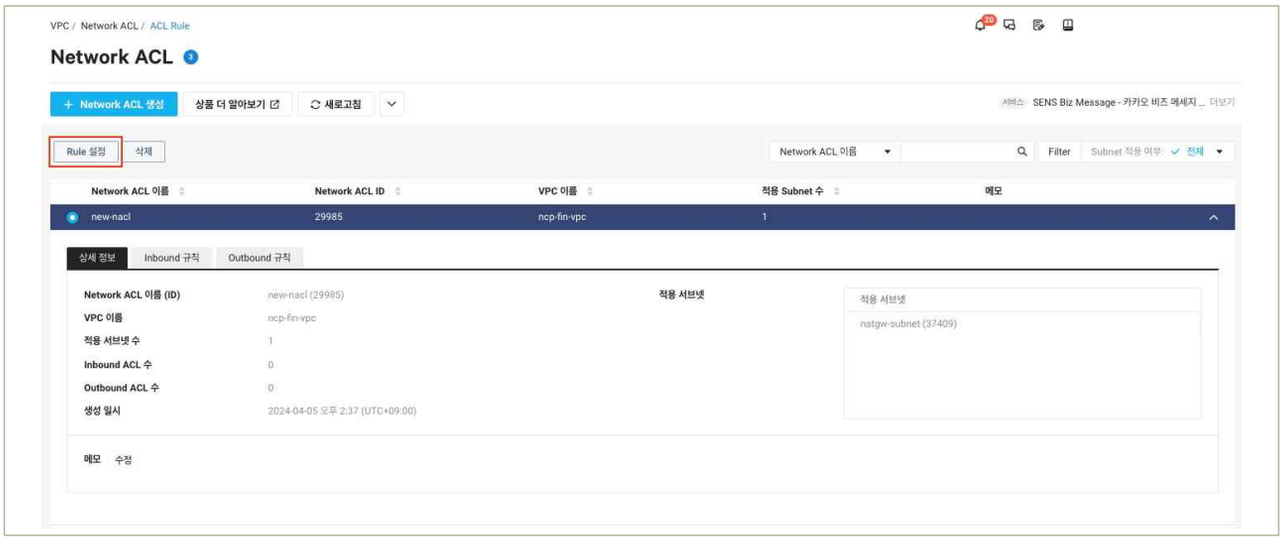
| 그림 2-2-17 | NACL 관리 콘솔

③ **(가상자원관리시스템)** ‘Network ACL 이름’, ‘VPC’을 입력하고 생성 버튼을 클릭합니다.



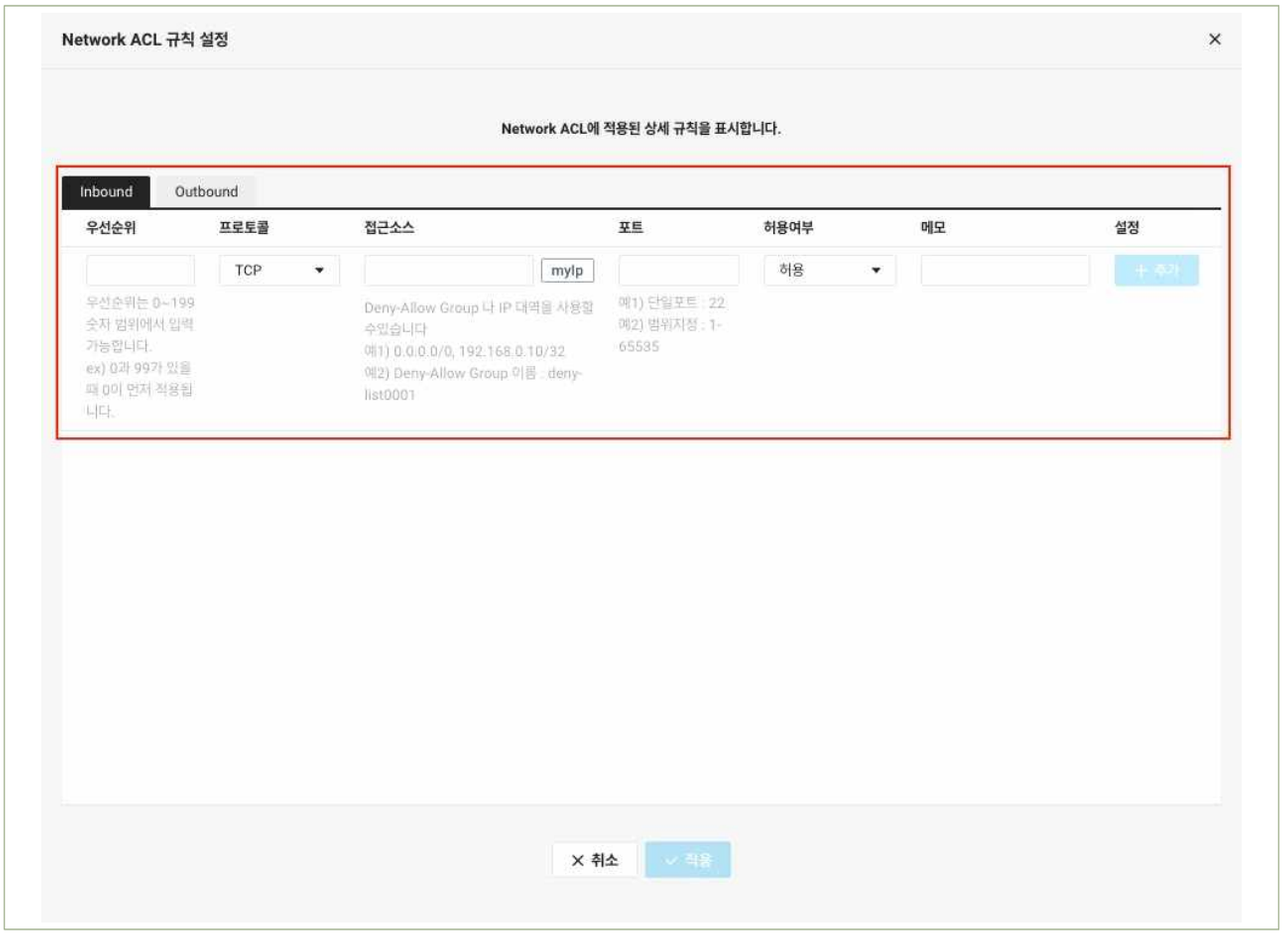
| 그림 2-2-18 | 신규 NACL 생성

④ **(가상자원관리시스템)** ‘Network ACL’ → ‘ACL Rule’ → ‘NCAL 선택’ → ‘Rule 설정’을 클릭합니다.



| 그림 2-2-19 | 신규 NACL의 Rule 설정

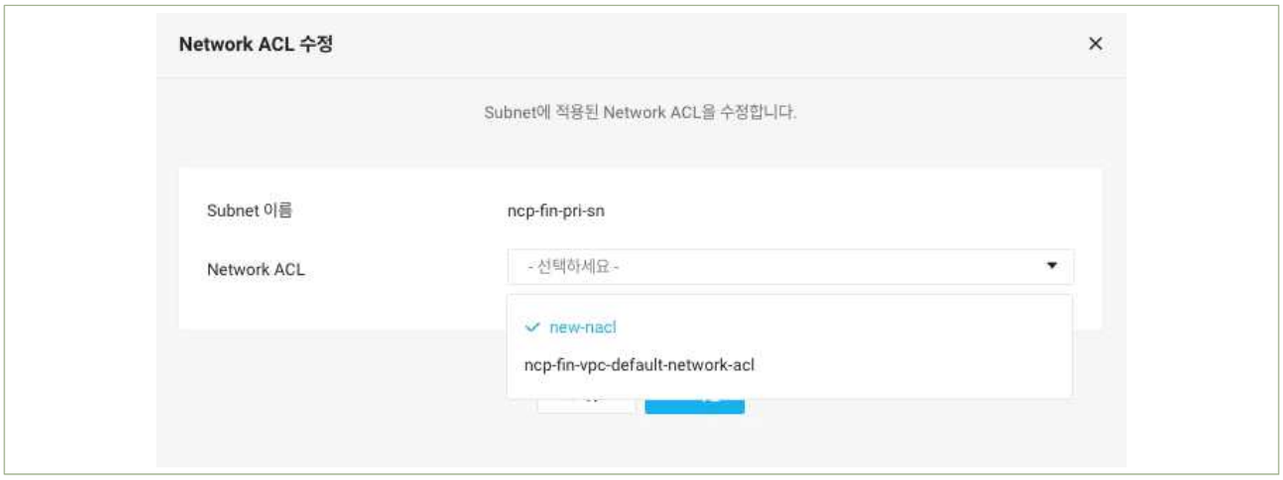
⑤ **(가상자원관리시스템)** ‘우선순위’, ‘프로토콜’, ‘접근소스’, ‘포트’, ‘허용여부’ 항목을 입력/선택하여 규칙을 추가하고, 적용 버튼을 클릭하여 NACL에 대한 상세 접근제어 규칙을 구성합니다.



| 그림 2-2-20 | 신규 NACL의 상세 규칙 설정

⑥ **(가상자원관리시스템)** ‘Services’ → ‘VPC’ → ‘Subnet Management’ → ‘대상 Network ACL 선택’→ ‘Network ACL 변경’을 통해 운영중인 Subnet에 대해서도 Network ACL을 변경할 수 있습니다.

| 그림 2-2-21 | Network ACL 변경 예시 1



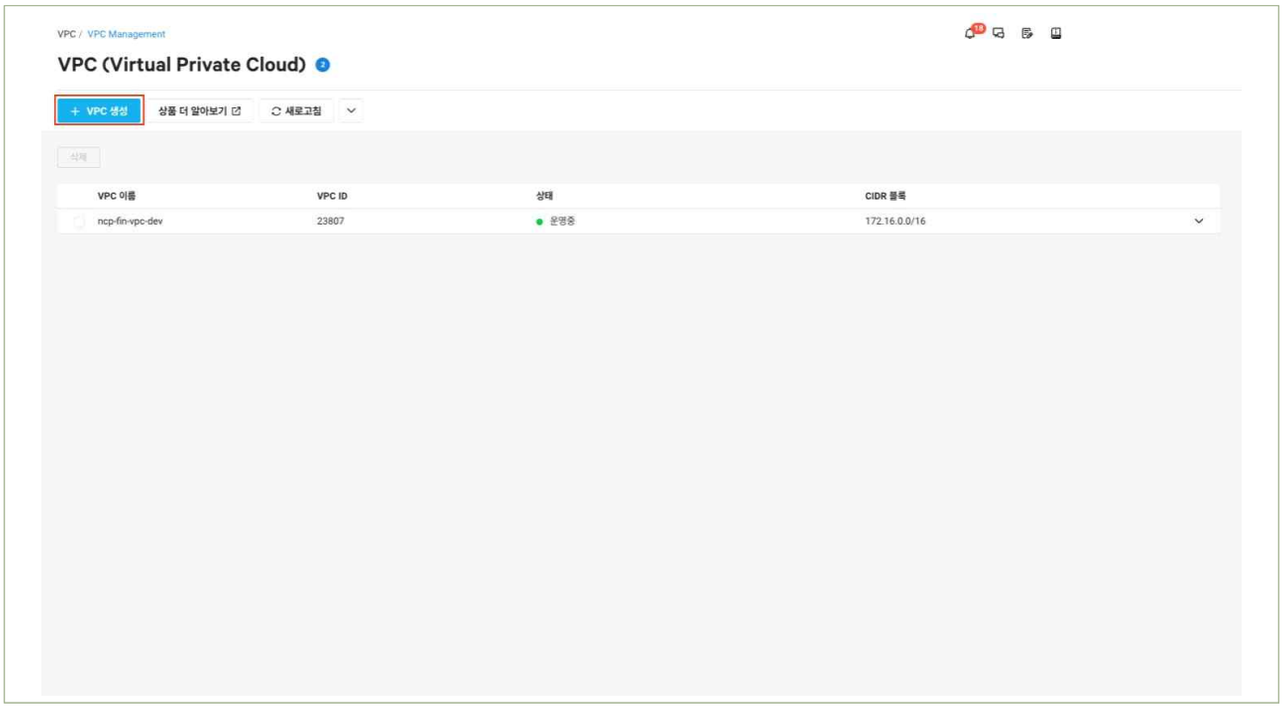
| 그림 2-2-22 | Network ACL 변경 예시 2

Service Function Chain을 통한 네트워크 보안 통제

① **(가상자원관리시스템)** 'Services' → 'VPC' 상품을 선택합니다.

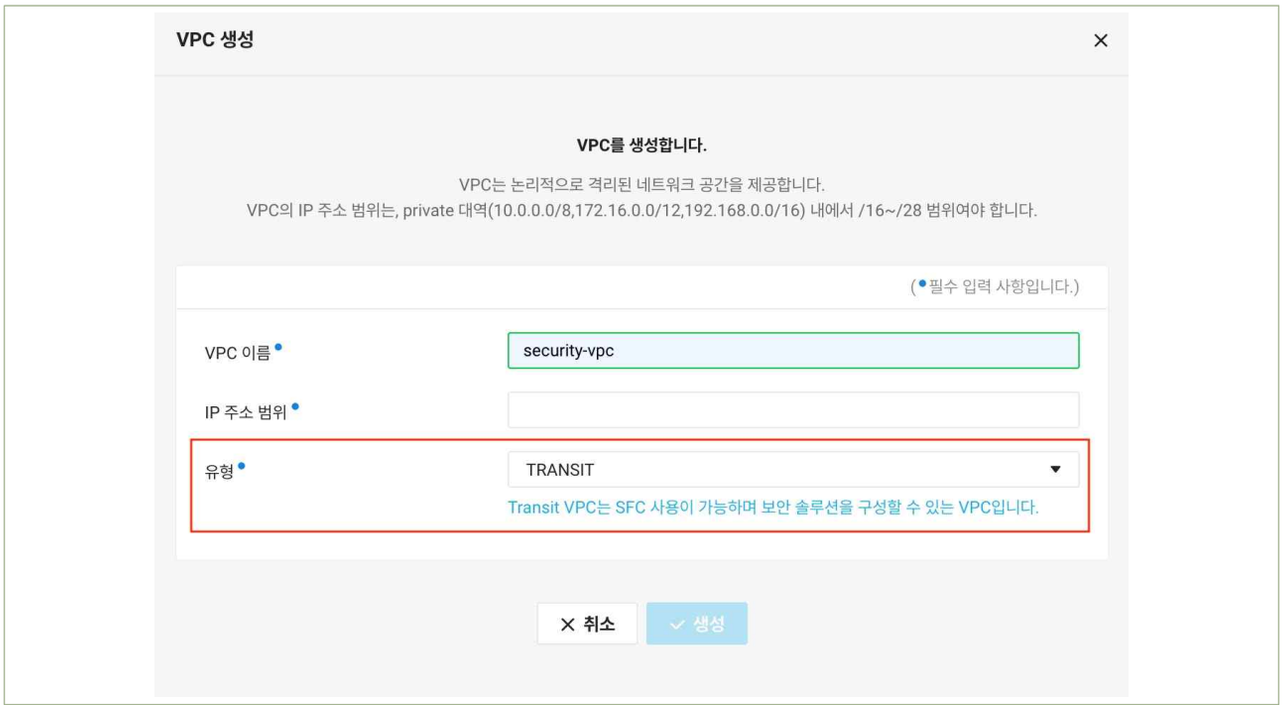
| 그림 2-2-23 | VPC 상품 선택

② **(가상자원관리시스템)** ‘VPC Management’ → ‘+ VPC 생성’을 클릭합니다.



| 그림 2-2-24 | Transit VPC 생성

③ **(가상자원관리시스템)** ‘VPC 이름’, ‘IP 주소 범위’를 입력하고 ‘TRANSIT’ 유형을 선택하여 Transit VPC를 생성합니다.

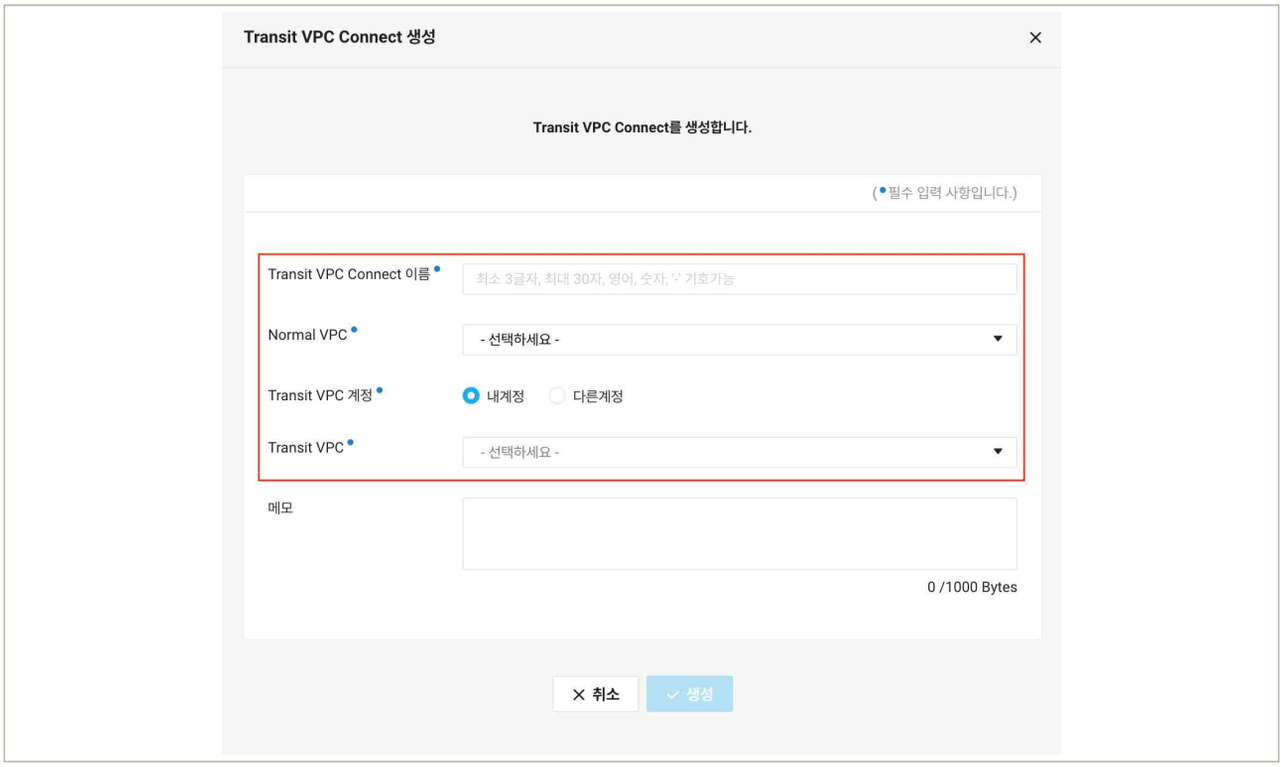


| 그림 2-2-25 | Transit VPC 생성

④ **(가상자원관리시스템)** ‘Services’ → ‘VPC’ → ‘Transit VPC Connect’→ ‘+ Transit VPC Connect 생성’을 클릭합니다.

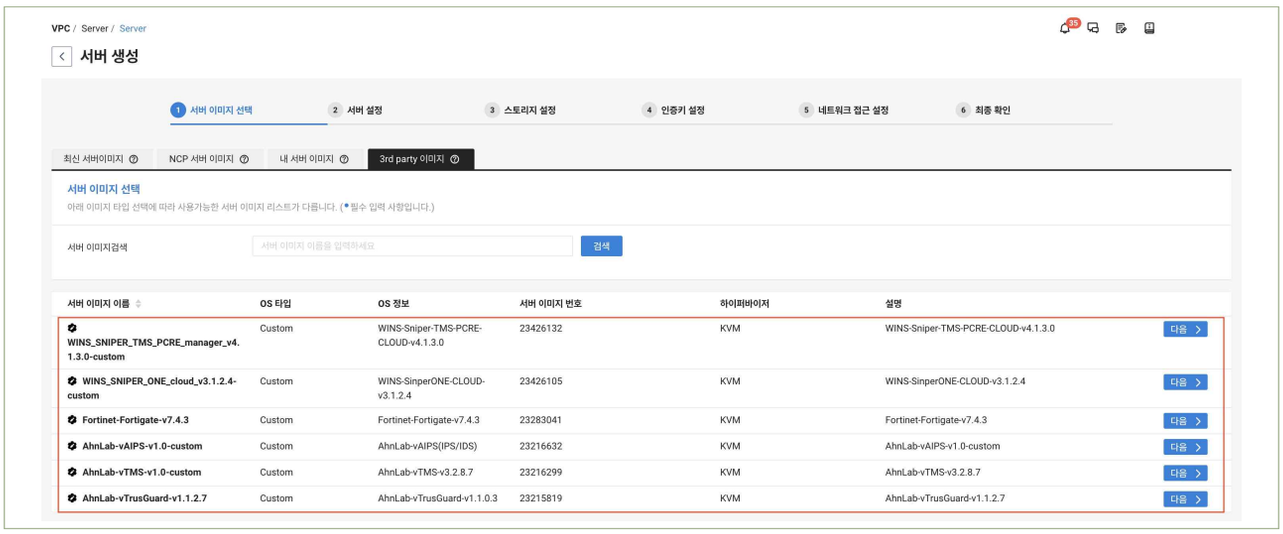
| 그림 2-2-26 | Transit VPC Connect 생성

⑤ **(가상자원관리시스템)** 생성된 Transit VPC와 서비스 VPC를 선택하여 VPC를 연결합니다.



| 그림 2-2-27 | Transit VPC Connect 생성

⑥ **(가상자원관리시스템)** ‘Services’ → ‘Server’ → ‘+ 서버 생성’을 통한 서버 생성 이미지 선택 단계에서 ‘3rd Party 이미지’ 탭을 클릭하고 원하는 가상 어플라이언스 이미지를 Transit VPC에 생성합니다.

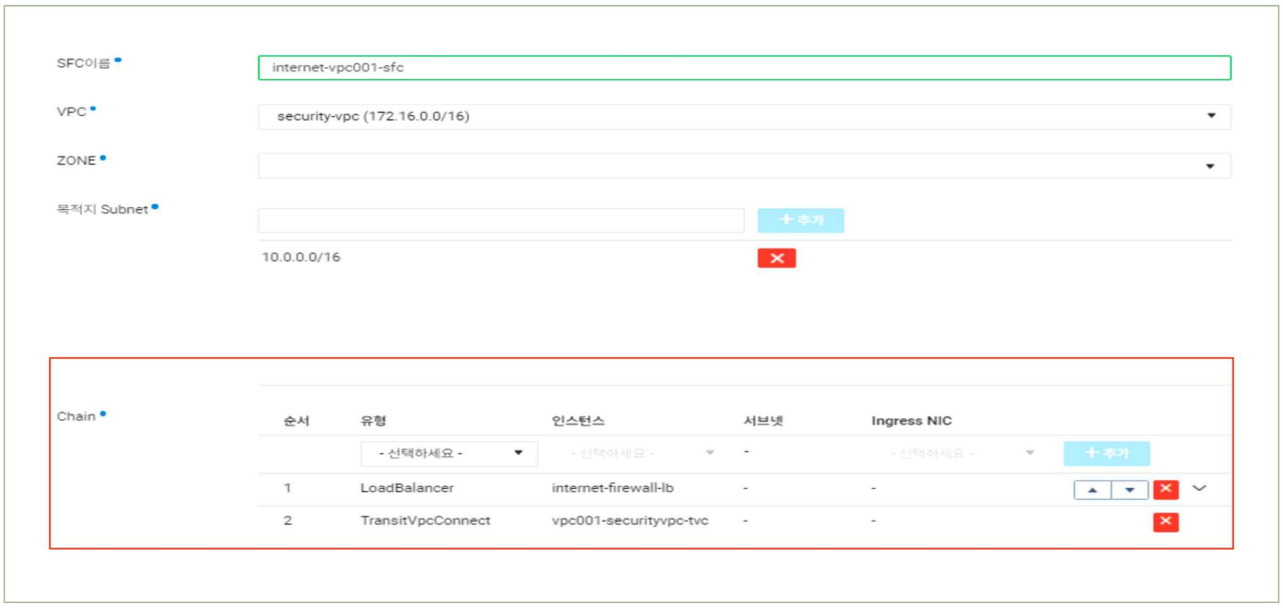


| 그림 2-2-28 | 3rd Party 이미지 선택

⑦ **(가상자원관리시스템)** ‘Services’ → ‘VPC’ → ‘Service Function Chain’ → ‘+ Service Function Chain 생성’을 클릭합니다.

| 그림 2-2-29 | Service Function Chain 생성

⑧ **(가상자원관리시스템)** Transit VPC 내 보안 어플라이언스로 인입된 네트워크 트래픽이 Transit VPC Connect를 통해 서비스 VPC로 전달될 수 있도록 Chain을 구성합니다.



| 그림 2-2-30 | Service Function Chain 생성

※ Service Function Chain은 네이버 클라우드 플랫폼의 민간/공공 클라우드를 통해 사용하실 수 있습니다.
※ 네이버 클라우드 플랫폼의 '민간 클라우드'는 기존 '금융 클라우드'와 같이 금융보안원의 CSP 안전성평가를 완료하여 금융 회사, 전자금융업자도 안심하고 사용할 수 있습니다.
※ 위의 Service Function Chain구성 절차에는 상세 설정 등의 내용이 생략되어 있습니다. Service Function Chain 구성을 위한 보다 자세한 절차 및 내용은 아래 참고 사항의 링크를 통해 확인하여 주시기 바랍니다.

ACG(Access Control Group) API를 통한 접근 통제

① **(API(CLI))** 'createAccessControlGroup' API를 통해 신규 ACG를 생성하고, 운영, 개발 VPC를 각각 생성하여 네트워크 분리와 접근통제를 강화합니다.

- 요청 예시

```
GET https://fin-ncloud.apigw.fin-ntruss.com/vserver/v2/createAccessControlGroup
?regionCode=FKR
&vpcNo=***04
&accessControlGroupName=test-***
```

- 응답 예시

```
<createAccessControlGroupResponse>
<requestId>cf08459a-2f8e-4a73-9b1c-cc31d74466ae</requestId>
<returnCode>0</returnCode>
<returnMessage>success</returnMessage>
<totalRows>1</totalRows>
<accessControlGroupList>
    <accessControlGroup>
      <accessControlGroupNo>***63</accessControlGroupNo>
      <accessControlGroupName>test-***</accessControlGroupName>
      <isDefault>false</isDefault>
      <vpcNo>***04</vpcNo>
      <accessControlGroupStatus>
        <code>RUN</code>
        <codeName>run</codeName>
      </accessControlGroupStatus>
      <accessControlGroupDescription></accessControlGroupDescription>
    </accessControlGroup>
</accessControlGroupList>
</createAccessControlGroupResponse>
</vpcList>
</createVpcResponse>
```

| 그림 2-2-31 | API를 통한 ACG 생성

- **NACL(Network Access Control List) API를 통한 접근 통제**

① **(API(CLI))** 'createNetworkAcl' API를 통해 신규 Network ACL을 생성합니다.

- 요청 예시

```
GET https://fin-ncloud.apigw.fin-ntruss.com/vpc/v2//vpc/v2/createNetworkAcl
?regionCode=FKR
&vpcNo=***04
&networkAclName=test-***
```

- 응답 예시

```
<createNetworkAclResponse>
<requestId>2828ed65-e3ad-48ef-ac80-ca2e31c33544</requestId>
<returnCode>0</returnCode>
<returnMessage>success</returnMessage>
<totalRows>1</totalRows>
<networkAclList>
    <networkAcl>
      <networkAclNo>***31</networkAclNo>
      <networkAclName>test-***</networkAclName>
      <vpcNo>***04</vpcNo>
      <networkAclStatus>
        <code>RUN</code>
        <codeName>run</codeName>
      </networkAclStatus>
      <networkAclDescription></networkAclDescription>
      <createDate>2020-07-31T16:38:52+0900</createDate>
      <isDefault>false</isDefault>
    </networkAcl>
</networkAclList>
</createNetworkAclResponse>
```

| 그림 2-2-32 | API를 통한 Network ACL 생성

4 참고 사항

- [참고1] ACG 사용 가이드
- [참고2] NACL 사용 가이드
- [참고3] ACG 생성 API 사용 가이드
- [참고4] NACL 생성 API 사용 가이드
- [참고5] Service Function Chain 구성 절차 가이드

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.

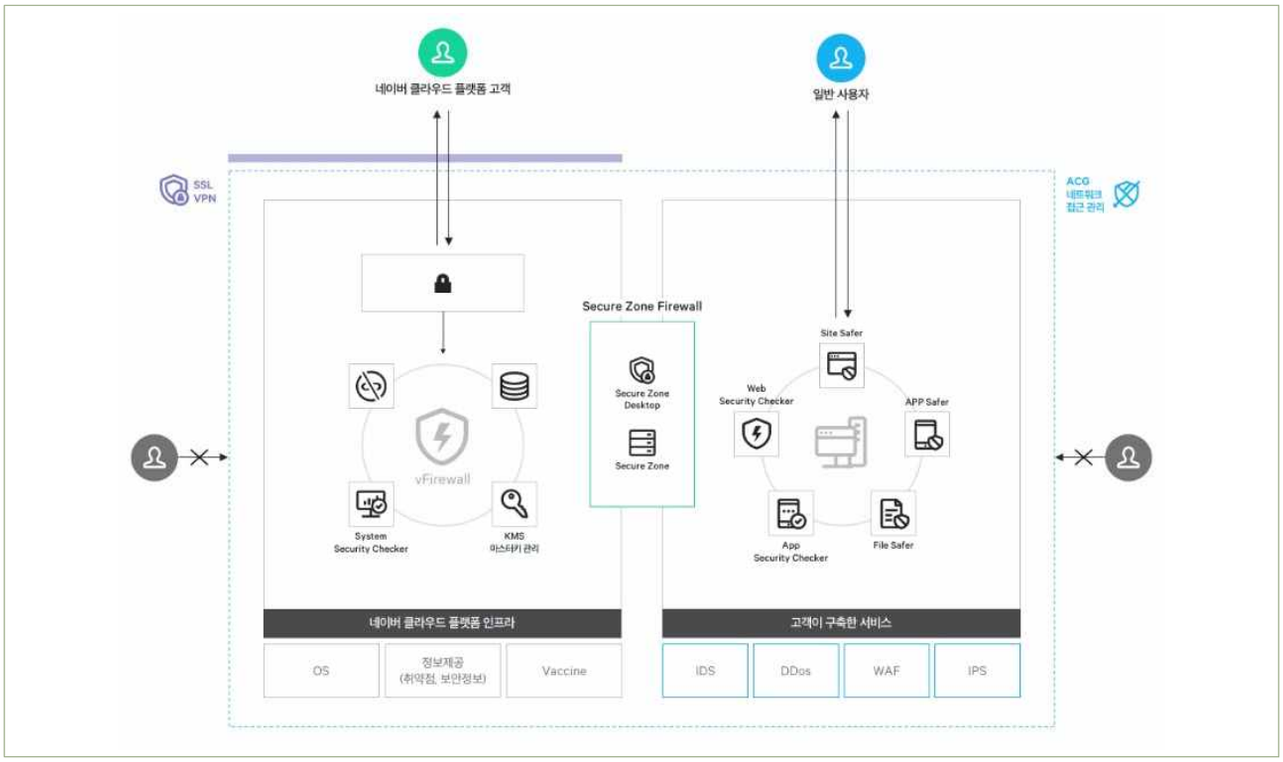
  - 예시

    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

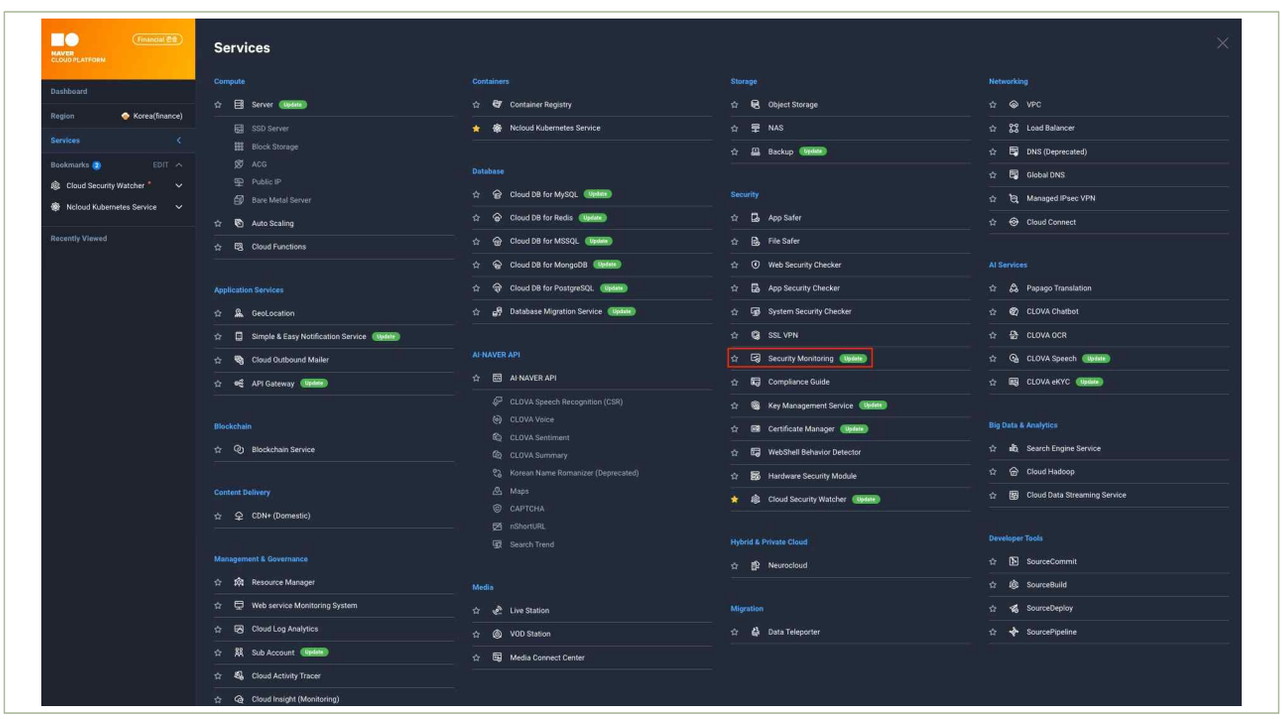
- 네이버 클라우드 플랫폼은 사용자의 가상자원을 안전하게 보호하기 위하여 Anti-Virus, IDS, IPS, WAS, Anti-DDoS 구성 및 보안전문 인력이 24시간 365일 보안관제 서비스를 수행하는 Security Monitoring 상품을 제공하고 있습니다. 사용자는 Security Monitoring 상품내에 포함된 DDoS, WAF, IPS, IDS, Anti-DDoS 등을 통해 가상자원에 대한 보안 관제를 수행할 수 있습니다.



| 그림 2-3-1 | Security Monitoring 아키텍처

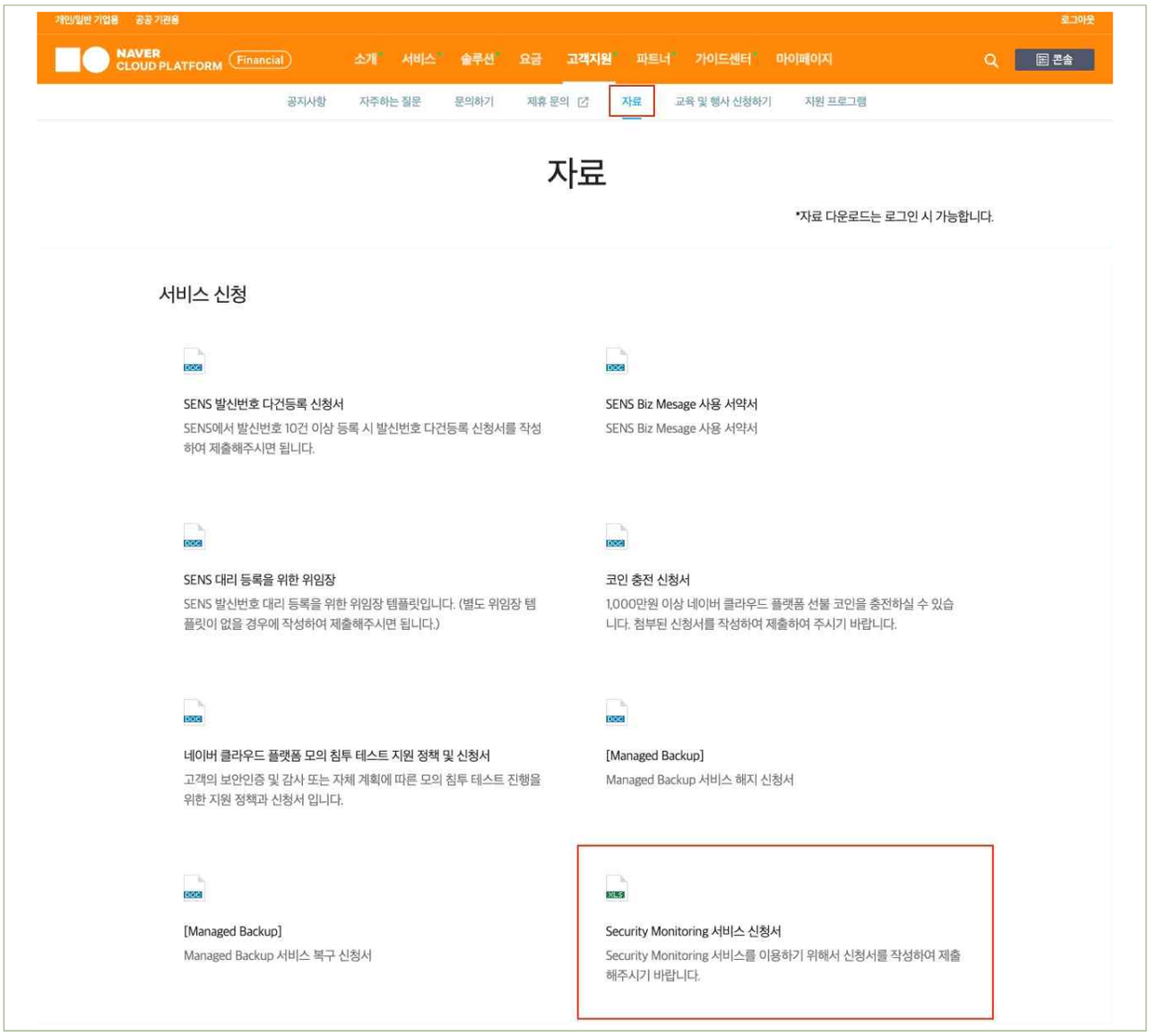
Security Monitoring 상품을 통한 네트워크 보안관제

① **(가상자원관리시스템)** 'Services' → 'Security Monitoring' 상품을 선택하고, '+ 상품 이용 신청'을 통해 상품을 활성화합니다.



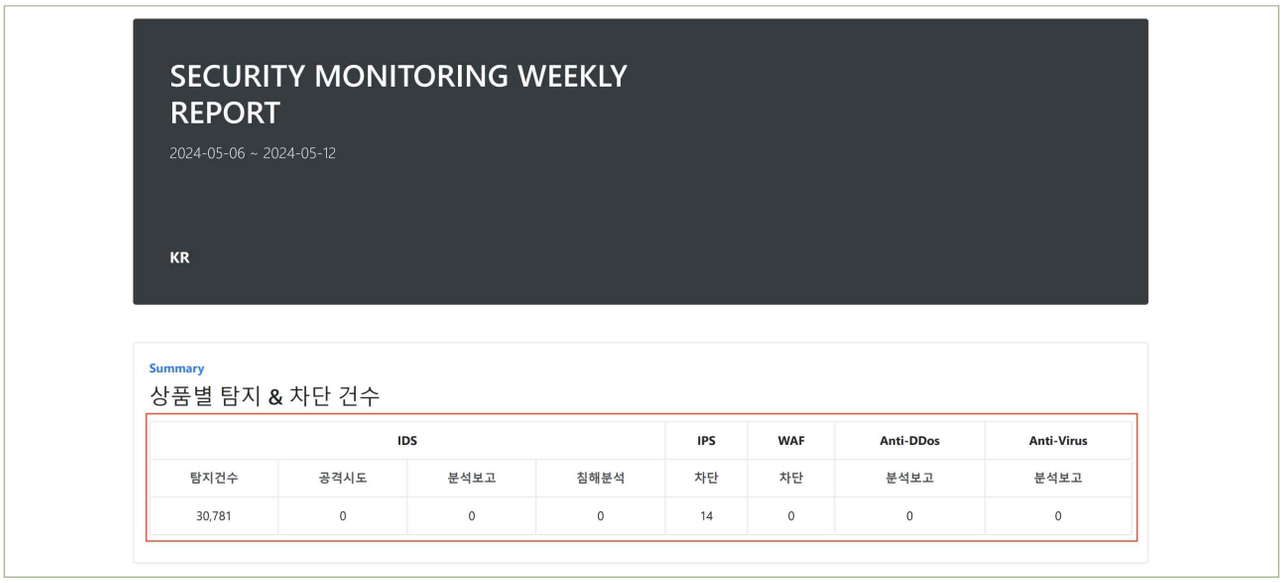
| 그림 2-3-2 | Security Monitoring 상품 선택

② **(네이버 클라우드 플랫폼 포털)** 상세 서비스 신청을 위해 '고객지원' → '자료' → 'Security Monitoring 서비스 신청서'를 다운받아 신청서를 작성합니다. 작성이 완료된 신청서는 네이버 클라우드 플랫폼 포털의 '고객지원' → '문의하기'를 통해 제출합니다.



| 그림 2-3-3 | Security Monitoring 상세 서비스 신청

③ 신청서를 통해 지정한 가상자원(Server)에 대해 WAF, IPS, IDS, DDoS 공격에 대한 모니터링이 수행되며, '가상자원관리시스템'의 Security Monitoring 콘솔 또는 주기적으로 수신되는 Report를 통해 WAF, IPS, IDS, DDoS 공격탐지 결과를 확인합니다.



SECURITY MONITORING WEEKLY REPORT

2024-05-06 ~ 2024-05-12

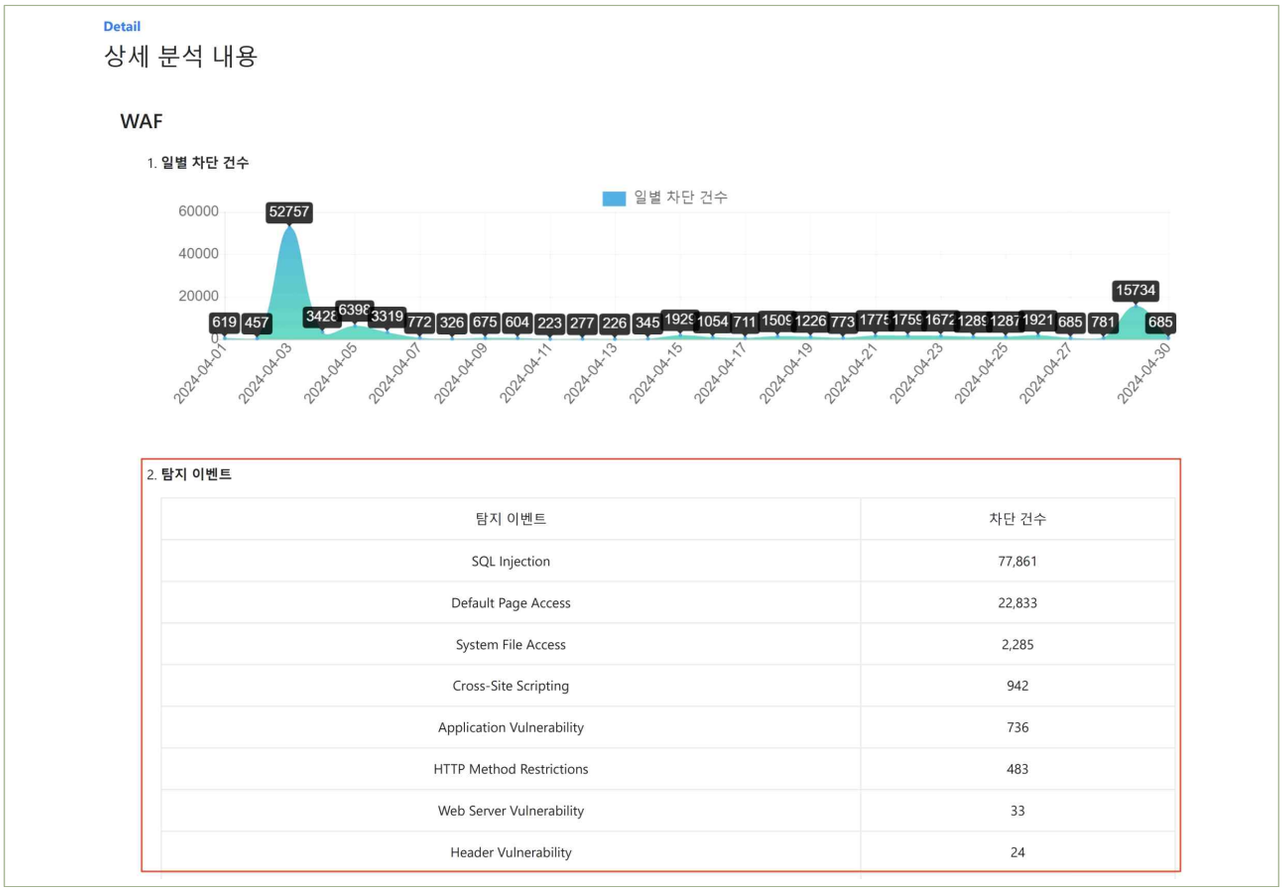
KR

Summary

상품별 탐지 & 차단 건수

IDS				IPS	WAF	Anti-DDos	Anti-Virus
탐지건수	공격시도	분석보고	침해분석	차단	차단	분석보고	분석보고
30,781	0	0	0	14	0	0	0

| 그림 2-3-4 | Security Monitoring Weekly Report 예시



Detail

상세 분석 내용

WAF

1. 일별 차단 건수

2. 탐지 이벤트

탐지 이벤트	차단 건수
SQL Injection	77,861
Default Page Access	22,833
System File Access	2,285
Cross-Site Scripting	942
Application Vulnerability	736
HTTP Method Restrictions	483
Web Server Vulnerability	33
Header Vulnerability	24

| 그림 2-3-5 | Security Monitoring Weekly Report 상세 예시

4 참고 사항

- [참고1] Security Monitoring 사용 가이드
- [참고2] Security Monitoring 상품 사용 신청서

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 공개용웹서버의 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

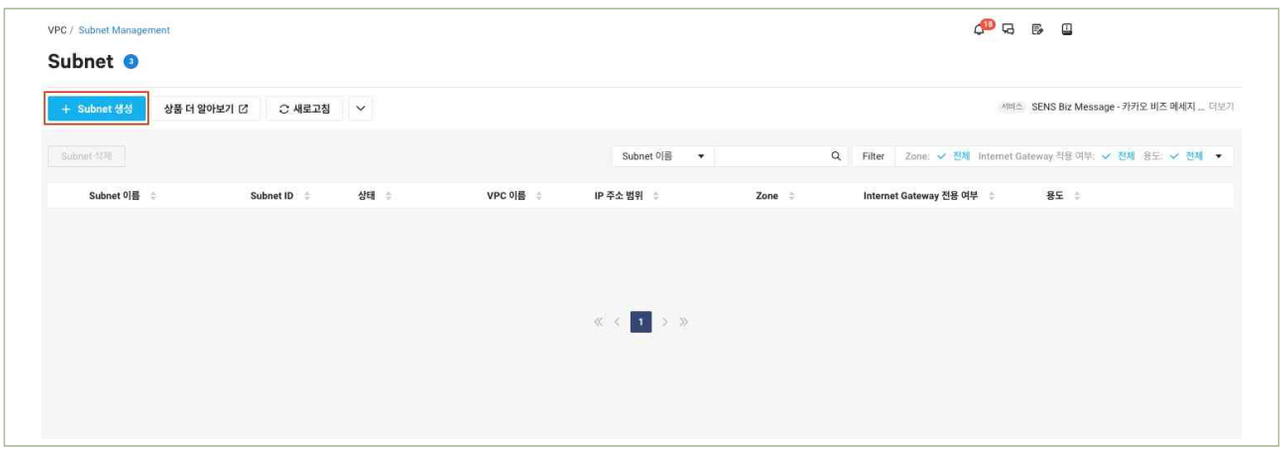
- 네이버 클라우드 플랫폼 환경에서 공개용 웹서버를 구성하는 경우, 웹서버가 구성될 Private Subnet과 DBMS가 구성될 Private Subnet을 각각 분리하여야 합니다. 웹서버를 인터넷과 연결되지 않는 Private Subnet에 구성하고 Application Load Balancer 등을 통해 웹서버까지 트래픽이 전달될 수 있도록 구성하여야 합니다. 이러한 구성은 웹서버를 인터넷망에 직접적으로 노출시키지 않으므로 불필요한 네트워크 프로토콜에 대한 접근을 제한하여 웹서버를 안전하게 보호할 수 있습니다.

안전한 네트워크 구성을 통한 웹서버 보호

① **(가상자원관리시스템)** ‘Services’ → ‘VPC’ 상품을 선택합니다.

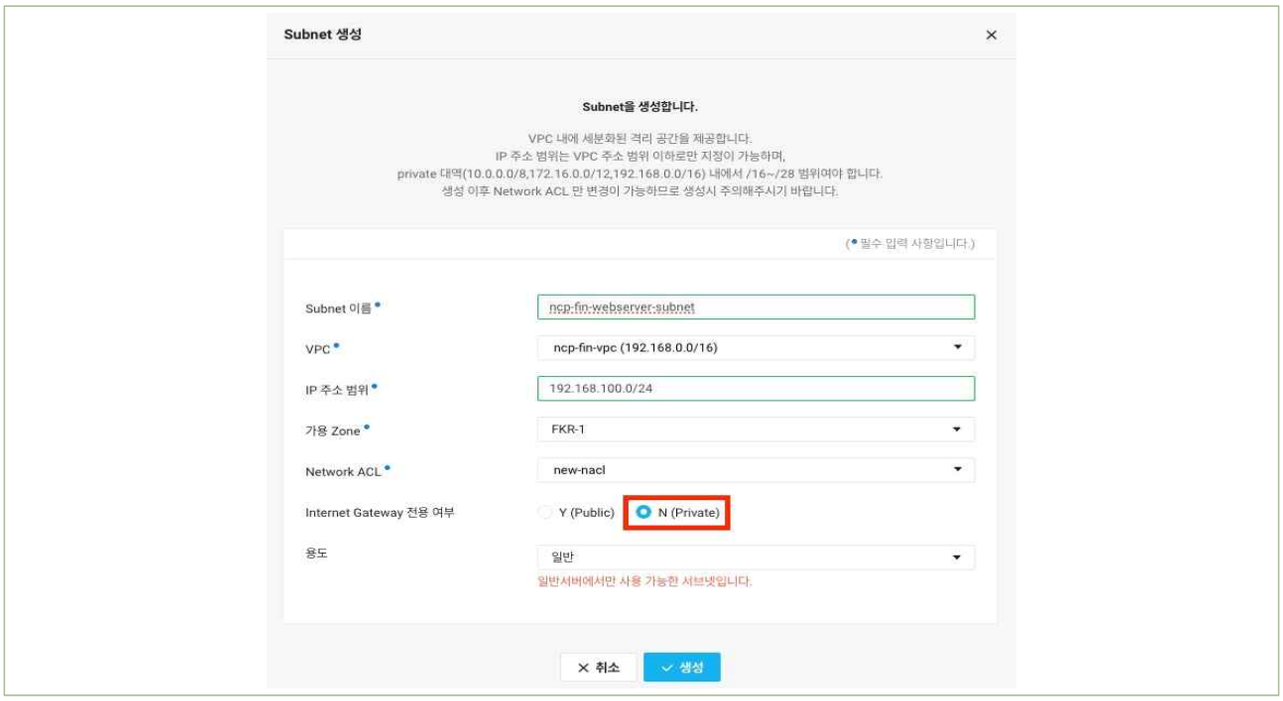
| 그림 2-3-6 | VPC 상품 선택

② **(가상자원관리시스템)** ‘Subnet Management’ → ‘+ Subnet 생성’을 클릭합니다.



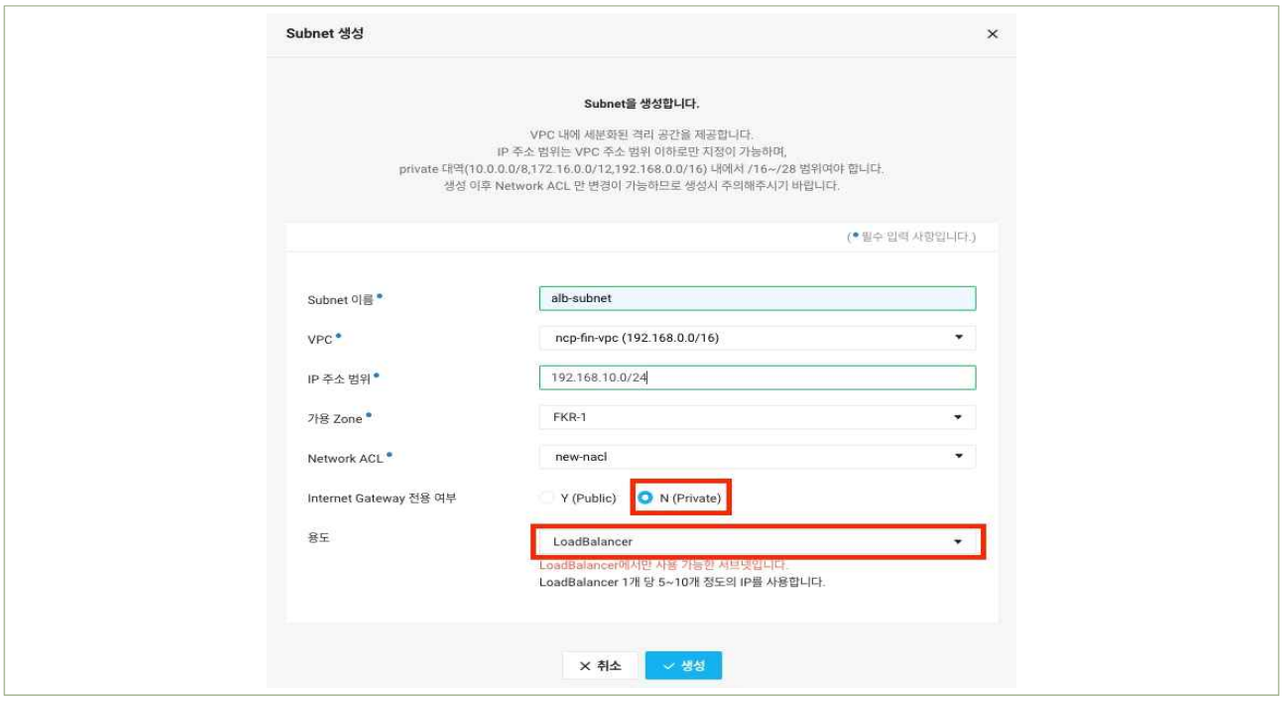
| 그림 2-3-7 | Subnet 관리 콘솔

③ **(가상자원관리시스템)** 'Internet Gateway 전용 여부' 라디오 버튼에서 'N (Private)'을 클릭하여 Private Subnet을 생성합니다.



| 그림 2-3-8 | 웹서버 Subnet 생성 예시

④ **(가상자원관리시스템)** 위와 동일한 방법을 통해 Application Load Balancer를 구성할 신규 Private Subnet을 생성합니다.

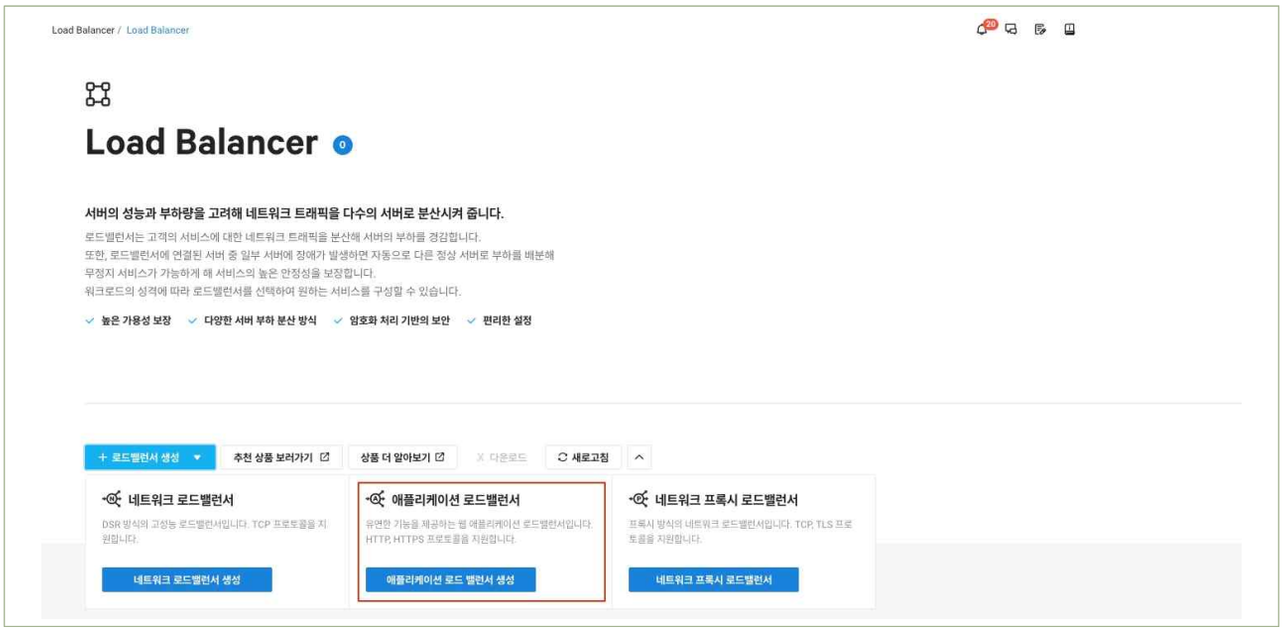


| 그림 2-3-9 | Application Load Balancer Subnet 생성 예시

⑤ **(가상자원관리시스템)** ‘Services’ → ‘Load Balancer’ 상품을 선택합니다.

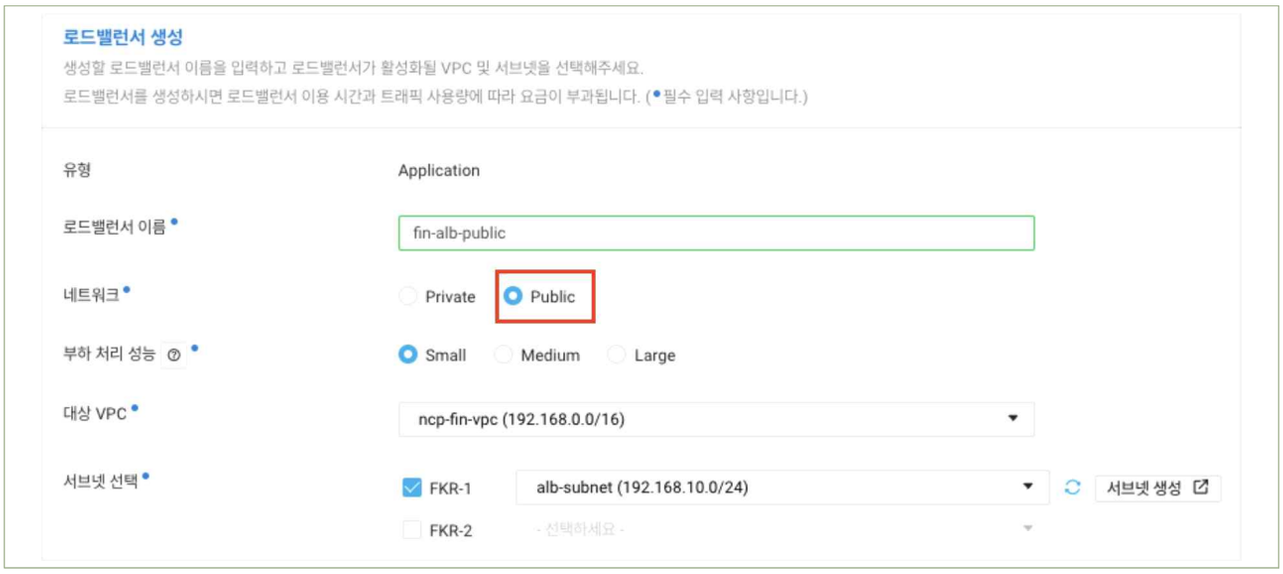
| 그림 2-3-10 | Load Balancer 상품 선택

⑥ **(가상자원관리시스템)** ‘+ 로드밸런서 생성’ → ‘애플리케이션 로드 밸런서 생성’을 클릭합니다.



| 그림 2-3-11 | Application Load Balancer 생성

⑦ **(가상자원관리시스템)** 로드밸런서 생성 단계에서 인터넷망으로부터 HTTP, HTTPS 요청을 받을 수 있도록 Public 네트워크 타입의 Application Load Balancer를 생성합니다. 생성이 완료되면 Application Load Balancer의 '접속 정보', 'IP'를 통해 웹서버에 접속 할 수 있습니다.



| 그림 2-3-12 | Application Load Balancer 생성 예시

| 그림 2-3-13 | Application Load Balancer의 웹서버 접속정보 예시

API를 통한 안전한 네트워크 구성

① **(API(CLI))** 'createSubnet' API를 통해 웹서버와 Application Load Balancer 구성을 위한 신규 Private Subnet을 생성합니다.

- 요청 예시

```
GET https://fin-ncloud.apigw.fin-ntruss.com/vpc/v2/createSubnet
?regionCode=FKR
&zoneCode=FKR-1
&vpcNo=***04
&subnetName=test-***
&subnet=***.***.1.0/24
&networkAclNo=***31
&subnetTypeCode=PRIVATE
&usageTypeCode=GEN
```

- 응답 예시

```
<createSubnetResponse>
<requestId>0f539b1b-10ef-43fa-a2c4-3670e601251b</requestId>
<returnCode>0</returnCode>
<returnMessage>success</returnMessage>
<totalRows>1</totalRows>
<subnetList>
    <subnet>
      <subnetNo>***43</subnetNo>
      <vpcNo>***04</vpcNo>
      <zoneCode>FKR-1</zoneCode>
      <subnetName>test-***</subnetName>
      <subnet>***.***.1.0/24</subnet>
      <subnetStatus>
        <code>CREATING</code>
        <codeName>creating</codeName>
      </subnetStatus>
      <createDate>2020-07-31T14:32:28+0900</createDate>
      <subnetType>
        <code>PRIVATE</code>
        <codeName>Private</codeName>
      </subnetType>
      <usageType>
        <code>GEN</code>
        <codeName>General</codeName>
      </usageType>
      <networkAclNo>***31</networkAclNo>
    </subnet>
</subnetList>
</createSubnetResponse>
</vpcList>
</createVpcResponse>
```

| 그림 2-3-14 | API를 통한 Private Subnet 생성 예시

② **(API(CLI))** 'createLoadBalancerInstance' API를 통해 웹서버 구성을 위한 신규 Application Load Balancer를 생성합니다.

- 요청 예시

```
GET https://fin-ncloud.apigw.fin-ntruss.com/vpc/v2/createLoadBalancerInstance
?regionCode=FKR
&loadBalancerTypeCode=APPLICATION
&loadBalancerName=test-***
&loadBalancerNetworkTypeCode=PUBLIC
&throughputTypeCode=SMALL
&idleTimeout=60
&vpcNo=***04
&subnetNoList.1=***43
&loadBalancerListenerList.1.protocolTypeCode=HTTPS
&loadBalancerListenerList.1.port=443
&loadBalancerListenerList.1.targetGroupNo=***095
```

- 응답 예시

```
<createLoadBalancerInstanceResponse>
<requestId>959a2fe5-fd1b-459a-9af3-df0e51b68e1d</requestId>
<returnCode>0</returnCode>
<returnMessage>success</returnMessage>
<totalRows>1</totalRows>
<loadBalancerInstanceList>
    <loadBalancerInstance>
      <loadBalancerInstanceNo>***887</loadBalancerInstanceNo>
      <loadBalancerInstanceStatus>
        <code>INIT</code>
        <codeName>LB INIT state</codeName>
      </loadBalancerInstanceStatus>
      <loadBalancerInstanceOperation>
        <code>CREAT</code>
        <codeName>LB CREATE OP</codeName>
      </loadBalancerInstanceOperation>
 <loadBalancerInstanceStatusName>Creating</loadBalancerInstanceStatusName>
      <loadBalancerDescription></loadBalancerDescription>
      <createDate>2020-12-20T19:21:02+0900</createDate>
      <loadBalancerName>test-***</loadBalancerName>
      <loadBalancerDomain>test-***-***887-***.com</loadBalancerDomain>
      <loadBalancerIpList>
        <loadBalancerIp>***.***.5.6</loadBalancerIp>
      </loadBalancerIpList>
      <loadBalancerType>
        <code>APPLICATION</code>
        <codeName>Application Load Balancer</codeName>
      </loadBalancerType>
      <loadBalancerNetworkType>
        <code>PUBLIC</code>
        <codeName>Public</codeName>
      </loadBalancerNetworkType>
      <throughputType>
```

```
            <code>SMALL</code>
            <codeName>Small</codeName>
        </throughputType>
        <idleTimeout>60</idleTimeout>
        <vpcNo>***04</vpcNo>
        <regionCode>FKR</regionCode>
        <subnetNoList>
            <subnetNo>***43</subnetNo>
        </subnetNoList>
        <loadBalancerSubnetList>
            <loadBalancerSubnet>
                <zoneCode>FKR-1</zoneCode>
                <subnetNo>***43</subnetNo>
                <publicIpInstanceNo/>
            </loadBalancerSubnet>
        </loadBalancerSubnetList>
        <loadBalancerListenerNoList>
            <loadBalancerListenerNo>***961</loadBalancerListenerNo>
        </loadBalancerListenerNoList>
    </loadBalancerInstance>
</loadBalancerInstanceList>
</createLoadBalancerInstanceResponse>
```

| 그림 2-3-15 | API를 통한 Application Load Balancer 생성 예시

4 참고 사항

- [참고1] Private Subnet을 통한 웹서버 구성 아키텍처 예시
- [참고2] Application Load Balancer 생성 가이드
- [참고3] Subnet 생성 API 가이드
- [참고4] Application Load Balancer 생성 API 가이드

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.

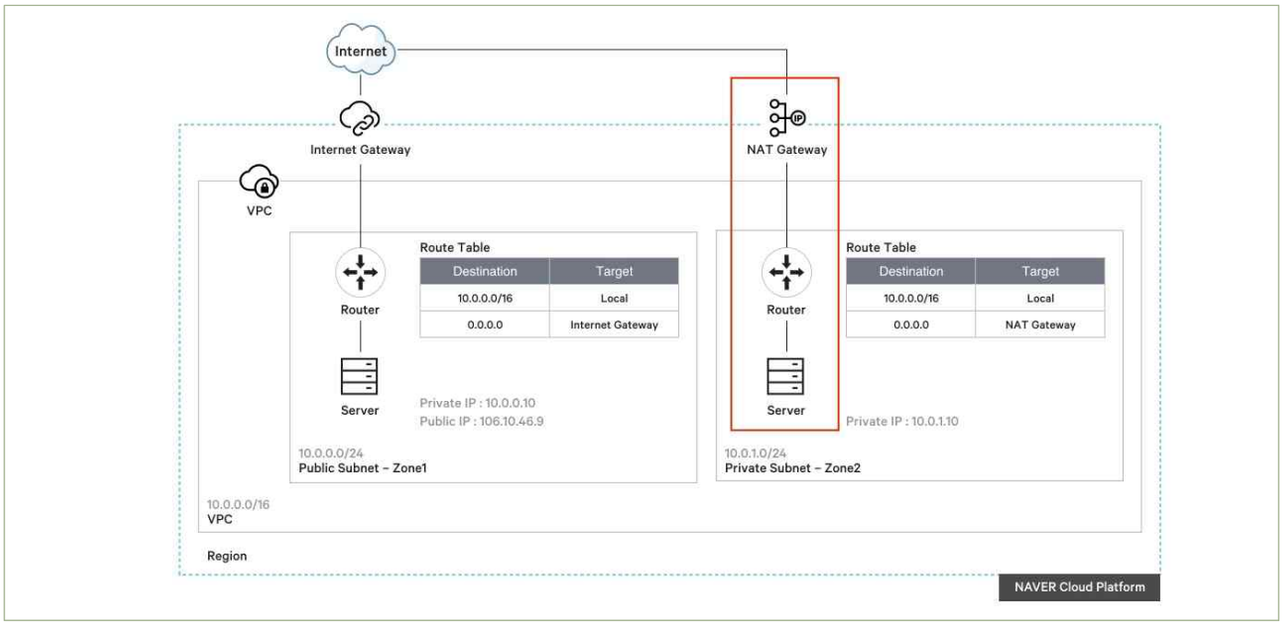
  - 예시

    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

- 네이버 클라우드 플랫폼 내의 가상자원은 기본적으로 사설 IP가 부여되며, 공인 IP는 사용자가 직접 생성할 경우에만 생성되기 때문에 인터넷 게이트웨이와 연결된 Public Subnet에 존재하는 가상자원이라 하더라도 기본적으로는 인터넷 통신이 불가능합니다.
  따라서, 정보처리시스템의 특성에 따라 Private Subnet 내의 가상자원과 PG, VAN 등과의 연동을 위해 외부 네트워크 연결이 필요한 경우, NAT Gateway를 통하여 인터넷 게이트웨이 및 외부 네트워크에 연결될 수 있도록 Route Table을 구성하여야 합니다.



| 그림 2-5-1 | NAT Gateway를 통한 Private Subnet, 인터넷망의 통신 예시

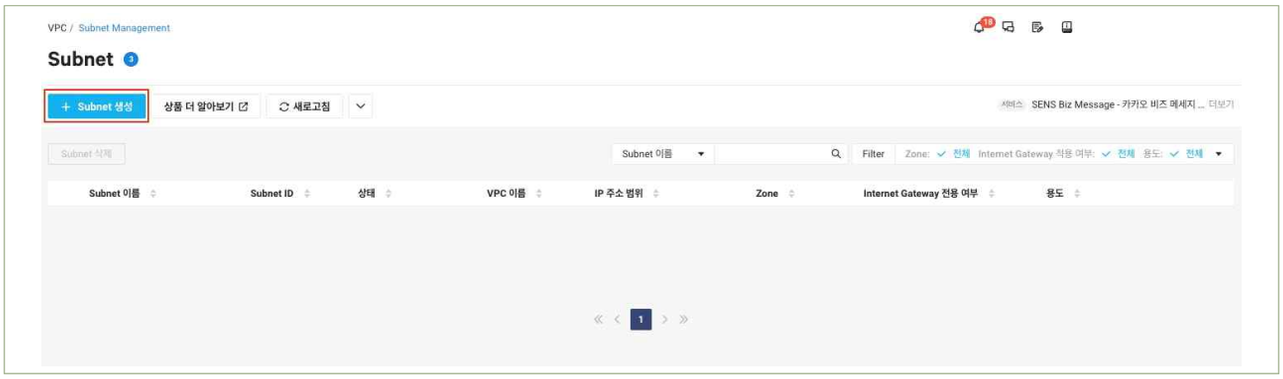
또한, 가상자원과 연결된 Network Interface의 사설 IP 현황과 Public IP 현황의 검토를 통해 불필요한 공인 IP가 연결된 가상자원을 검토할 수 있습니다.

◦ 가상자원의 사설 IP 관리를 위한 NAT Gateway 구성

① **(가상자원관리시스템)** 'Services' → 'VPC' 상품을 선택합니다.

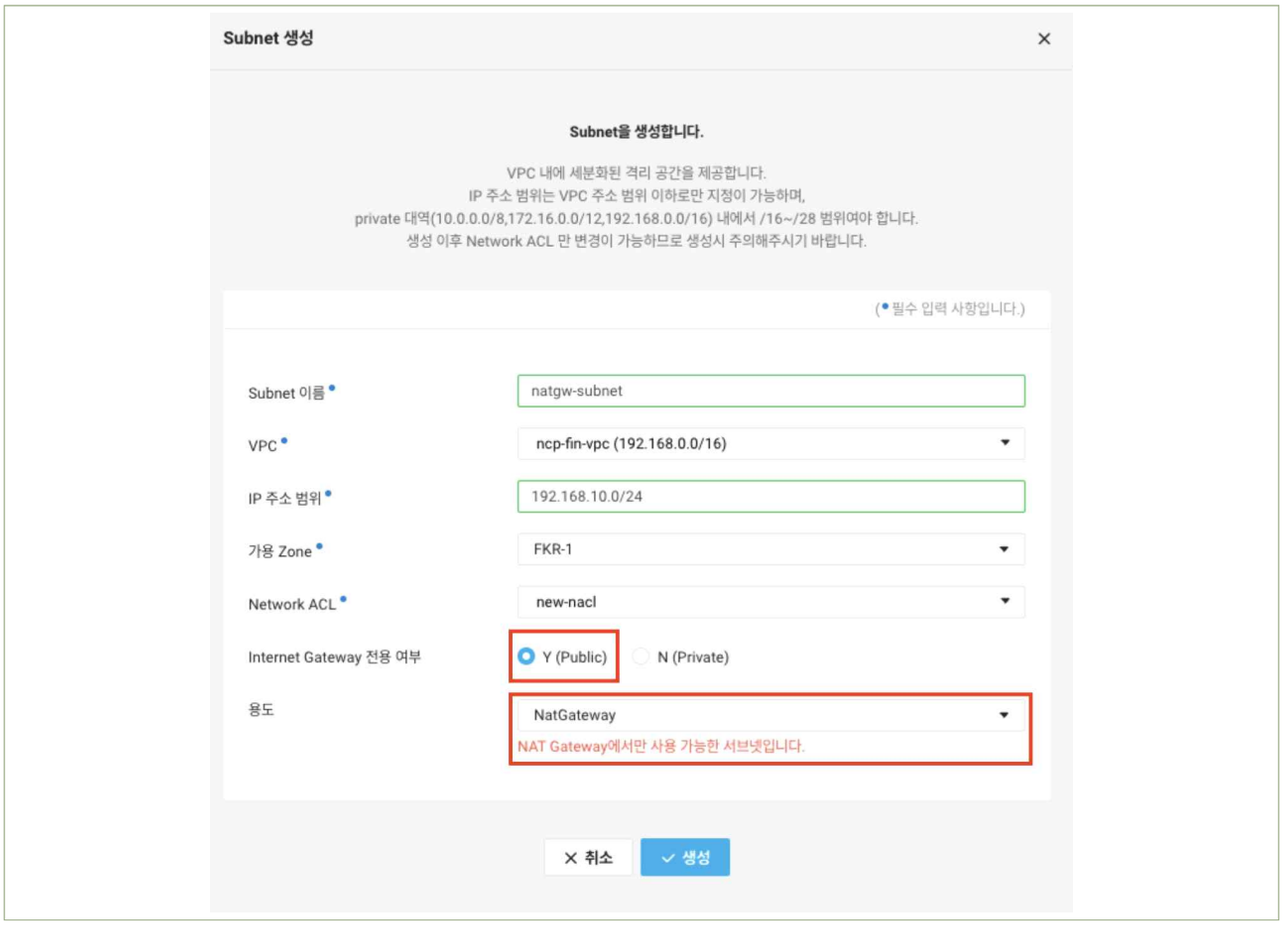
| 그림 2-5-2 | VPC 상품 선택

② **(가상자원관리시스템)** ‘Subnet Management’ → ‘+ Subnet 생성’을 클릭합니다.



| 그림 2-5-3 | Subnet 관리 콘솔

③ **(가상자원관리시스템)** ‘용도’ 드롭박스에서 NAT Gateway를 선택하여 NAT Gateway 전용 Subnet을 생성합니다. NAT Gateway의 Subnet은 Public, Private 타입을 모두 선택할 수 있으므로 정보처리시스템 특성을 고려하여 선택합니다.

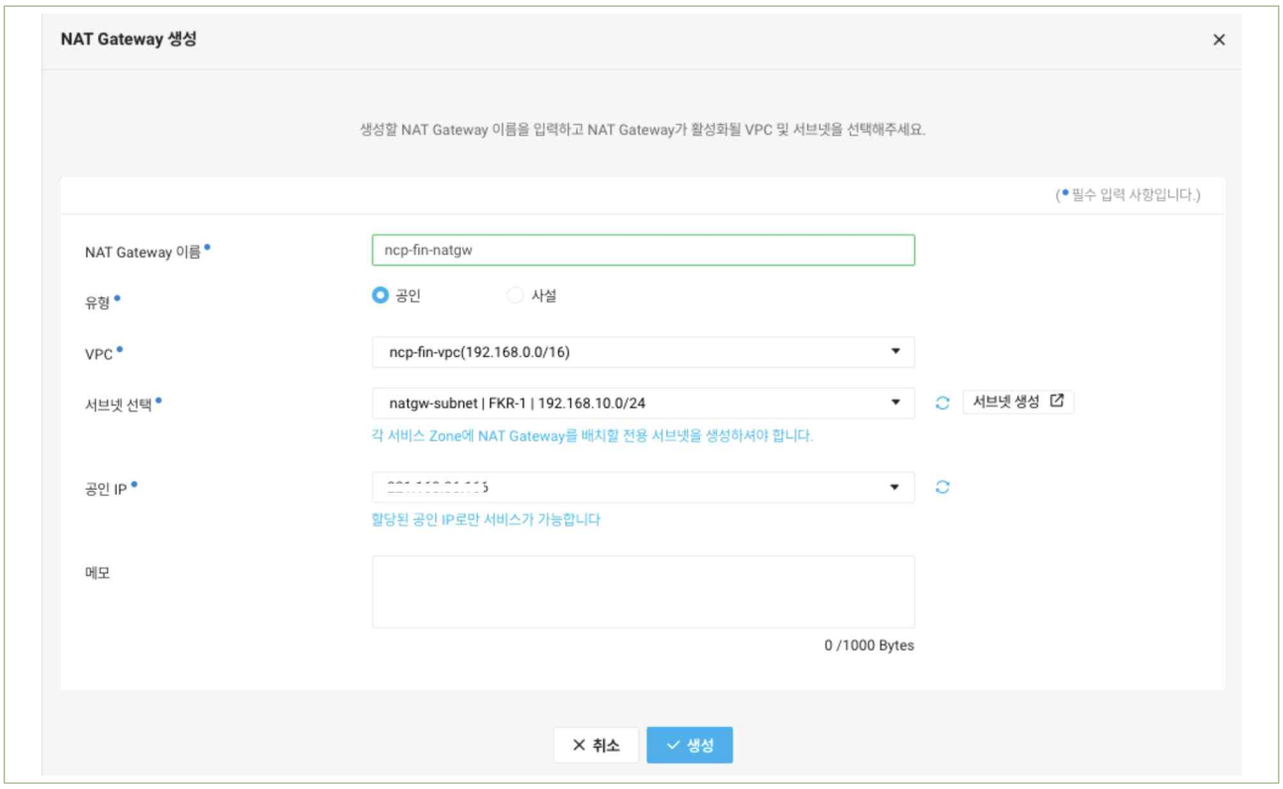


| 그림 2-5-4 | NAT Gateway 전용 Subnet 생성 예시

④ **(가상자원관리시스템)** VPC 상품 좌측 메뉴에서 'NAT Gateway' → '+ NAT Gateway 생성'을 클릭합니다.

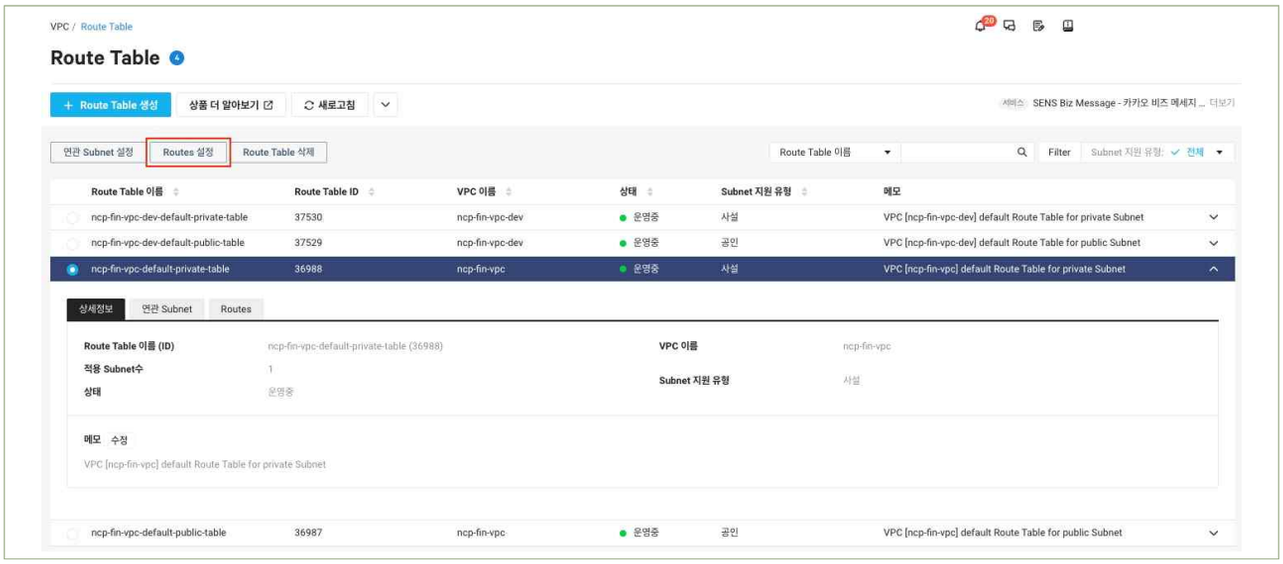
| 그림 2-5-5 | NAT Gateway 생성

⑤ **(가상자원관리시스템)** '서브넷 선택' 드롭박스에서 NAT Gateway 전용 Subnet을 선택하고 NAT Gateway를 생성합니다.



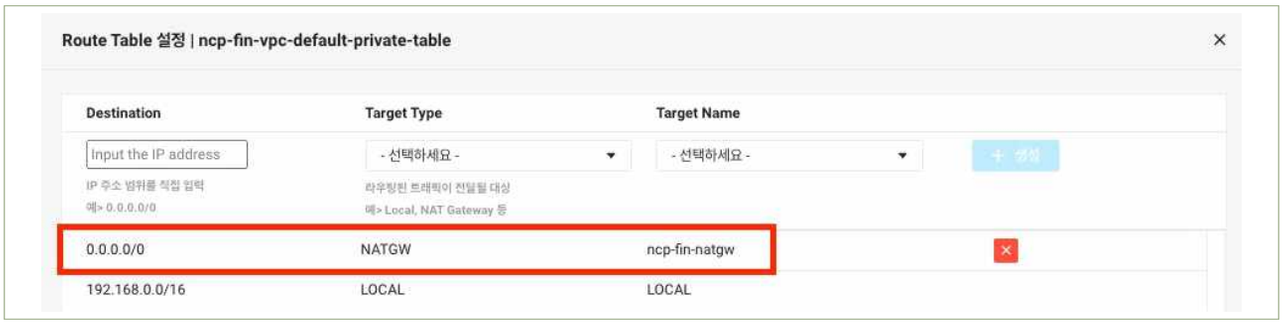
| 그림 2-5-6 | NAT Gateway 생성 예시

⑥ **(가상자원관리시스템)** VPC 상품 좌측 메뉴에서 'Route Table'을 클릭하고, 가상자원이 위치한 Private Subnet 선택 후 'Routes 설정'을 클릭합니다.



| 그림 2-5-7 | Route Table 설정

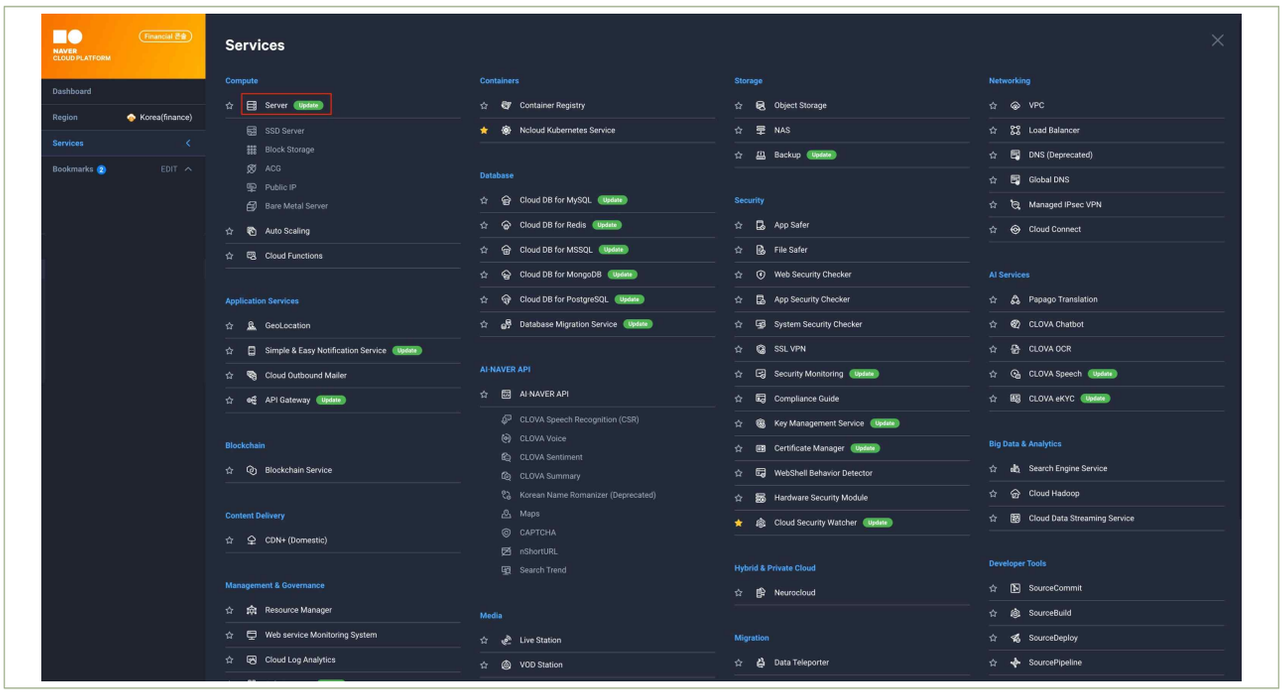
⑥ **(가상자원관리시스템)** 가상자원에 대한 인터넷(0.0.0.0/0) Routing 경로를 NAT Gateway로 설정하여 NAT Gateway 설정을 완료합니다.



| 그림 2-5-8 | NAT Gateway 경유를 위한 Route Table 설정 예시

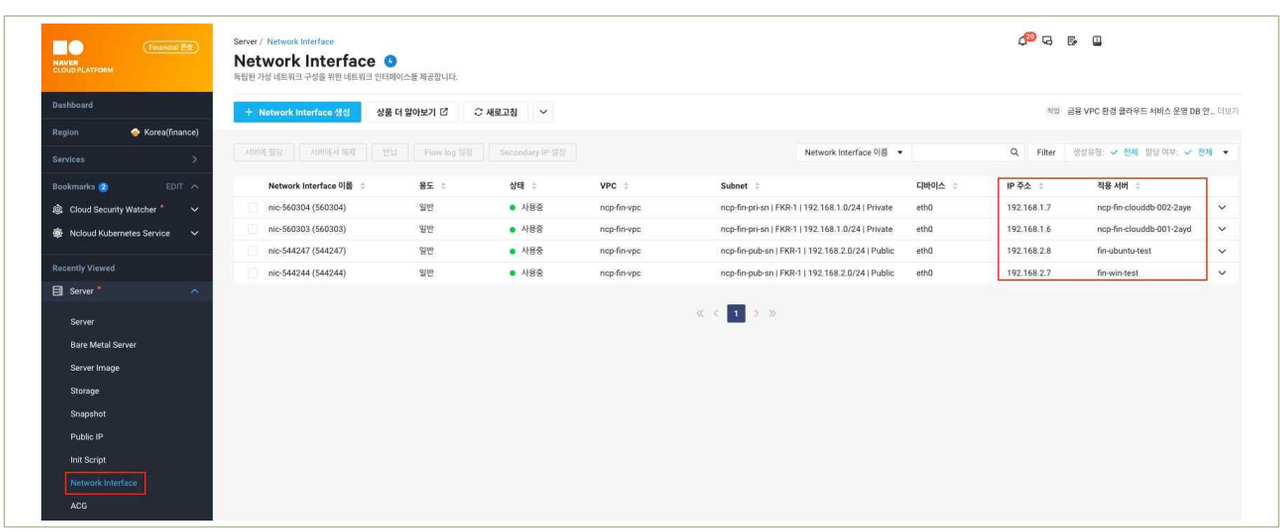
사설 및 공인 IP 현황 검토

① **(가상자원관리시스템)** ‘Services’ → ‘Server’ 상품을 선택합니다.



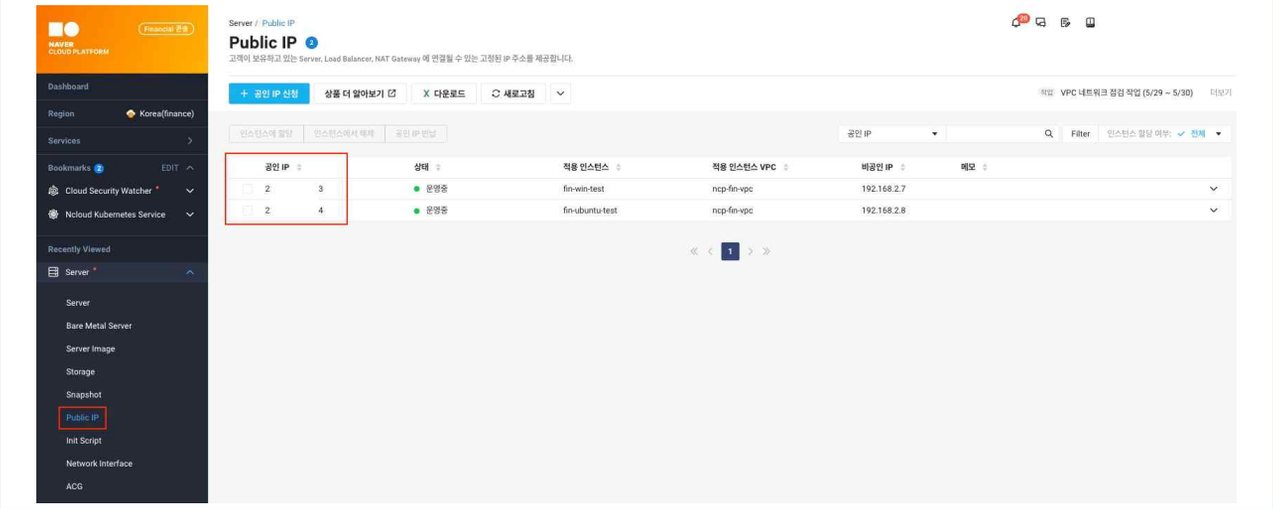
| 그림 2-5-9 | Server 상품 선택

② **(가상자원관리시스템)** ‘Network Interface’ 관리 콘솔에서 사설 IP 현황을 검토합니다.



| 그림 2-5-10 | 사설 IP 현황 예시

③ **(가상자원관리시스템)** ‘Public IP’ 관리 콘솔에서 공인 IP 현황을 검토합니다.



| 그림 2-5-11 | 공인 IP 현황 예시

API를 통한 NAT Gateway 구성

① **(API(CLI))** ‘createNatGatewayInstance’ API를 통해 NAT Gateway를 생성합니다.

- 요청 예시

```
GET https://fin-ncloud.apigw.fin-ntruss.com/vpc/v2/createNatGatewayInstance
?regionCode=FKR
&zoneCode=FKR-1
&vpcNo=***04
&natGatewayName=test-***
&subnetNo=***28
&publicIpInstanceNo=***25
```

- 응답 예시

```
<createNatGatewayInstanceResponse>
<requestId>4475d78c-4c27-4404-807d-7b0b645bb127</requestId>
<returnCode>0</returnCode>
<returnMessage>success</returnMessage>
<totalRows>1</totalRows>
<natGatewayInstanceList>
    <natGatewayInstance>
      <vpcNo>***04</vpcNo>
      <vpcName>test-***</vpcName>
      <natGatewayInstanceNo>***734</natGatewayInstanceNo>
      <natGatewayName>test-***</natGatewayName>
      <publicIp>***.***.109.101</publicIp>
      <natGatewayInstanceStatus>
        <code>INIT</code>
        <codeName>init</codeName>
      </natGatewayInstanceStatus>
```

```
        <natGatewayInstanceStatusName>준비중</natGatewayInstanceStatusName>
        <natGatewayInstanceOperation>
          <code>NULL</code>
          <codeName>NULL OP</codeName>
        </natGatewayInstanceOperation>
        <createDate>2020-08-07T16:05:52+0900</createDate>
        <natGatewayDescription></natGatewayDescription>
        <zoneCode>FKR-1</zoneCode>
        <natGatewayType>
            <code>PBLIP</code>
            <codeName>Public</codeName>
         </natGatewayType>
         <subnetName>v-kr1-pub-natgw-***</subnetName>
         <subnetNo>***28</subnetNo>
         <privateIp>10.0.***.***</privateIp>
         <publicIpInstanceNo>***25</publicIpInstanceNo>
      </natGatewayInstance>
</natGatewayInstanceList>
</createNatGatewayInstanceResponse>
```

| 그림 2-5-12 | API를 통한 NAT Gateway 생성 예시

4 참고 사항

- [참고1] NAT Gateway 사용 가이드
- [참고2] Route Table 사용 가이드
- [참고3] Network Interface 사용 가이드
- [참고4] Public IP 사용 가이드
- [참고5] NAT Gateway 생성 API 가이드

1 기준

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

2 설명

- 클라우드 네트워크 관련 서비스 관련 정책에 대한 적정성 여부를 주기적으로 검토하여야 한다.

  - 예시

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

3 우수 사례

- 금융회사 및 전자금융업자는 네이버 클라우드 플랫폼에서 제공하는 클라우드 서비스를 통해 구현한 네트워크 정책에 대해 주기적 검토를 수행

  - '2. 네트워크 관리' 분야 내 내용을 참고하여 내부에서 방화벽, NACL, ACG(Access Control Group) 등에 대해 검토

4 참고 사항

- [참고1] NAT Gateway 사용 가이드
- [참고2] Route Table 사용 가이드
- [참고3] Network Interface 사용 가이드
- [참고4] Public IP 사용 가이드
- [참고5] NAT Gateway 생성 API 가이드

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 IP 및 단말기의 MAC Address를 제한 하는 등 강화된 보안환경 구성

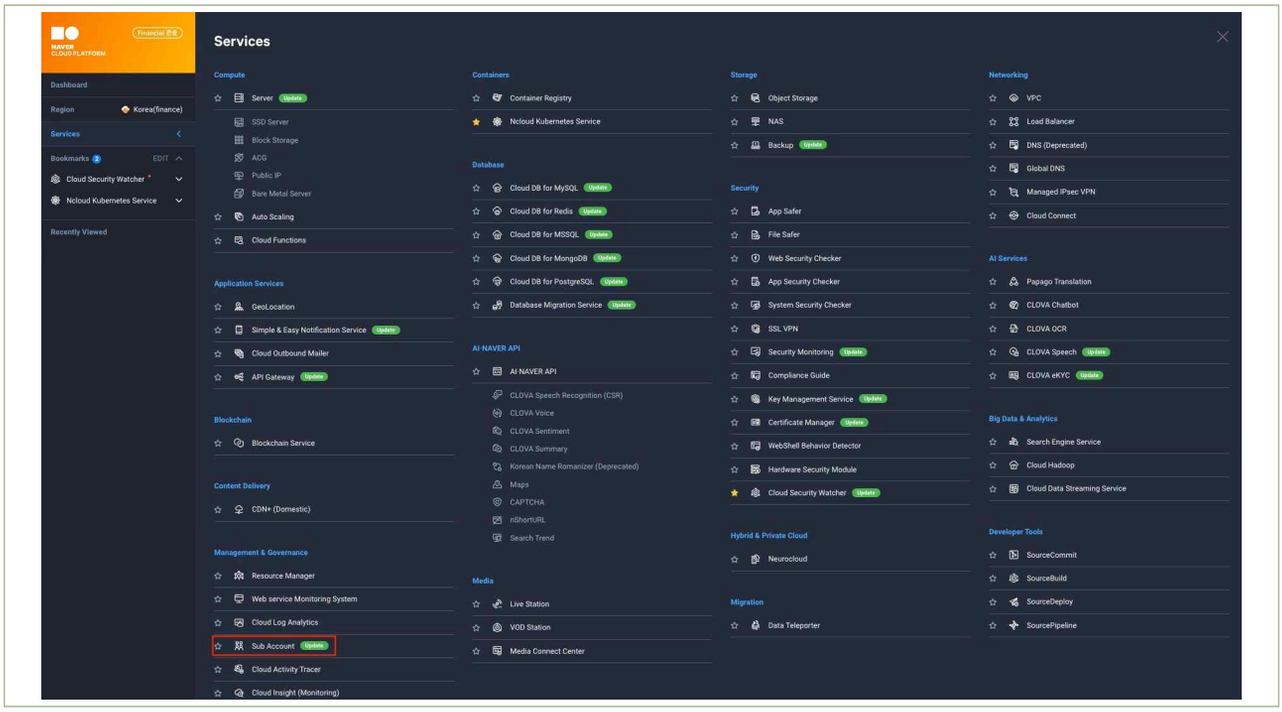
3 우수 사례

- 네이버 클라우드 플랫폼의 가상자원관리시스템(클라우드 콘솔) 계정은 메인계정과 서브계정이 존재합니다. 메인계정은 가상자원관리시스템의 모든 권한을 보유한 계정으로써 계정의 오/남용 및 유출 시 가상자원에 막대한 피해를 초래할 수 있으므로 계정관리에 많은 주의를 필요로 합니다. 서브계정은 메인계정의 자원을 함께 이용하고 관리하는 보조 역할을 수행하는 계정이며, 사용자 업무역할에 따라 최소한의 권한을 부여하여 가상자원을 관리하여야 합니다.

따라서, 네이버 클라우드 플랫폼에서는 Sub Account 상품을 통해 메인계정 하위에 여러 개의 서브계정을 생성하여 사용자의 업무별로 접근권한을 통제 및 관리하고 메인계정은 사용하지 않을 것을 권장하고 있으며, 부득이한 사유로 메인 계정을 통해 가상자원 관리가 필요한 경우에는 MFA와 같은 추가 인증방식과 가상자원관리시스템에 대한 로그인 가능 IP대역과 단말기의 MAC Address를 제한하여 비인가 접근 등에 대한 보안위협을 최소화하여야 합니다.

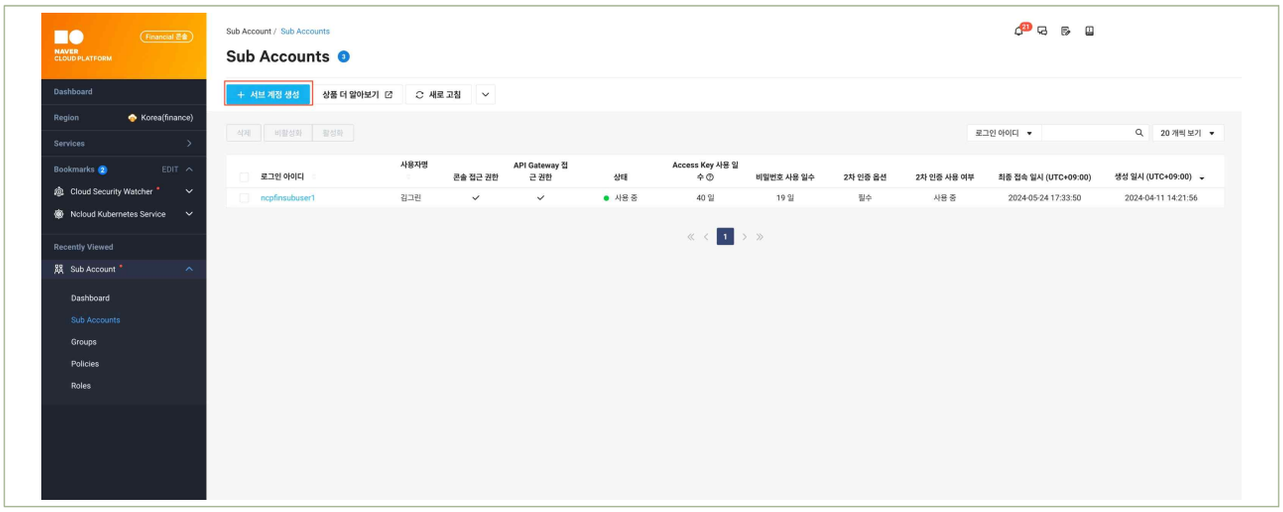
사용자 역할 별 서브계정 생성

① **(가상자원관리시스템)** 'Services' → 'Sub Account' 상품을 선택합니다.



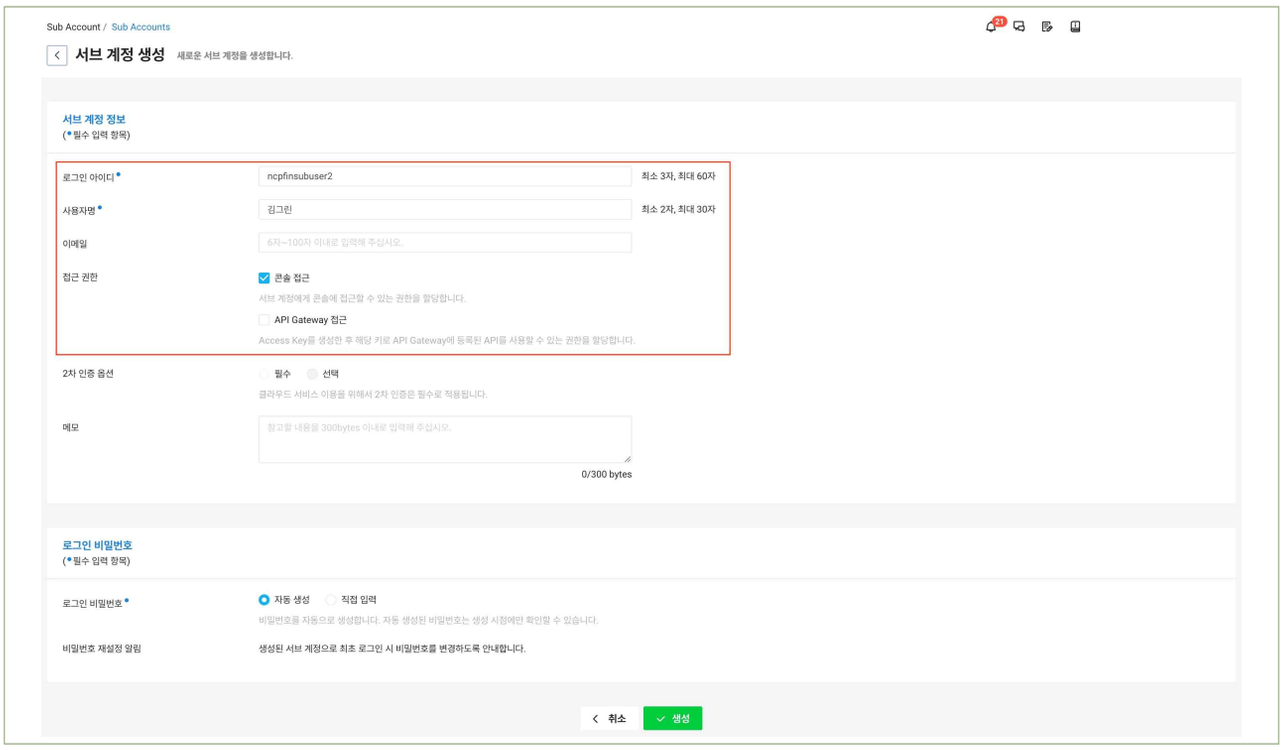
| 그림 3-1-1 | Sub Account 상품 선택

② **(가상자원관리시스템)** ‘Sub Accounts’ → ‘+ 서브 계정 생성’을 통해 가상자원 관리 계정을 생성합니다.



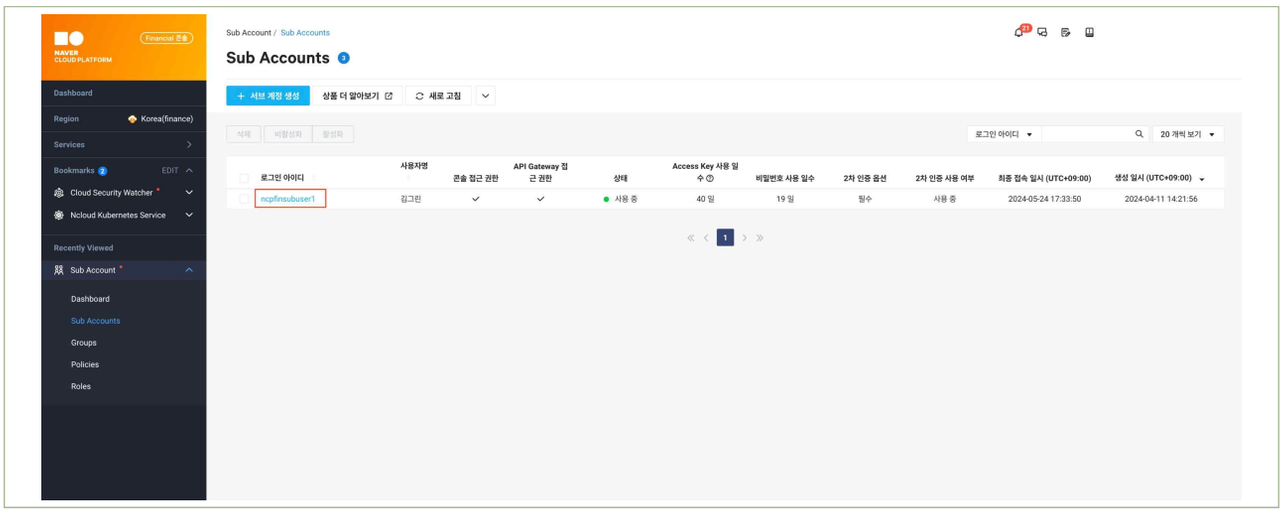
| 그림 3-1-2 | 서브계정 생성 예시

③ **(가상자원관리시스템)** 서브 계정 생성을 위해 ‘로그인 아이디’, ‘사용자명’, 접근권한을 설정하여 서브 계정을 생성합니다.



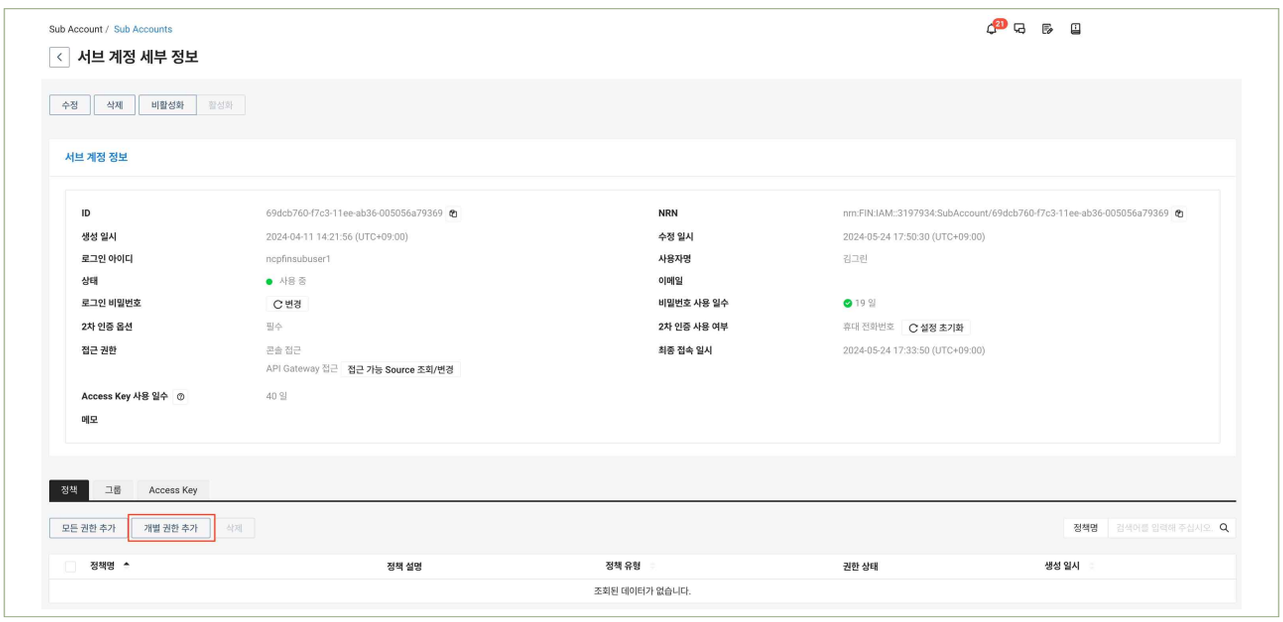
| 그림 3-1-3 | 서브계정 생성 예시

④ **(가상자원관리시스템)** 서브계정에 대한 권한 설정을 위해 서브계정(로그인 아이디)를 클릭합니다.



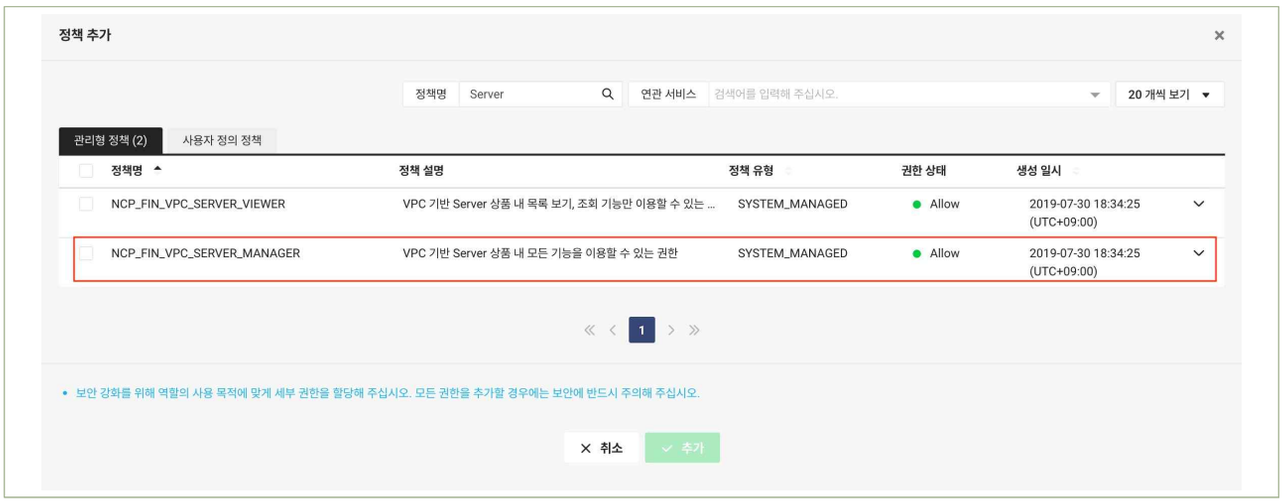
| 그림 3-1-4 | 권한설정을 위한 서브계정 선택

⑤ **(가상자원관리시스템)** '정책'탭의 '개별 권한 추가' 또는 '그룹' 탭의 '추가'를 통해 사용자 별 개별 권한 또는 권한 그룹을 할당합니다.



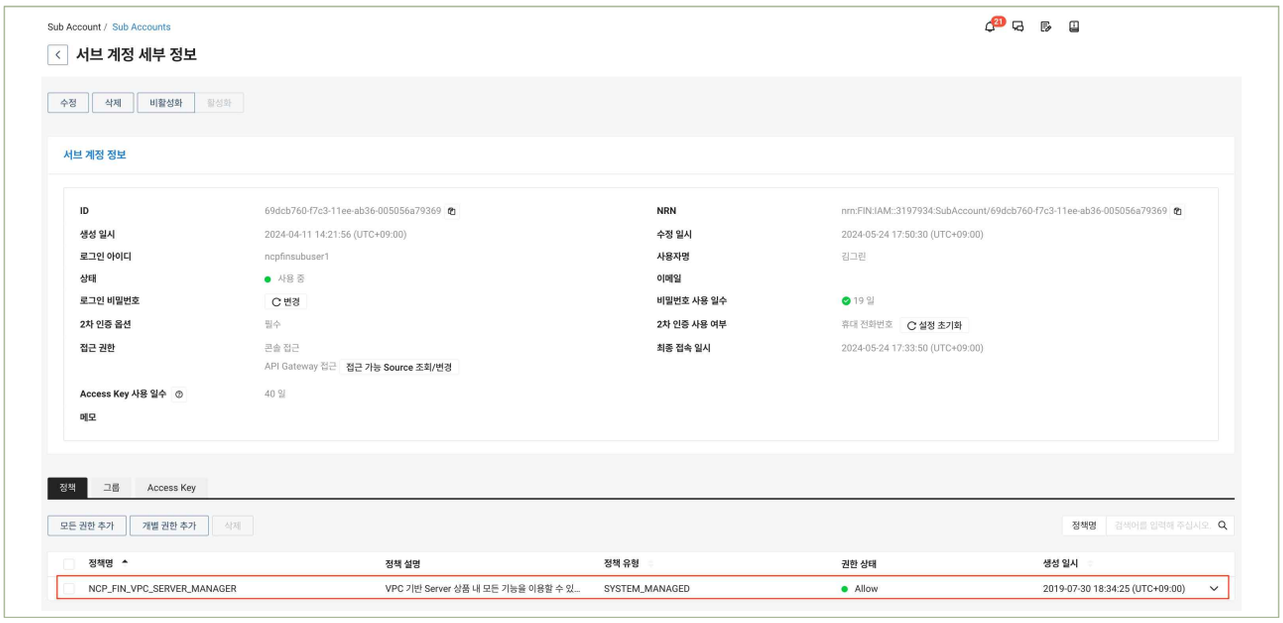
| 그림 3-1-5 | 서브계정의 권한 설정

⑥ **(가상자원관리시스템)** '관리형 정책'탭에서 서브 계정 별 필요한 NCP 상품 권한을 추가 합니다.



| 그림 3-1-6 | 서브계정에 대한 Server 상품 관리 권한 설정 예시

⑦ **(가상자원관리시스템)** 서브계정에 할당된 NCP 관리형 정책을 확인합니다.

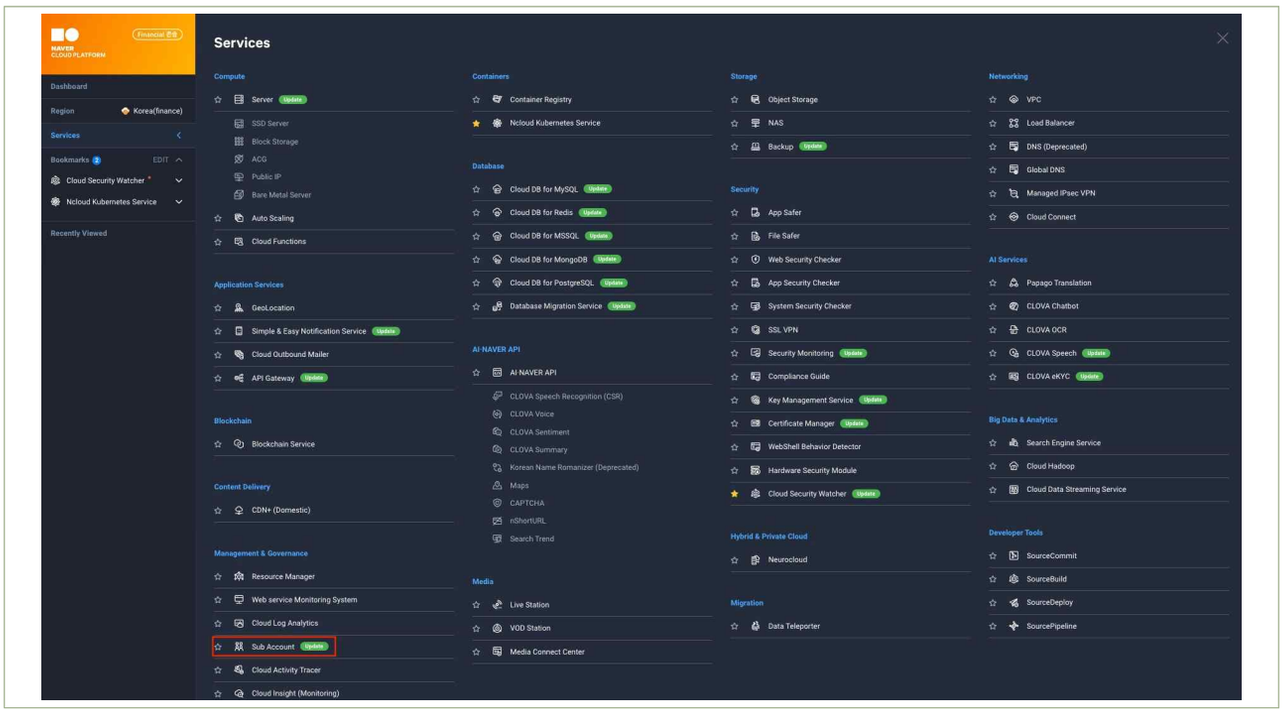


| 그림 3-1-7 | 서브계정 별 권한 부여 완료 예시

※ NCP에 정의된 권한(SYSTEM_MANAGED) 외 사용자 정의 정책을 생성하여 권한을 부여할 수 있으며, 사용자 정의 정책을 사용하는 경우 상품 별 가상자원 대상 및 액션 권한 수준까지 세부적으로 권한 관리를 적용할 수 있습니다.

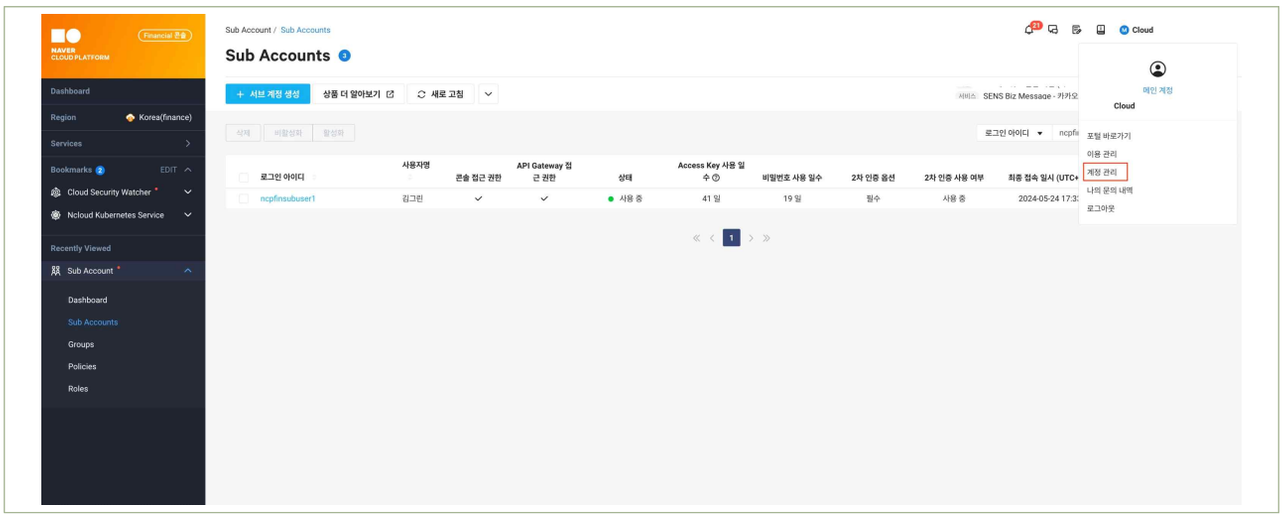
메인계정에 대한 추가인증 수단 및 접근 허용 IP 제한 적용

① **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ 상품을 선택합니다.



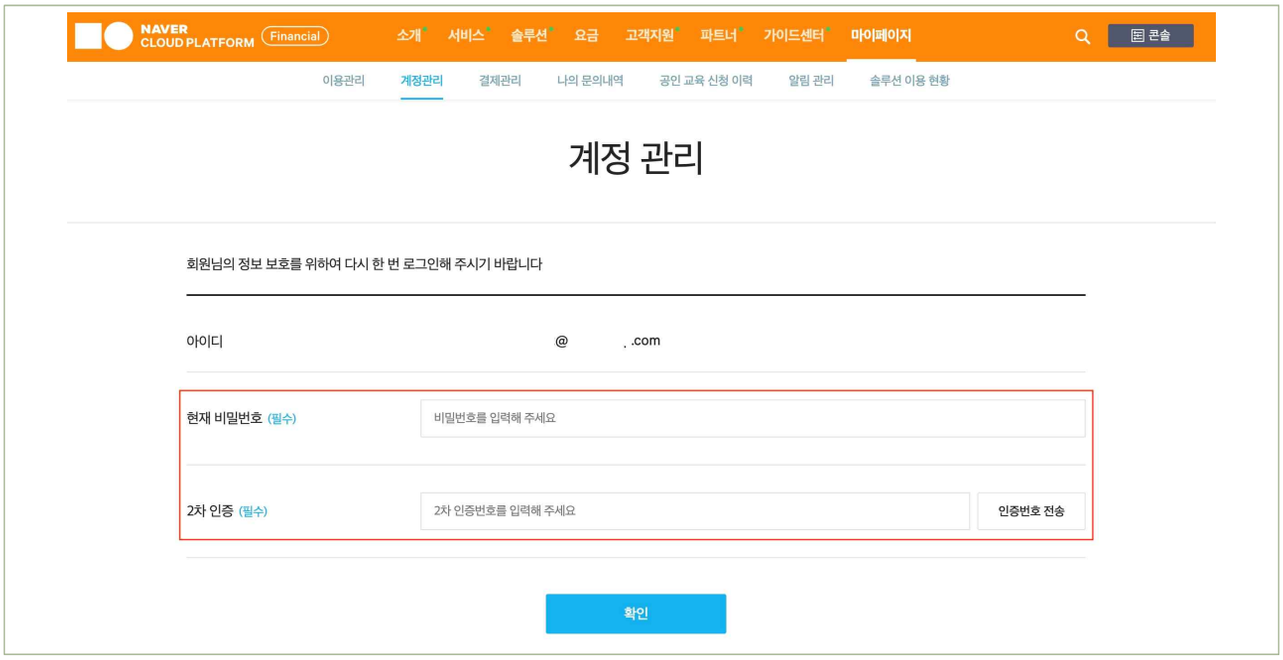
| 그림 3-1-8 | Sub Account 상품 선택

② **(가상자원관리시스템)** 우측 상단 ‘메인계정’ 선택 → ‘계정 관리’를 클릭하여 네이버 클라우드 플랫폼 포털의 계정 관리 페이지에 접속합니다.



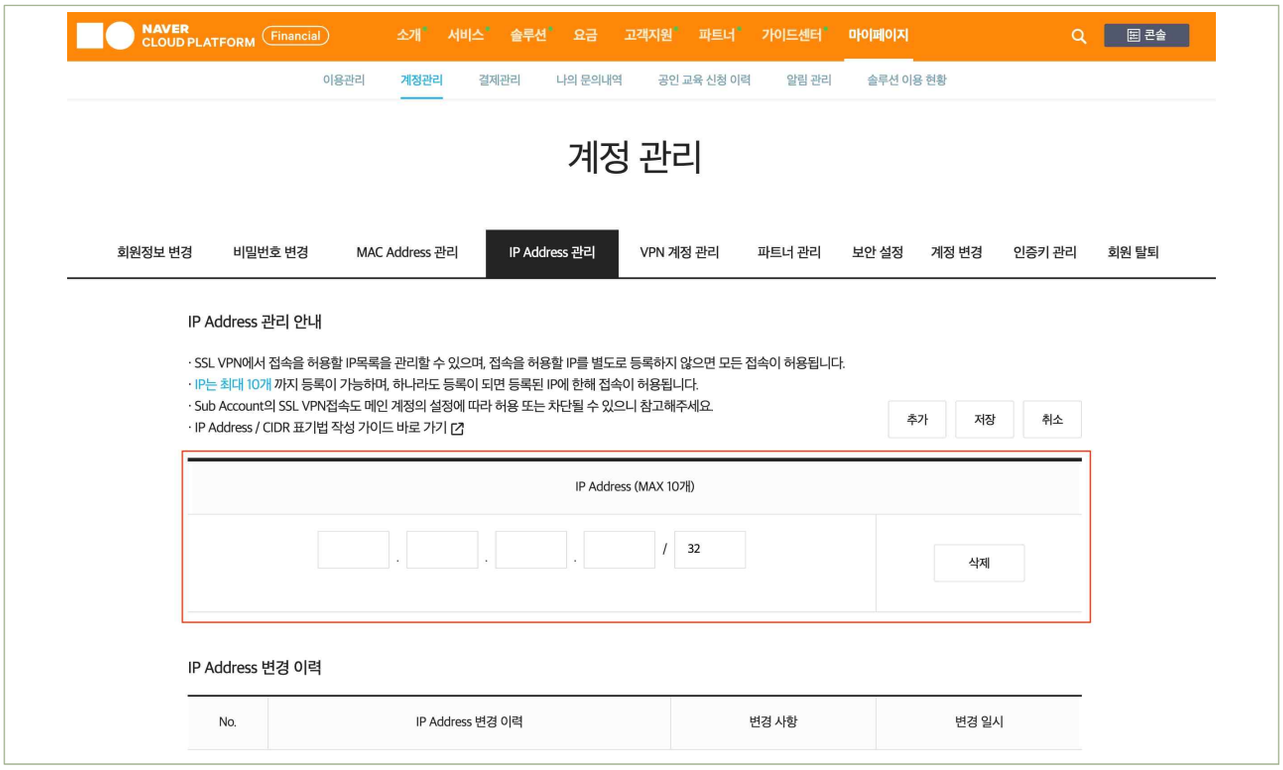
| 그림 3-1-9 | 메인계정의 계정 관리 선택

③ **(네이버 클라우드 플랫폼 포털)** 메인 계정의 정보 수정을 위해 비밀번호화 2차 인증을 수행합니다.



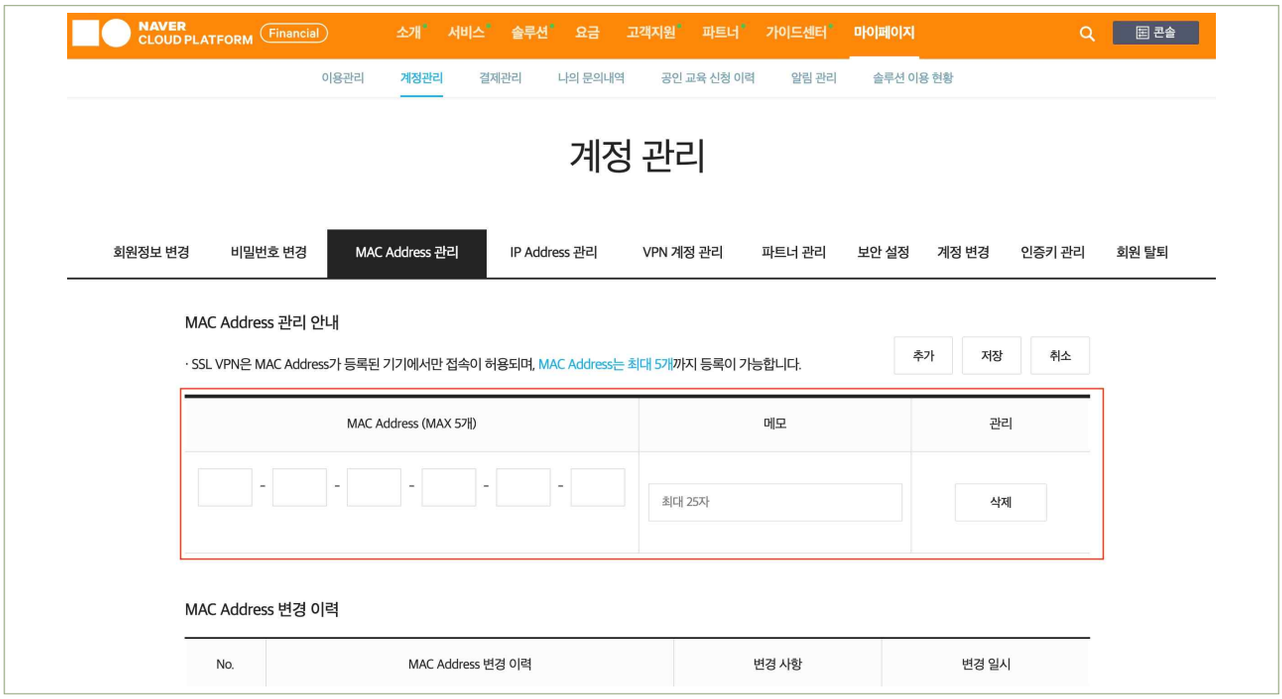
| 그림 3-1-10 | 메인계정 수정을 위한 재인증

④ **(네이버 클라우드 플랫폼 포털)** 'IP Address 관리' → '추가'를 통해 메인계정이 로그인 가능한 IP대역을 정의합니다.



| 그림 3-1-11 | 메인계정 로그인 IP 제한 예시

⑤ **(네이버 클라우드 플랫폼 포털)** ‘MAC Address 관리’ → ‘추가’를 통해 메인계정이 로그인 가능한 단말기의 MAC Address를 정의합니다.



| 그림 3-1-12 | 메인계정 단말기 MAC Address 제한 예시

API를 통한 서브계정 생성

① **(API(CLI))** ‘sub-account’ API를 통해 사용자 별 서브계정을 생성합니다.

- 요청 예시 (API)

```
POST https://subaccount.apigw.fin-ntruss.com/api/v1/sub-accounts
```

- 요청 예시 (Body)

```
{
    “active”: “ture”,
    “canAPIGatewayAccess”: “false”,
    “canConsoleAccess”: “ture”,
    “loginId”: “string”,
    “name”: “string”,
    “needPasswordGenerate”: “ture
}
```

- 응답 예시

```
{
    “success”: true,
    “id”: “subAccountId”,
    “generatedPassword”: “Pa$$w0rd”
}
```

| 그림 3-1-13 | 서브계정 생성 예시

4 참고 사항

- [참고1] 서브계정 생성 및 관리 가이드
- [참고2] 정책 및 역할 관리
- [참고3] 서브계정 생성 API 사용 가이드

1 기준

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

2 설명

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

  - 예시

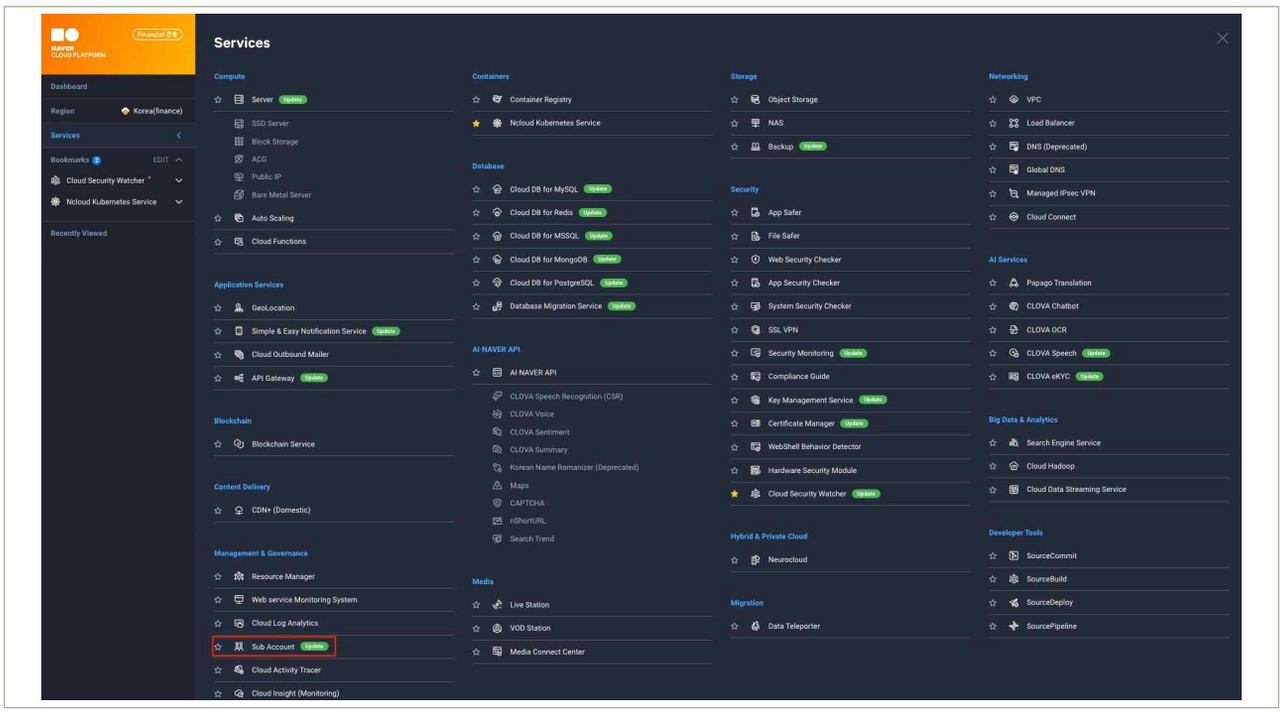
    1) IAM(Identity and Access Management) 기능 등을 이용하여 이용자별 인증수단 적용
    2) 업무 중요도에 따른 MFA 추가 인증(OTP, 바이오인증 등) 고려

3 우수 사례

- 네이버 클라우드 플랫폼은 Sub Account를 통해 가상자원관리시스템(클라우드 콘솔)에 접근 가능한 서브 계정를 생성하고 관리할 수 있습니다. 네이버 클라우드 플랫폼의 금융 클라우드에서는 이용자별 독립적인 서브 계정을 생성하는 경우, 기본 ID와 비밀번호 인증 외에 개인별 SMS, E-mail, OTP 등 소유 기반의 MFA가 필수로 적용되어 있으므로 모든 서브계정의 로그인 단계에서 MFA 등록 절차가 진행됩니다.

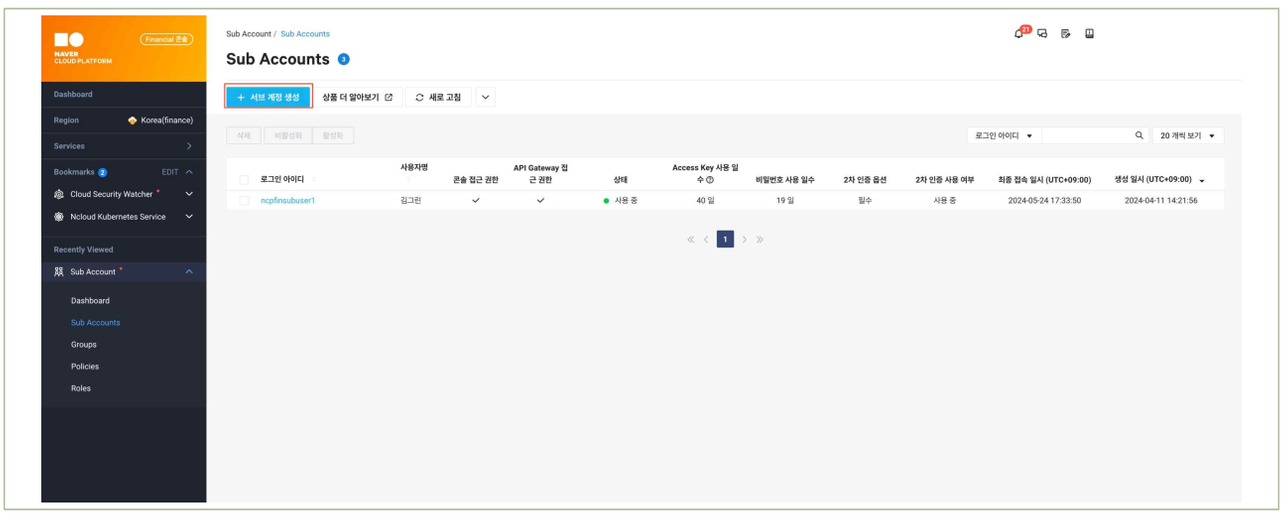
서브계정의 추가 인증수단 적용

① **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ 상품을 선택합니다.



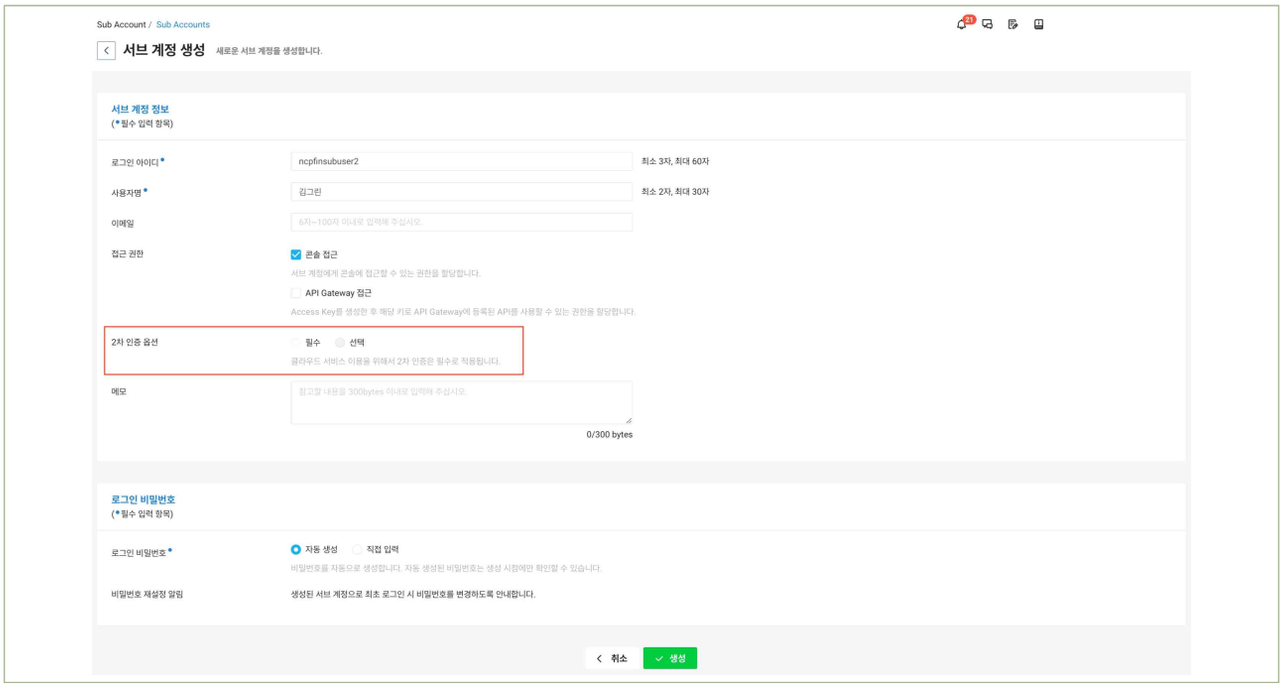
| 그림 3-2-1 | Sub Account 상품 선택

② **(가상자원관리시스템)** ‘Sub Accounts’ → ‘+ 서브 계정 생성’을 통해 가상자원 관리 계정을 생성합니다.



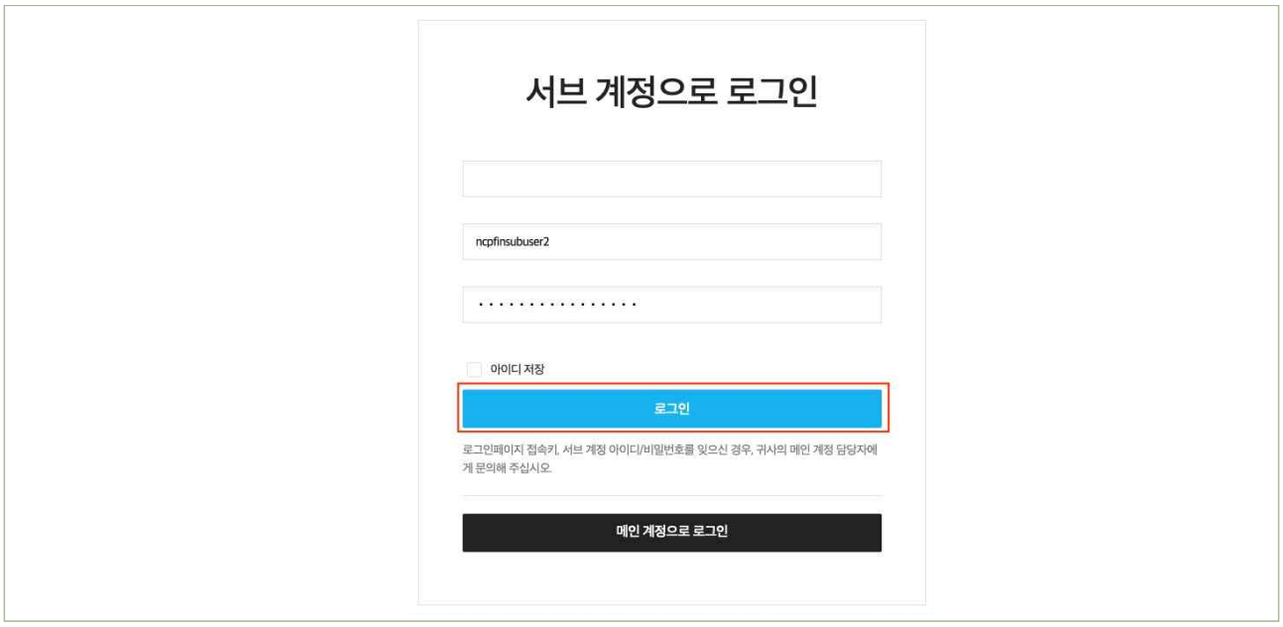
| 그림 3-2-2 | 서브계정 생성 예시

③ **(가상자원관리시스템)** 서브 계정 생성 시, ID, 비밀번호를 필수로 입력하여 서브계정을 생성합니다. (네이버 클라우드 플랫폼의 금융 클라우드는 2차 인증 옵션의 기본값은 선택이며, 수정할 수 없습니다.)



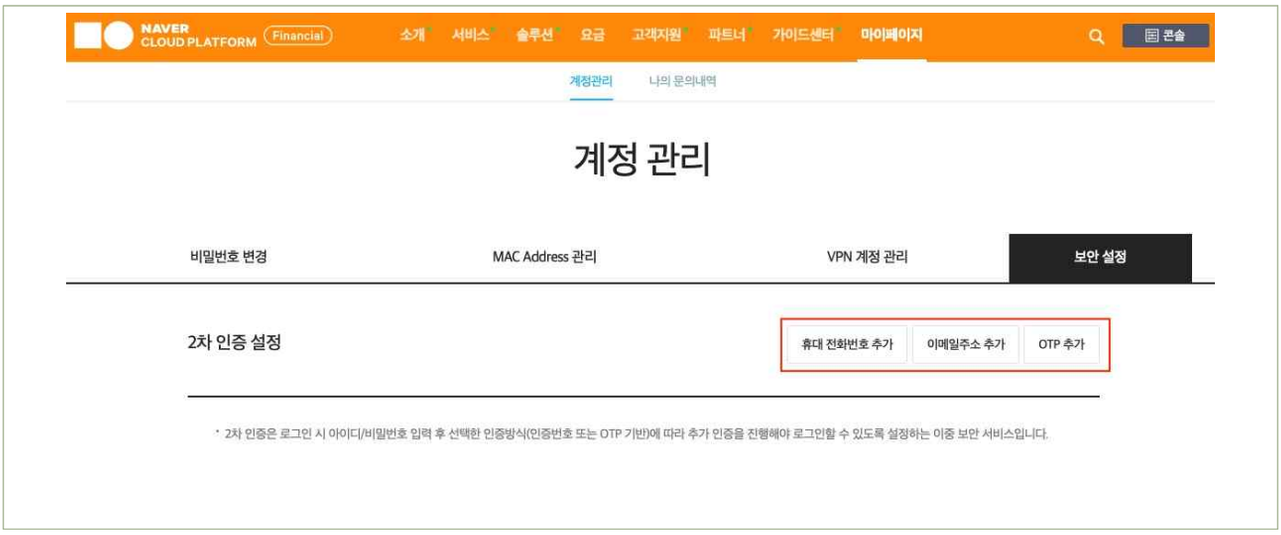
| 그림 3-2-3 | 서브 계정의 추가 인증수단 적용 예시

④ **(네이버 클라우드 플랫폼 포털)** 생성된 서브계정의 ID, 비밀번호와 접속키를 통해 가상자원 관리시스템에 로그인합니다.



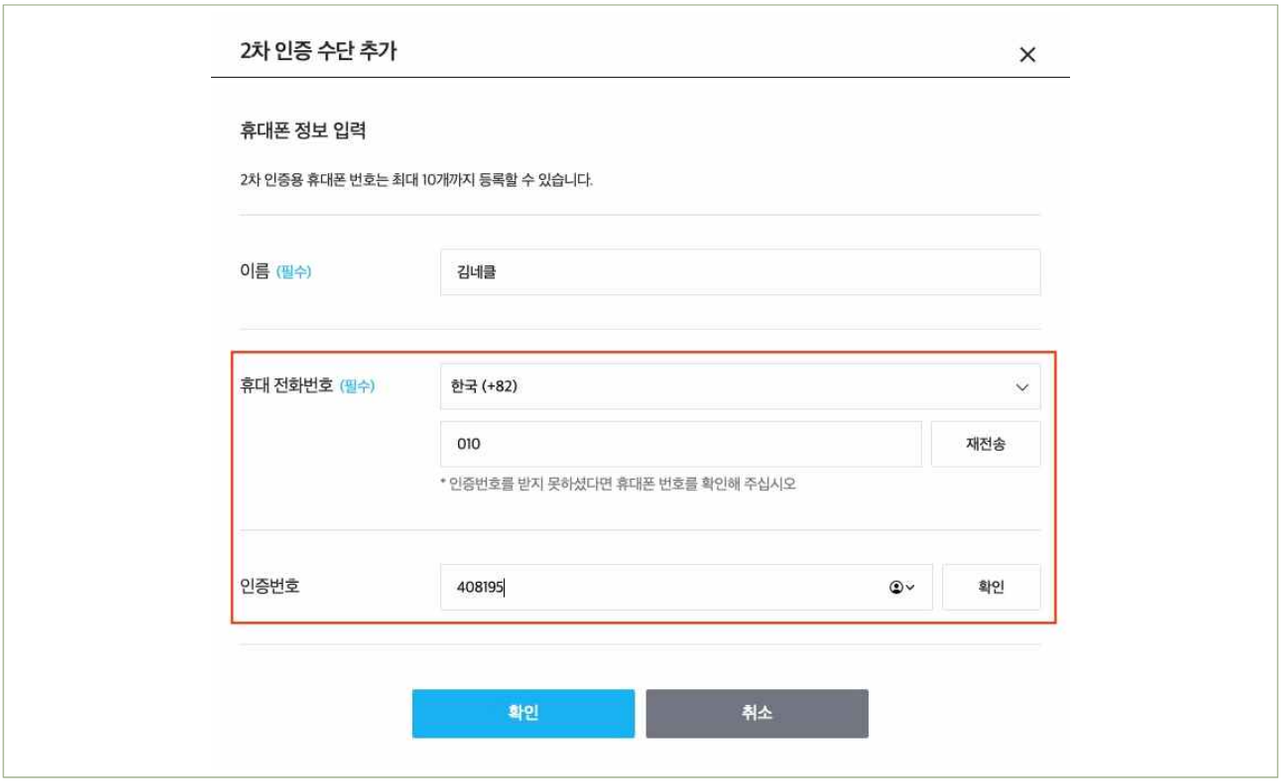
| 그림 3-2-4 | 서브 계정 로그인

⑤ **(네이버 클라우드 플랫폼 포털)** 서브계정의 최초 로그인 시 다음과 같이 2차 인증 설정을 진행하게 되며, 적절한 인증 수단을 선택하여 2차 인증을 설정합니다.



| 그림 3-2-5 | 서브 계정 2차 인증 수단 선택

⑥ **(네이버 클라우드 플랫폼 포털)** 인증 수단으로 휴대 전화번호를 선택한 경우, 인증번호의 확인을 통해 전화번호를 등록합니다.



| 그림 3-2-6 | 휴대 전화번호 인증 예시

⑦ **(네이버 클라우드 플랫폼 포털)** 2차 인증 수단 등록 완료 이후 로그인부터 다음과 같이 등록된 인증수단을 통해 인증번호를 확인하여 로그인을 진행합니다.

| 그림 3-2-7 | 로그인 시 2차 인증 확인

API를 통한 서브계정 생성

① **(API(CLI))** 'sub-account' API를 통해 사용자 별 서브계정을 생성합니다.

- 요청 예시 (API)

```
POST https://subaccount.apigw.fin-ntruss.com/api/v1/sub-accounts
```

- 요청 예시 (Body)

```
{
    "active": "ture",
    "canAPIGatewayAccess": "false",
    "canConsoleAccess": "ture",
    "loginId": "string",
    "name": "string",
    "needPasswordGenerate": "ture
}
```

- 응답 예시

```
{
    "success": true,
    "id": "subAccountId",
    "generatedPassword": "Pa$$w0rd"
}
```

| 그림 3-2-8 | 서브계정 생성 예시

4 참고 사항

- [참고1] 서브계정 생성 및 관리 가이드
- [참고2] 서브계정 로그인 가이드
- [참고3] 서브계정 생성 API 사용 가이드

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

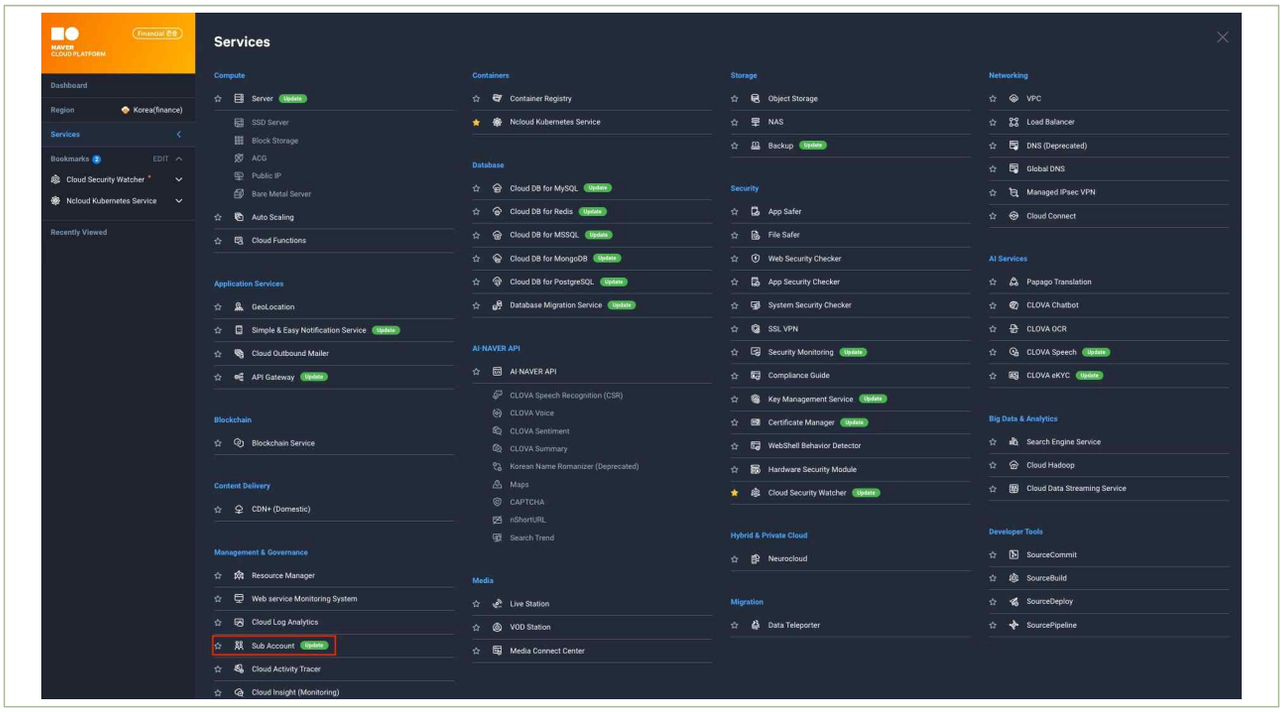
    2) 인사변경이 발생한 이용자가 공용 계정 이용 시 계정 비밀번호 변경 등

3 우수 사례

- 네이버 클라우드 플랫폼의 Sub Account 상품은 상시적으로 필요하지 않은 서브 계정을 비활성화 할 수 있습니다. 사용자는 이를 이용하여 주기적으로 임직원의 인사변경 여부 모니터링 결과에 따라 임직원의 서브 계정을 삭제하거나 비활성화하여 정지 상태로 변경하여야 합니다.

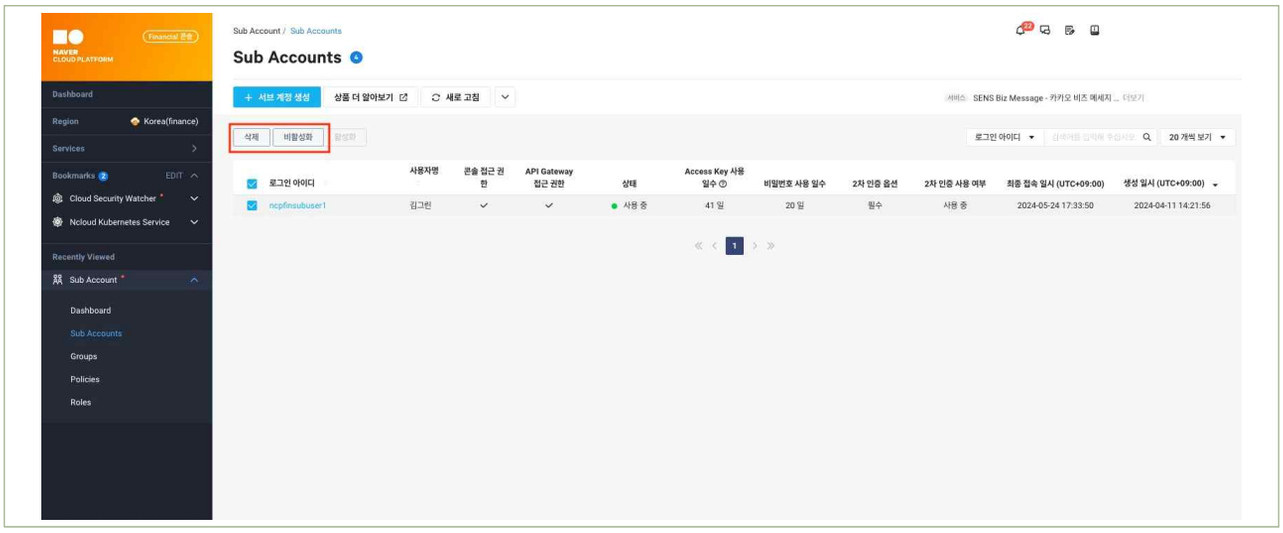
서브계정의 비활성화

① **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ 상품을 선택합니다.



| 그림 3-3-1 | Sub Account 상품 선택

② **(가상자원관리시스템)** ‘Sub Accounts’메뉴에서 비활성화 대상 서브계정을 선택하고 ‘삭제’ 또는 ‘비활성화’를 클릭합니다.



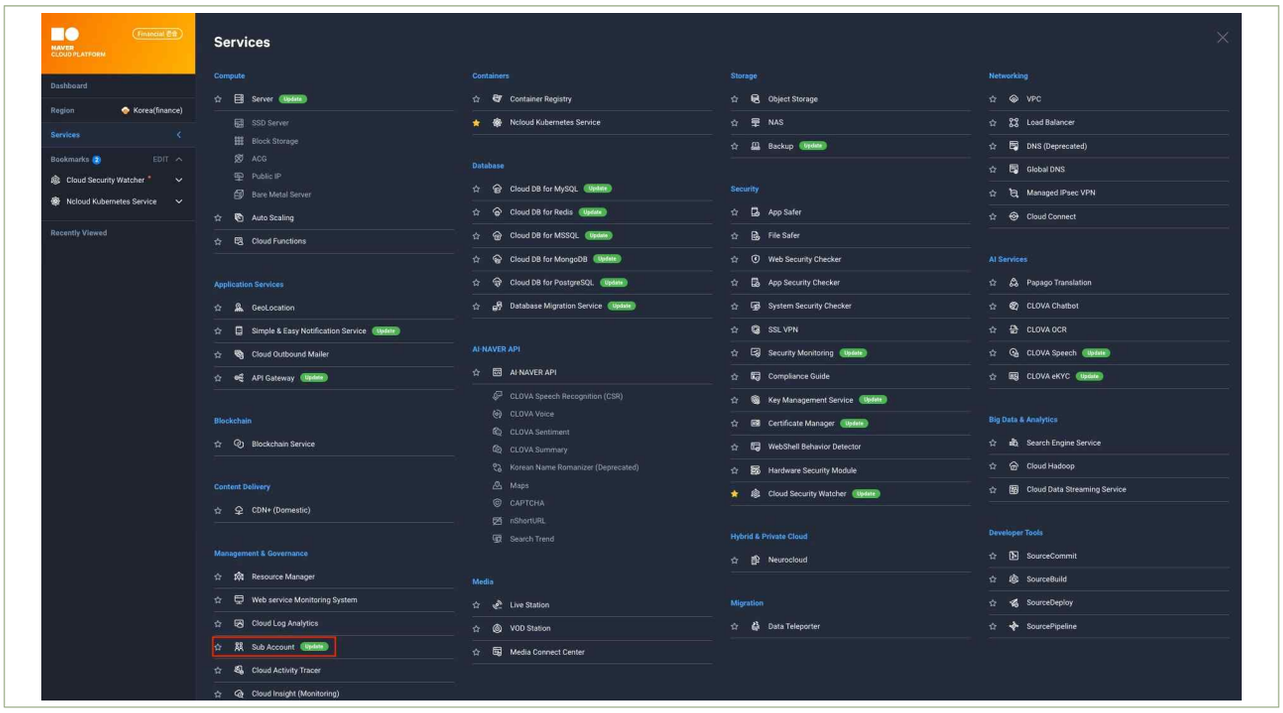
| 그림 3-3-2 | 서브계정 비활성화 예시

③ **(가상자원관리시스템)** 서브계정의 비활성화를 수행한 경우, 서브계정 목록에서 '상태'가 정지 상태로 변경되었는지 확인합니다.

| 그림 3-3-3 | 서브 계정의 비활성화 적용여부 확인

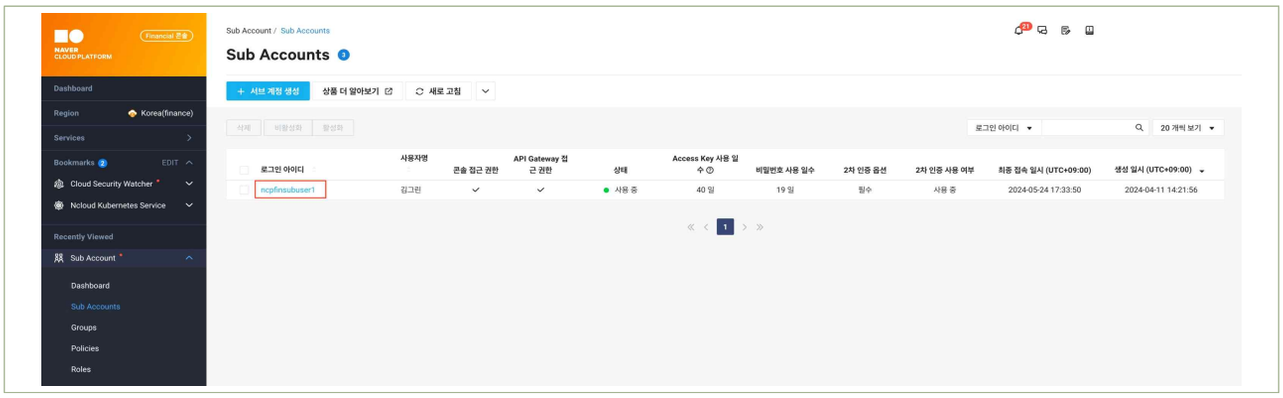
서브계정 비밀번호 초기화

① **(가상자원관리시스템)** 'Services' → 'Sub Account' 상품을 선택합니다.



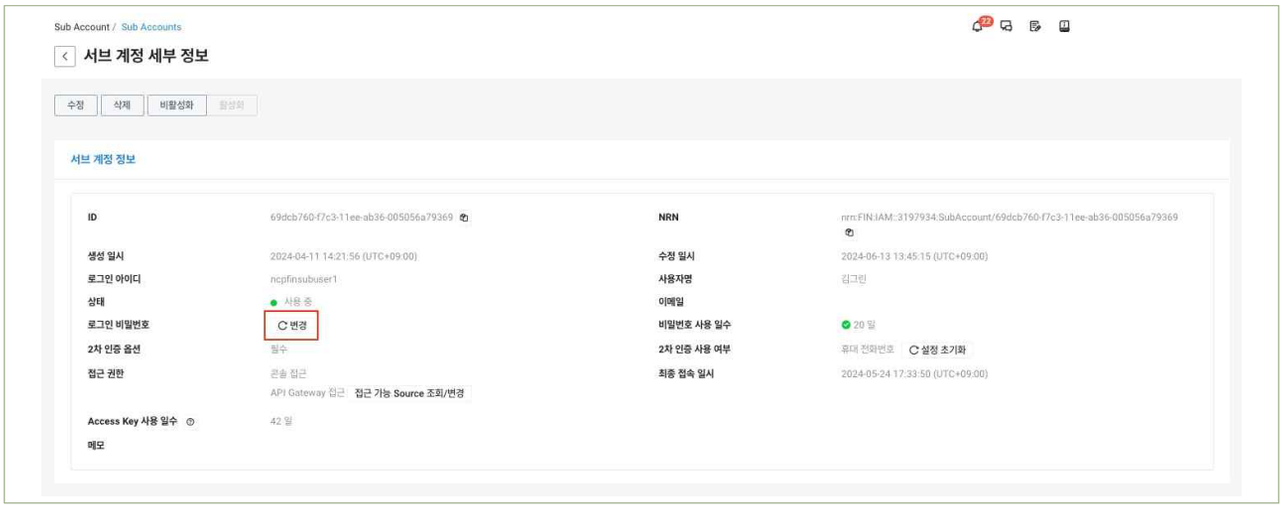
| 그림 3-3-4 | Sub Account 상품 선택

② **(가상자원관리시스템)** 비밀번호 변경 대상 서브계정(로그인 아이디)를 클릭합니다.



| 그림 3-3-5 | 비밀번호 변경 대상 서브계정 선택

③ **(가상자원관리시스템)** 서브계정 세부 정보에서 로그인 비밀번호 '변경'을 클릭합니다.



| 그림 3-3-6 | 서브 계정의 로그인 비밀번호 변경 예시

④ **(가상자원관리시스템)** 로그인 비밀번호를 '자동 생성' 또는 '직접 입력'하여 재설정 합니다.

| 그림 3-3-7 | 서브 계정의 로그인 비밀번호 변경 예시

※ 조직 내에서 SAML 표준을 이용한 Identity Provider (IdP) 계정이 존재하는 경우, 해당 계정을 통해 네이버 클라우드 플랫폼을 이용 및 계정별 접근 권한을 설정할 수 있도록 Ncloud Single Sign-On 상품과 연동할 수 있습니다. 이에 대한 보다 더 자세한 내용은 참고 사항의 링크를 참고하여 주시기 바랍니다.

API를 통한 서브계정 삭제

① **(API(CLI))** 'sub-accounts' API의 DELETE 메서드를 통해 서브 계정을 삭제합니다.

- 요청 예시

```
DELETE https://subaccount.apigw.fin-ntruss.com/api/v1/sub-accounts/{subAccountId}
```

- 응답 예시

```
{
    "success": true
}
```

| 그림 3-3-8 | API를 통한 서브 계정 삭제 예시

API를 통한 서브계정 비활성화

① **(API(CLI))** 'sub-accounts' API의 PUT 메서드를 통해 계정의 Active 파라미터를 수정하여 계정을 중지 상태로 변경합니다.

- 요청 예시 (API)

```
PUT https://subaccount.apigw.fin-ntruss.com/api/v1/sub-accounts/{subAccountId}
```

- 요청 예시 (Body)

```
{
    "active": "oolean",
    "canAPIGatewayAccess": "oolean",
    "canConsoleAccess": "oolean",
    "email": "string",
    "memo": "string",
    "name": "string",
        "useApiAllowSource": "oolean",
        "apiAllowSources": [
        {
            "type": "string",
            "source": "string"
        }
    ]
```

- 응답 예시

```
{
    "success": true,
    "id": "subAccountId"
}
```

| 그림 3-3-9 | API를 통한 서브 계정 비활성화 예시

4 참고 사항

- [참고1] 서브계정 삭제 가이드
- [참고2] 서브계정 비활성화 가이드
- [참고3] 서브계정 삭제 API 사용 가이드
- [참고4] 서브계정 비활성화 API 사용 가이드
- [참고5] Ncloud Single Sign-On 사용자 가이드

1 기준

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

2 설명

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

  - 예시

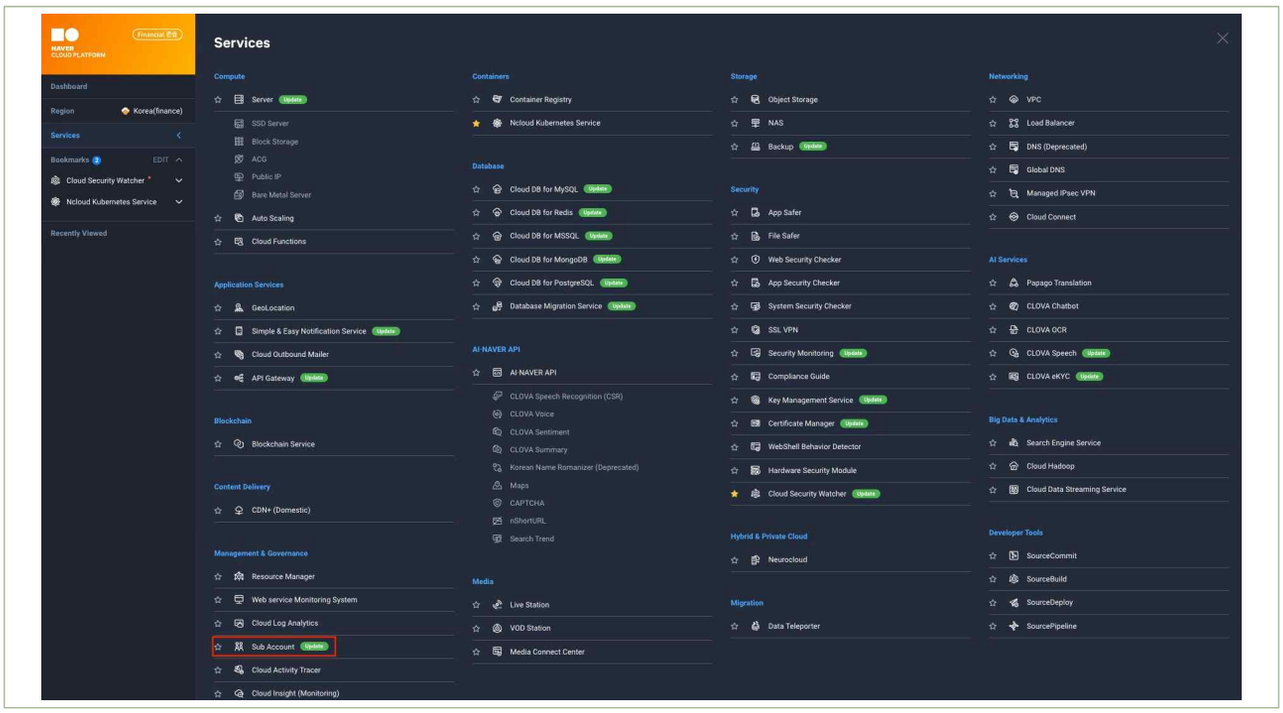
    1) 이메일 인증
    2) SMS 인증
    3) 별도 인증도구(OTP, 바이오인증 등) 활용 등

3 우수 사례

- 네이버 클라우드 플랫폼의 금융 클라우드는 서브 계정의 ID, 비밀번호 외 SMS, E-mail, OTP 등의 소유 기반 MFA는 필수로 적용되어 있으며, 서브 계정의 최초 로그인 시 2차 인증 수단은 필수로 설정하여야 합니다.

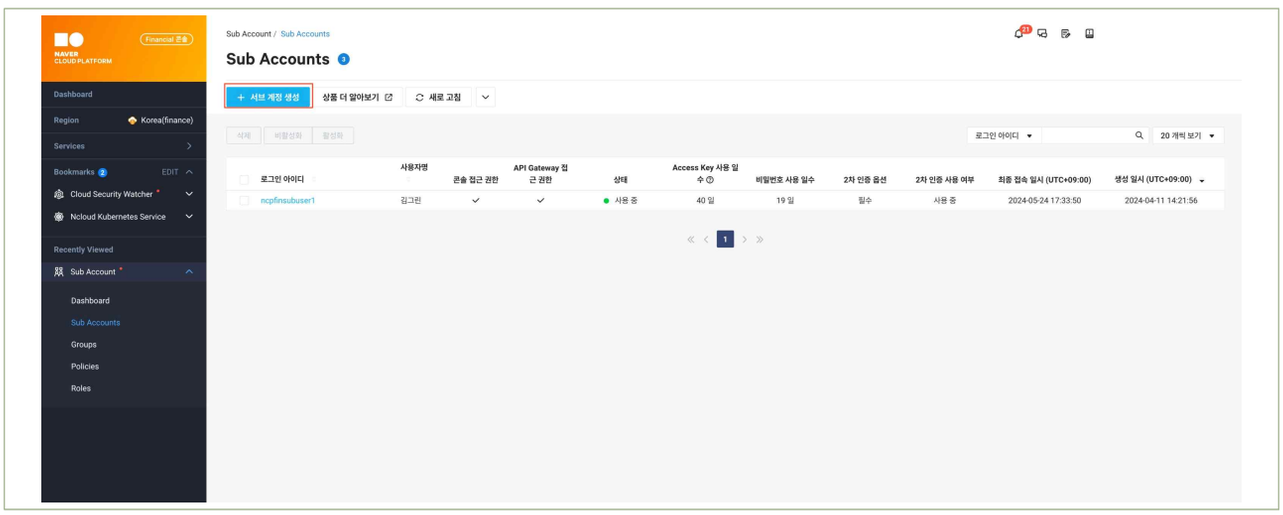
서브계정의 추가 인증수단 적용

① **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ 상품을 선택합니다.



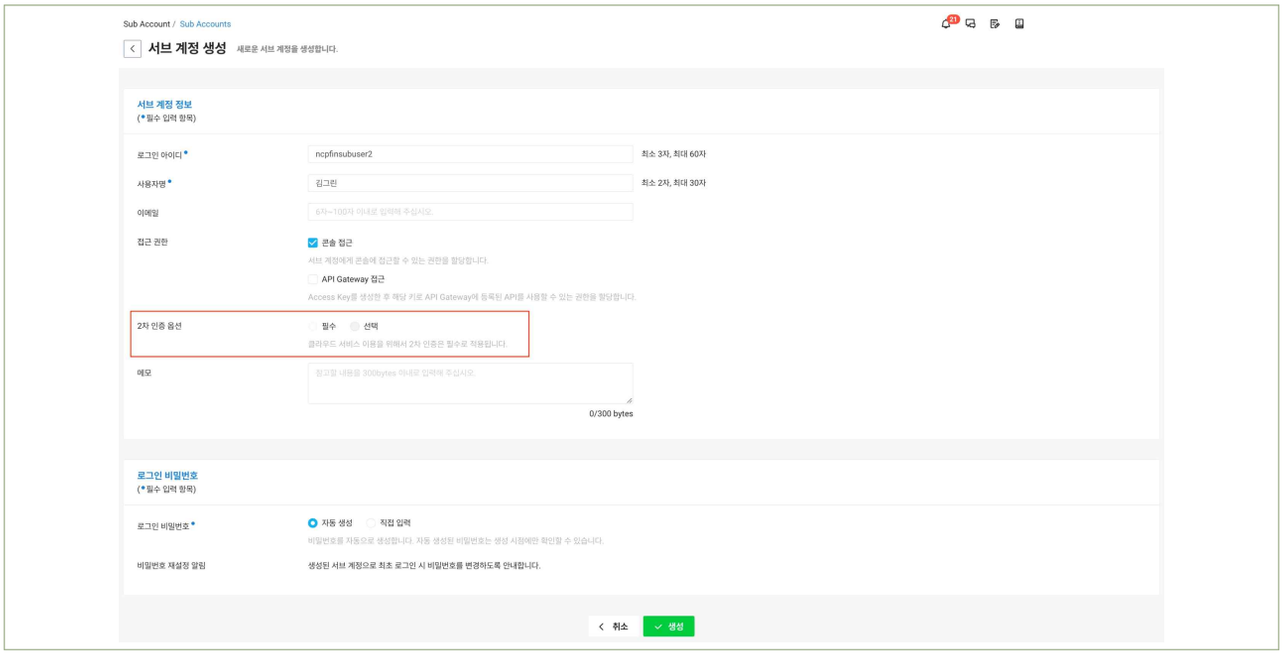
| 그림 3-4-1 | Sub Account 상품 선택

② **(가상자원관리시스템)** ‘Sub Accounts’ → ‘+ 서브 계정 생성’을 통해 가상자원 관리 계정을 생성합니다.



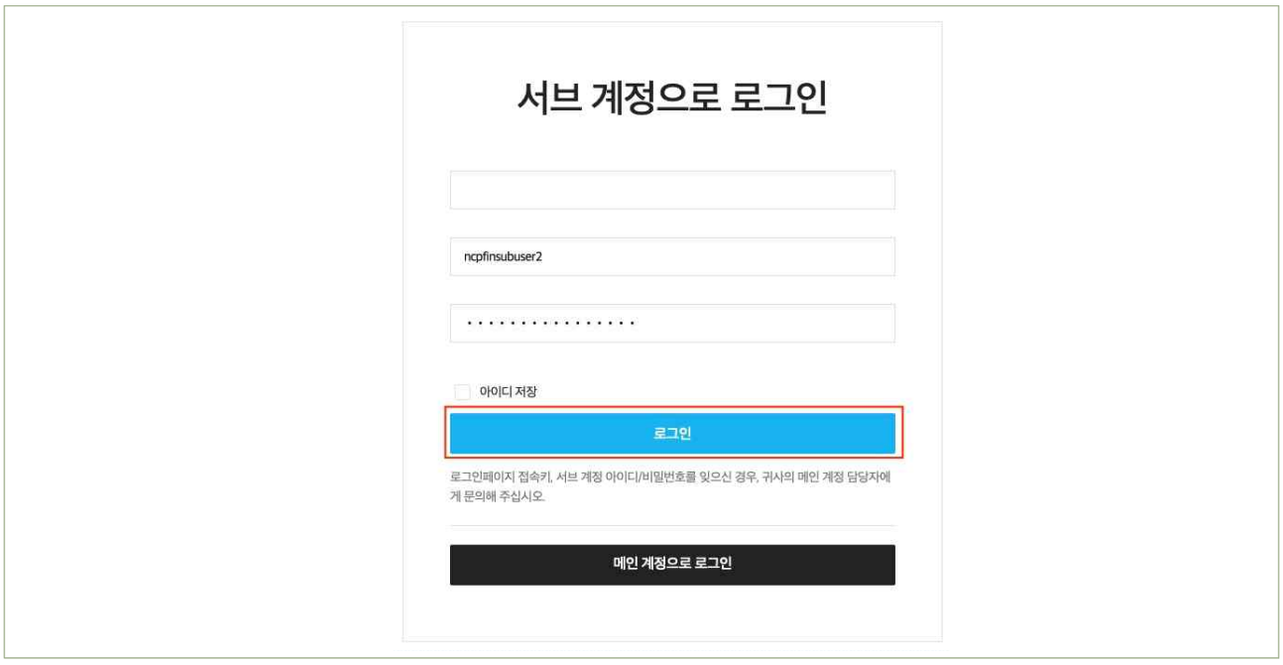
| 그림 3-4-2 | 서브계정 생성 예시

③ **(가상자원관리시스템)** 서브 계정 생성 시, ID, 비밀번호를 필수로 입력하여 서브계정을 생성합니다. (네이버 클라우드 플랫폼의 금융 클라우드는 2차 인증 옵션의 기본값은 선택이며, 수정할 수 없습니다.)



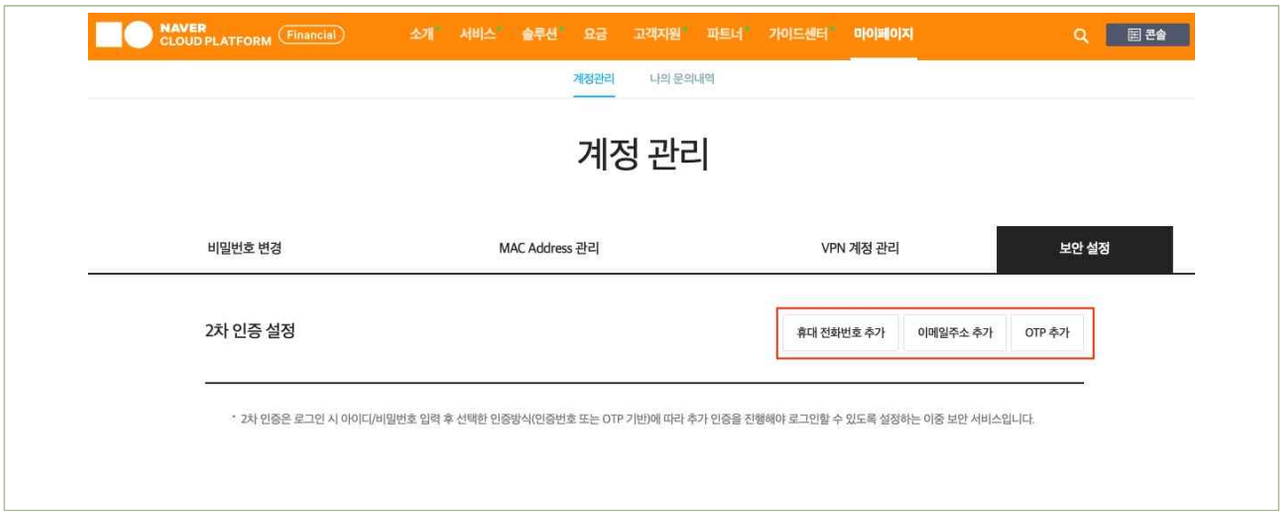
| 그림 3-4-3 | 서브 계정의 추가 인증수단 적용 예시

④ **(네이버 클라우드 플랫폼 포털)** 생성된 서브계정의 ID, 비밀번호와 접속키를 통해 가상자원 관리시스템에 로그인합니다.



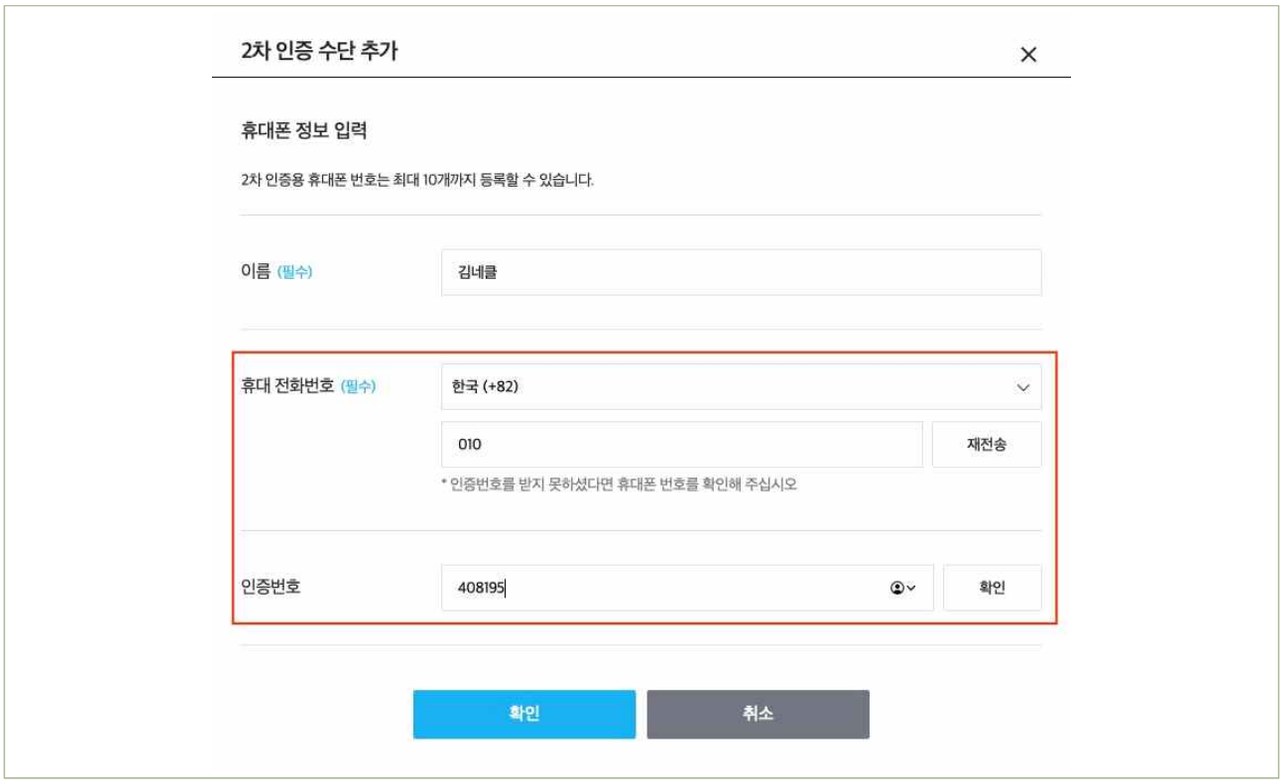
| 그림 3-4-4 | 서브 계정 로그인

⑤ **(네이버 클라우드 플랫폼 포털)** 서브계정의 최초 로그인 시 다음과 같이 2차 인증 설정을 진행하게 되며, 적절한 인증 수단을 선택하여 2차 인증을 설정합니다.



| 그림 3-4-5 | 서브 계정 2차 인증 수단 선택

⑥ **(네이버 클라우드 플랫폼 포털)** 인증 수단으로 휴대 전화번호를 선택한 경우, 인증번호의 확인을 통해 전화번호를 등록합니다.



| 그림 3-4-6 | 휴대 전화번호 인증 예시

⑦ **(네이버 클라우드 플랫폼 포털)** 2차 인증 수단 등록 완료 이후 로그인부터 다음과 같이 등록된 인증수단을 통해 인증번호를 확인하여 로그인을 진행합니다.

| 그림 3-4-7 | 로그인 시 2차 인증 확인

4 참고 사항

- [참고1] 서브계정 생성 및 관리 가이드
- [참고2] 서브계정 로그인 가이드

1 기준

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

2 설명

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

  - 예시

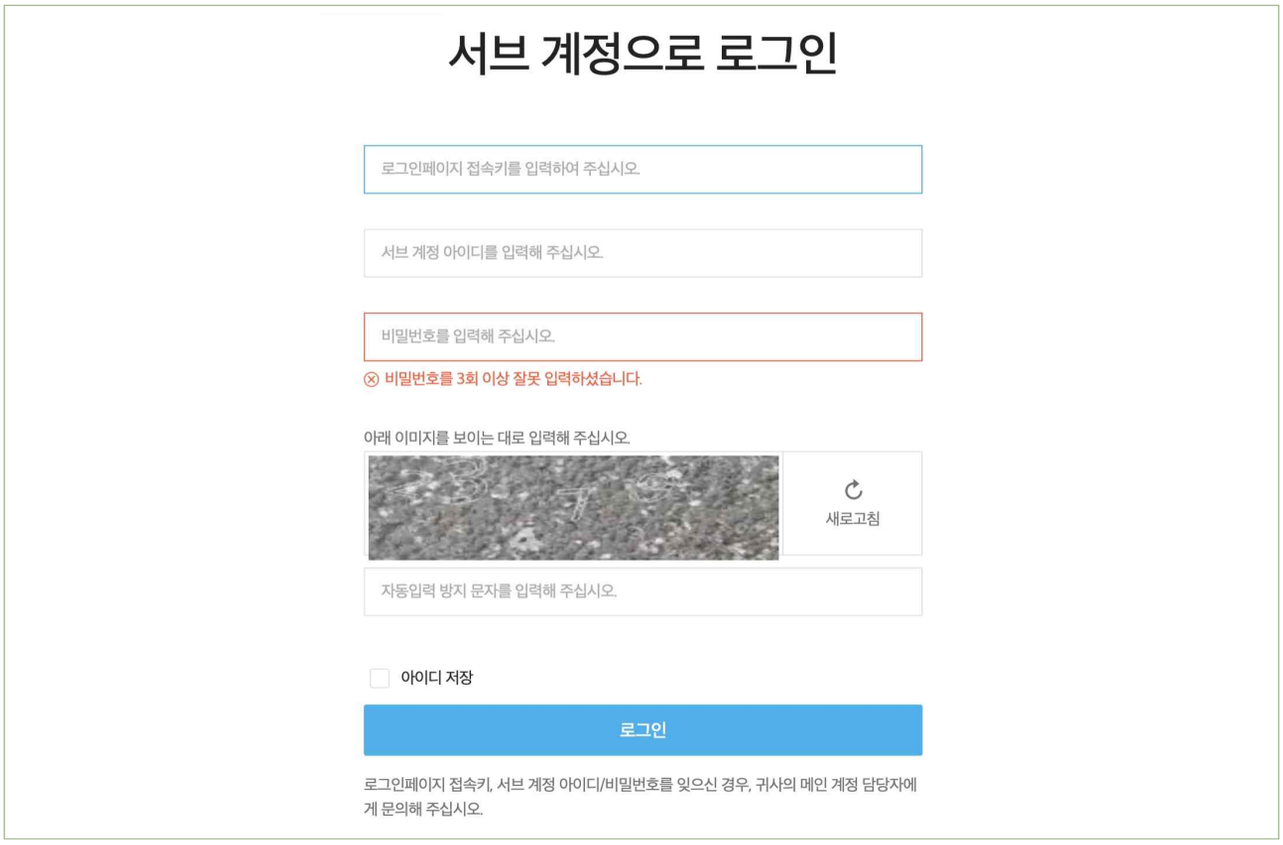
    1) 로그인 오류에 따른 보안통제 방안 수립 등

3 우수 사례

- 네이버 클라우드 플랫폼은 서브계정을 통해 로그인 시, 비밀번호를 5회 이상 잘못 입력할 경우 해당 서브 계정에 대한 로그인이 영구적으로 차단됩니다. 만약, 다시 로그인 하기 위해서는 메인계정 사용자가 서브 계정의 비밀번호를 재설정하여야 합니다.

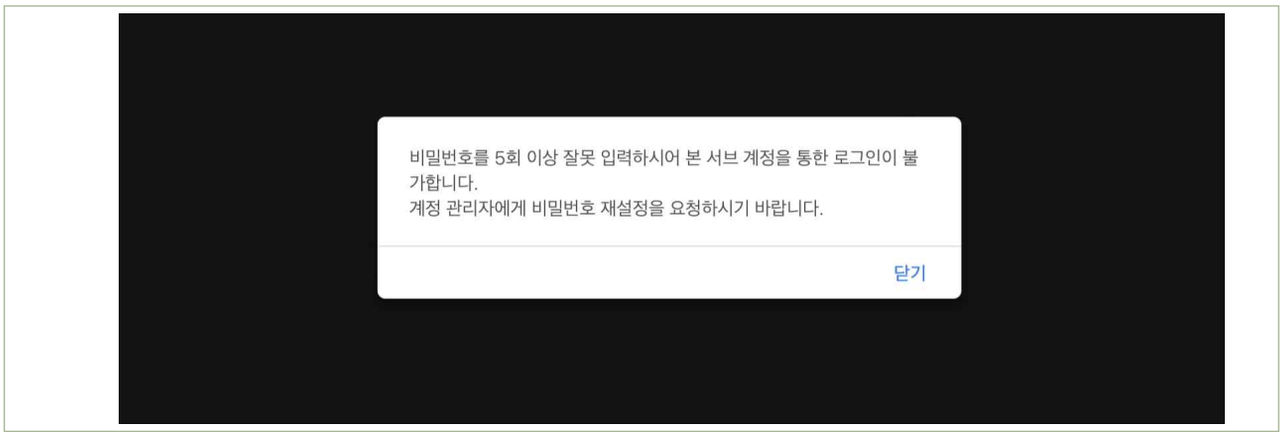
- **가상자원관리시스템(클라우드 콘솔) 비밀번호 입력 오류 방안**

  ① **(네이버 클라우드 플랫폼 포털)** 비밀번호 3회 이상 입력 오류 시, 무작위 대입 공격으로 인지하고 이를 차단하기 위해 자동입력 방지 문자 입력을 요구합니다.



| 그림 3-5-1 | 서브 계정 비밀번호 3회 입력 오류 예시

② **(네이버 클라우드 플랫폼 포털)** 비밀번호 5회 이상 입력 오류 시, 해당 서브계정의 로그인이 차단되며, 비밀번호 초기화 이후에만 정상 로그인이 가능합니다.



| 그림 3-5-2 | 서브 계정 비밀번호 5회 입력 오류 예시

4 참고 사항

- [참고1] 서브계정 로그인 가이드

1 기준

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

2 설명

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

  - 예시

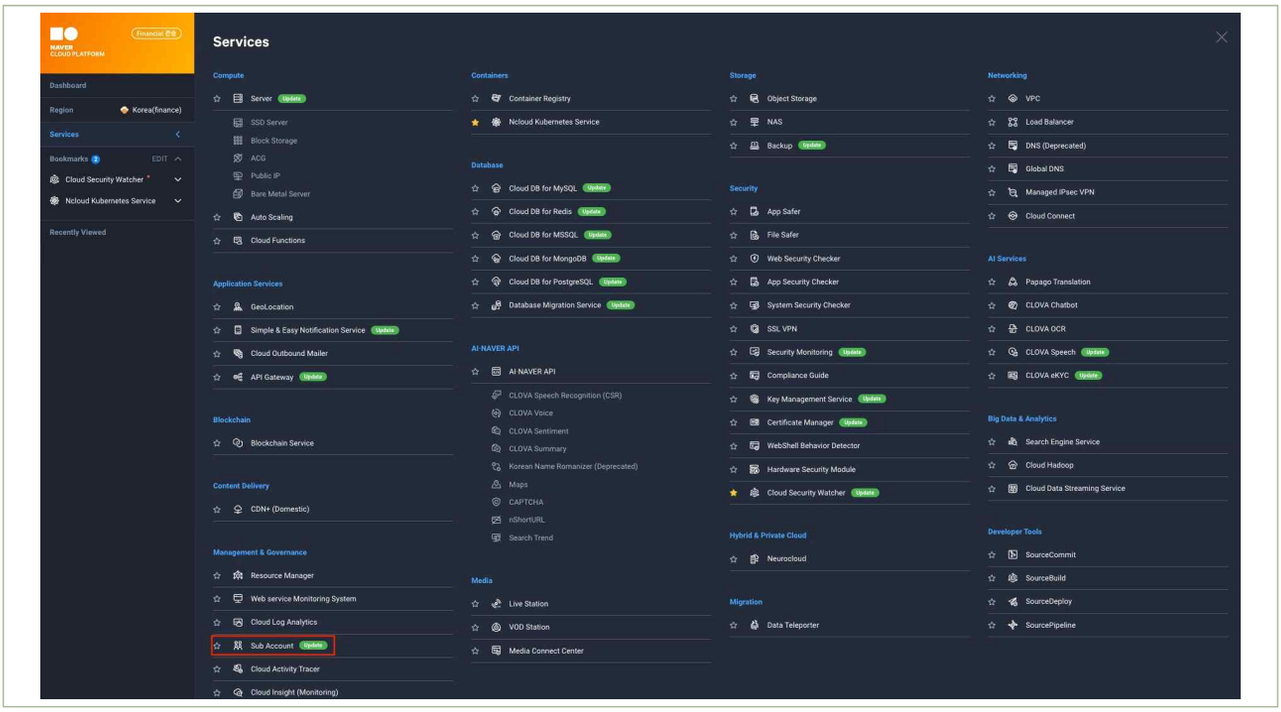
    1) 제3자가 쉽게 유추할 수 없는 비밀번호 작성 규칙 수립

3 우수 사례

- 네이버 클라우드 플랫폼의 서브 계정 비밀번호는 전자금융감독규정 제32조(내부사용자 비밀번호 관리) 등에 따라 안전한 비밀번호 규칙이 기본적으로 적용되어 있습니다. 따라서, 사용자는 영문자, 숫자, 특수문자를 조합하여 최소 8자 이상의 비밀번호를 입력하여야 합니다.

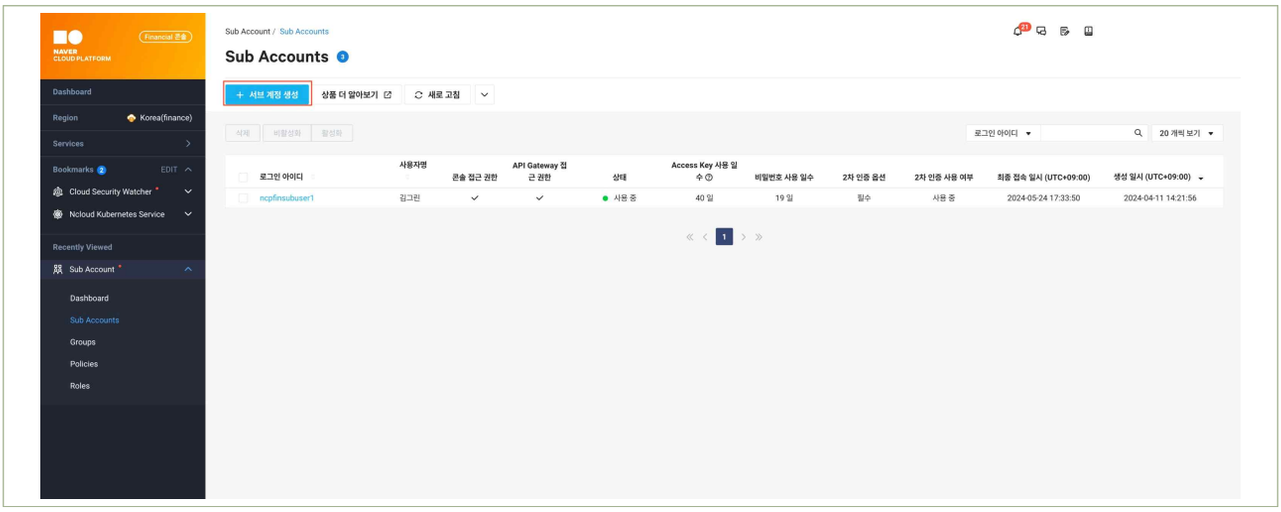
서브계정의 안전한 비밀번호 규칙 적용

① **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ 상품을 선택합니다.



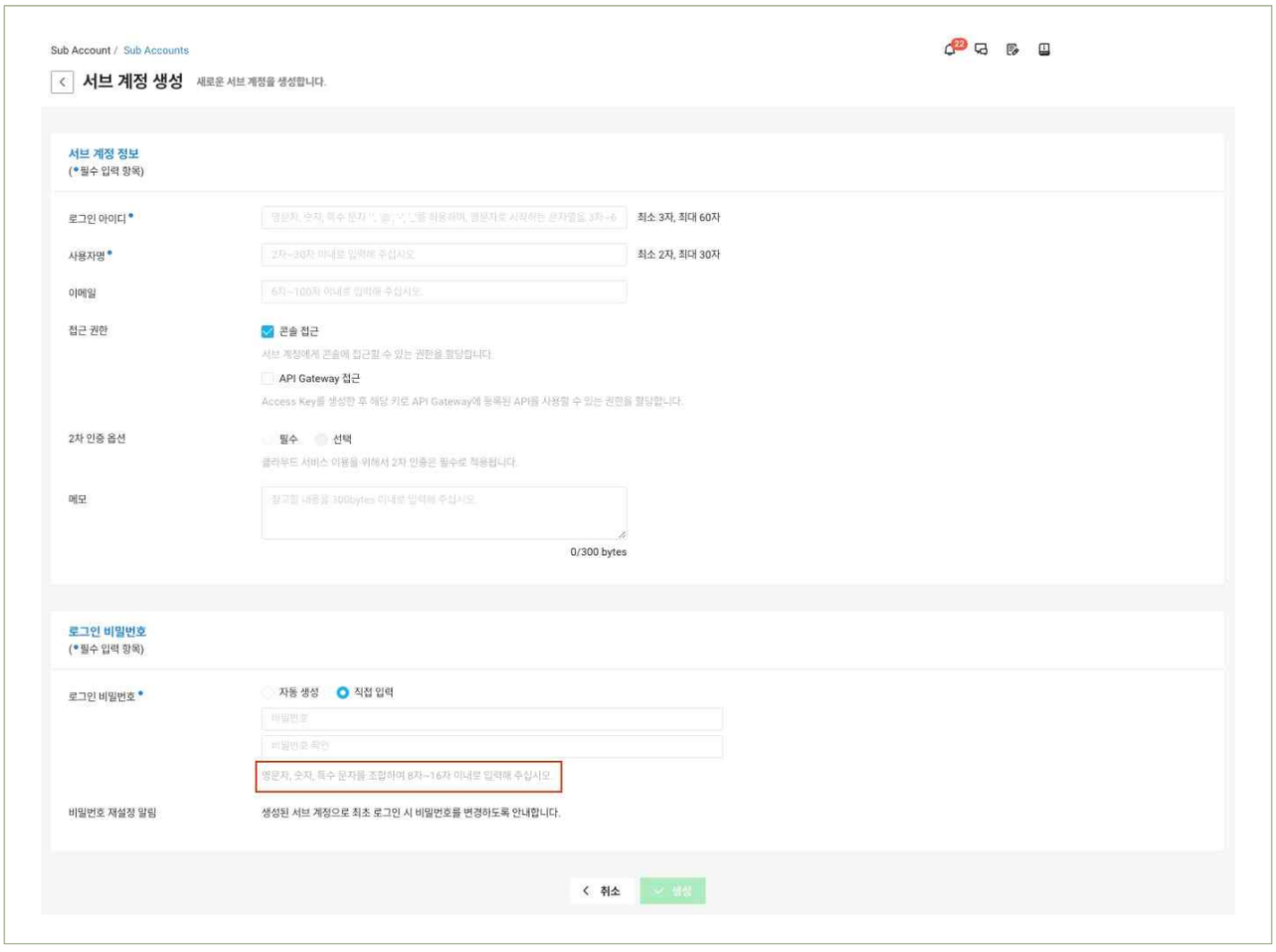
| 그림 3-6-1 | Sub Account 상품 선택

② **(가상자원관리시스템)** ‘Sub Accounts’ → ‘+ 서브 계정 생성’을 통해 가상자원 관리 계정을 생성합니다.



| 그림 3-6-2 | 서브계정 생성 예시

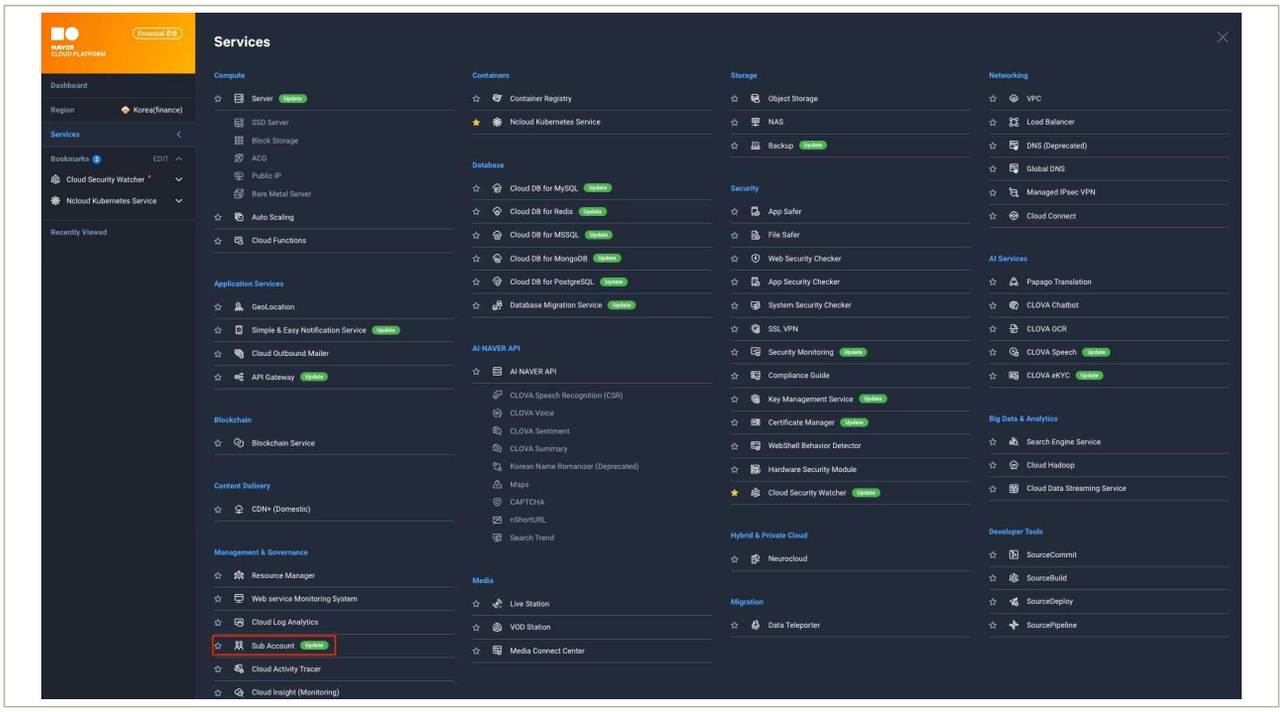
③ **(가상자원관리시스템)** 로그인 비밀번호를 '직접 입력'할 경우 안전한 비밀번호 규칙에 따라 비밀번호를 작성합니다.



| 그림 3-6-3 | 서브계정의 안전한 비밀번호 규칙 적용 예시

서브계정 비밀번호 만료 기한 적용

① **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ 상품을 선택합니다.



| 그림 3-6-4 | Sub Account 상품 선택

② **(가상자원관리시스템)** ‘Dashboard’메뉴의 비밀번호 만료 설정의 ‘설정’을 클릭합니다.

| 그림 3-6-5 | 비밀번호 만료 설정 예시

③ **(가상자원관리시스템)** 비밀번호 변경 주기 설정에서 비밀번호 변경을 활성화하고, 전자금융감독규정 등에 따라 변경 주기를 설정 합니다.

| 그림 3-6-6 | 비밀번호 만료 설정 예시

API를 통한 서브계정 비밀번호 복잡도 준수 여부 확인

① **(API(CLI))** 'check-password' API를 통해 서브 계정의 비밀번호의 복잡도 준수 여부를 확인합니다.

- 요청 예시

```
GET https://subaccount.apigw.fin-ntruss.com/api/v1/join/check-password
?password=String
```

- 응답 예시 (성공)

```
{
    "success": true,
    "message": ""
}
```

- 응답 예시 (복잡도 낮음)

```
{
    "success": false,
    "message": "안전하지 않은 비밀번호입니다."
}
```

| 그림 3-6-7 | API를 통한 안전한 비밀번호 체크 예시

API를 통한 서브계정 비밀번호 만료일 적용

① **(API(CLI))** 'sub-account-password-policy' API를 통해 서브 계정의 안전한 비밀번호 관리를 위해 비밀번호 만료일(유효기간)을 설정합니다.

- 요청 예시 (API)

```
POST https://subaccount.apigw.fin-ntruss.com/api/v1/tenant-settings/sub-account-password-policy
```

- 요청 예시 (Body)

```
{
    "passwordExpirationDays": "integer",
    "usePasswordExpiration": "oolean"
}
```

- 응답 예시

```
{
    "success": true
}
```

| 그림 3-6-8 | API를 통한 비밀번호 만료 설정 예시

4 참고 사항

- [참고1] 서브계정 비밀번호 만료 설정 가이드
- [참고2] 서브계정 비밀번호 복잡도 확인 API 사용 가이드
- [참고3] 서브계정 비밀번호 만료일 설정 API 사용 가이드

1 기준

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

2 설명

- 클라우드 환경을 통해 공개용 웹서버를 운영하는 경우 접근 계정을 적절하게 제한하여야 한다.

  - 예시

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

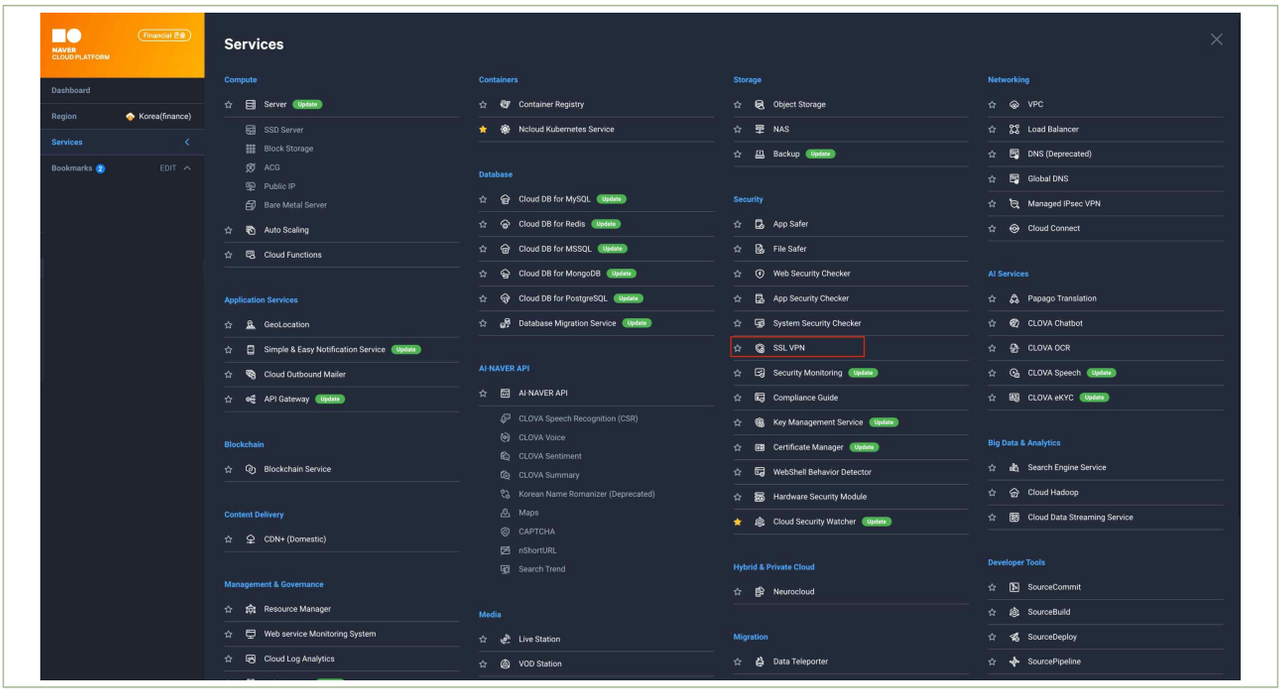
    2) 공개용 웹서버에 접근 가능한 계정으로 로그인 시 추가인증 수단 적용 등

3 우수 사례

- 네이버 클라우드 플랫폼은 사용자의 안전한 가상자원(Server) 접근을 위해 SSL VPN 보안상품의 사용을 권장하고 있습니다. SSL VPN 상품은 로그인 단계에서 사용자의 ID/Password 인증 외에도 SMS, Email 인증과 같은 추가 인증 수단을 통해 인증이 적용되어 있어 사용자는 가상자원(Server)에 안전한 인증절차를 통해 접근하도록 구성할 수 있습니다.

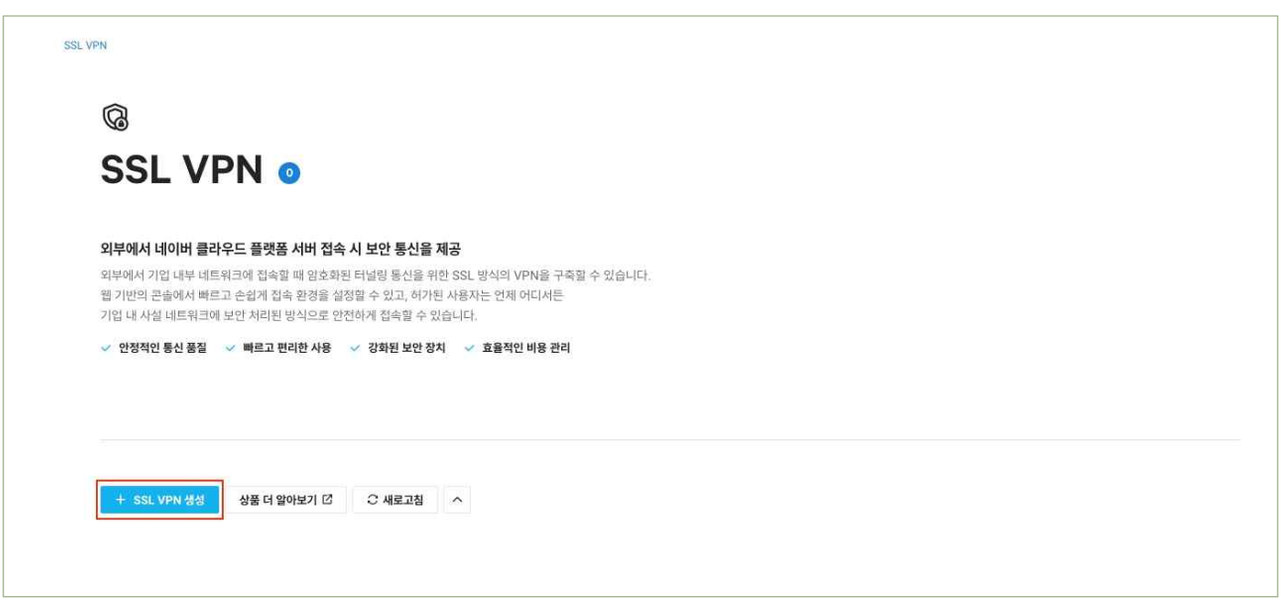
공개용 웹서버 계정 접근 시 추가인증 수단 확보

① **(가상자원관리시스템)** ‘Services’ → ‘SSL VPN’ 상품을 선택합니다.



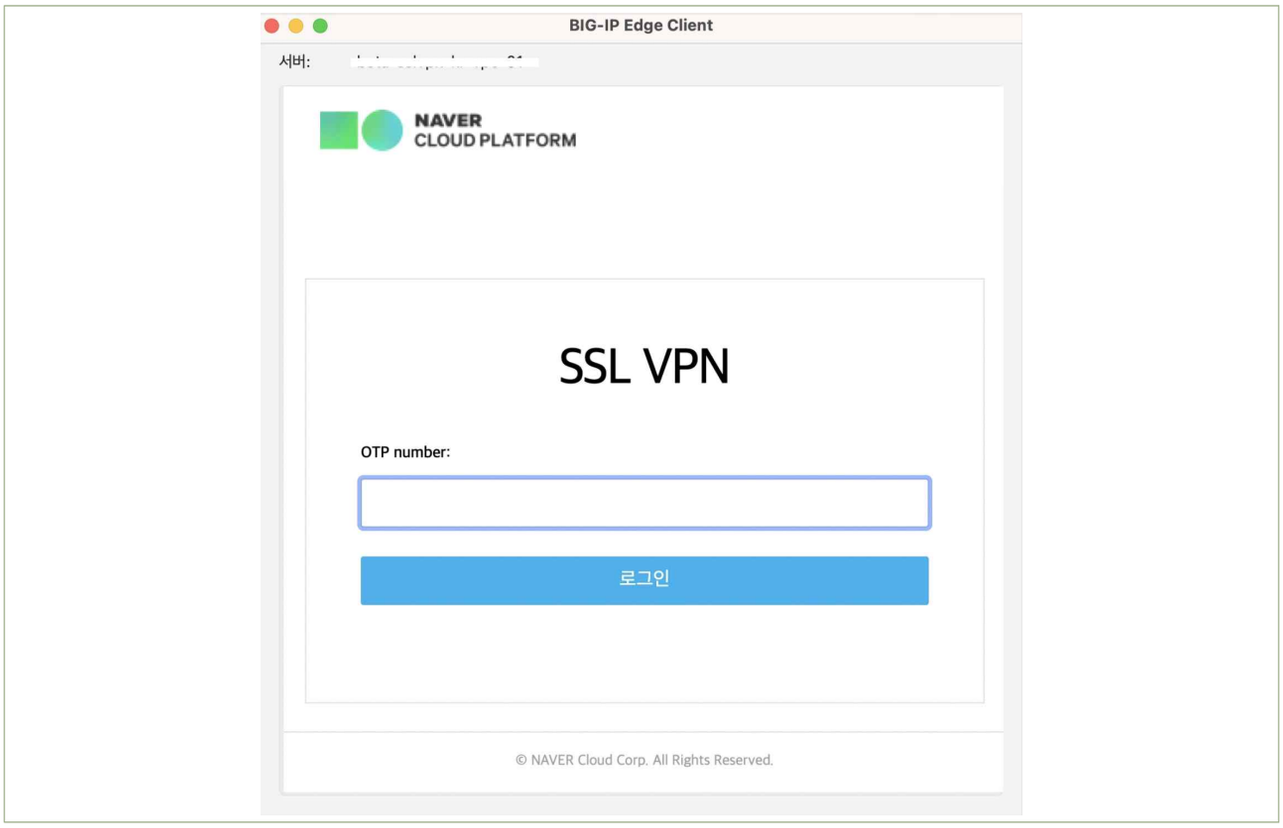
| 그림 3-7-1 | SSL VPN 상품 선택

② **(가상자원관리시스템)** ‘+ SSL VPN 생성’ 버튼을 클릭하여 SSL VPN 상품을 활성화 합니다.



| 그림 3-7-2 | SSL VPN 상품 활성화

③ **(PC)** SSL VPN Agent 다운로드(링크) 및 설치를 통해 가상자원(Server) 접근 시 ID/Password 인증과 추가 인증수단(SMS, Email)을 통해 접근합니다.



| 그림 3-7-3 | SSL VPN을 통한 추가 인증 수단 적용

- **마켓플레이스 보안 솔루션을 통한 공개용 웹서버 계정 접근 시 추가인증 수단 확보**

① **(네이버 클라우드 플랫폼 포털)** '솔루션' → '마켓플레이스'를 클릭합니다.

| 그림 3-7-4 | NCP 마켓플레이스

② **(네이버 클라우드 플랫폼 포털)** '검색창'에 서버접근통제, 서버보안 등의 3rd Party보안 솔루션을 검색합니다.

| 그림 3-7-5 | 3rd Party 보안 솔루션 검색

③ **(네이버 클라우드 플랫폼 포털)** 적합한 3rd Party 보안 솔루션의 선택 및 이용 신청을 통해 VPC내에 보안 솔루션을 구성하여 가상자원 루트 계정 접속 시 추가 인증수단을 적용합니다.

| 그림 3-7-6 | 3rd Party 보안솔루션 이용신청

※ 3rd Party 보안 솔루션 구성에 대한 보다 자세한 사항 및 문의는 마켓플레이스 기술 지원 탭에 안내된 연락처를 통해 문의하여 주시기 바랍니다.

4 참고 사항

- [참고1] SSL VPN Agent 설치 및 접속 가이드
- [참고2] SSL VPN Agent 다운로드
- [참고3] 네이버 클라우드 플랫폼 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, 신용정보법 등)에 따른 암호화 대상이 저장 및 처리되는 가상자원(서버, 스토리지 등)에 대한 암호화 기능 적용 여부를 확인하여야 한다.

  - 예시

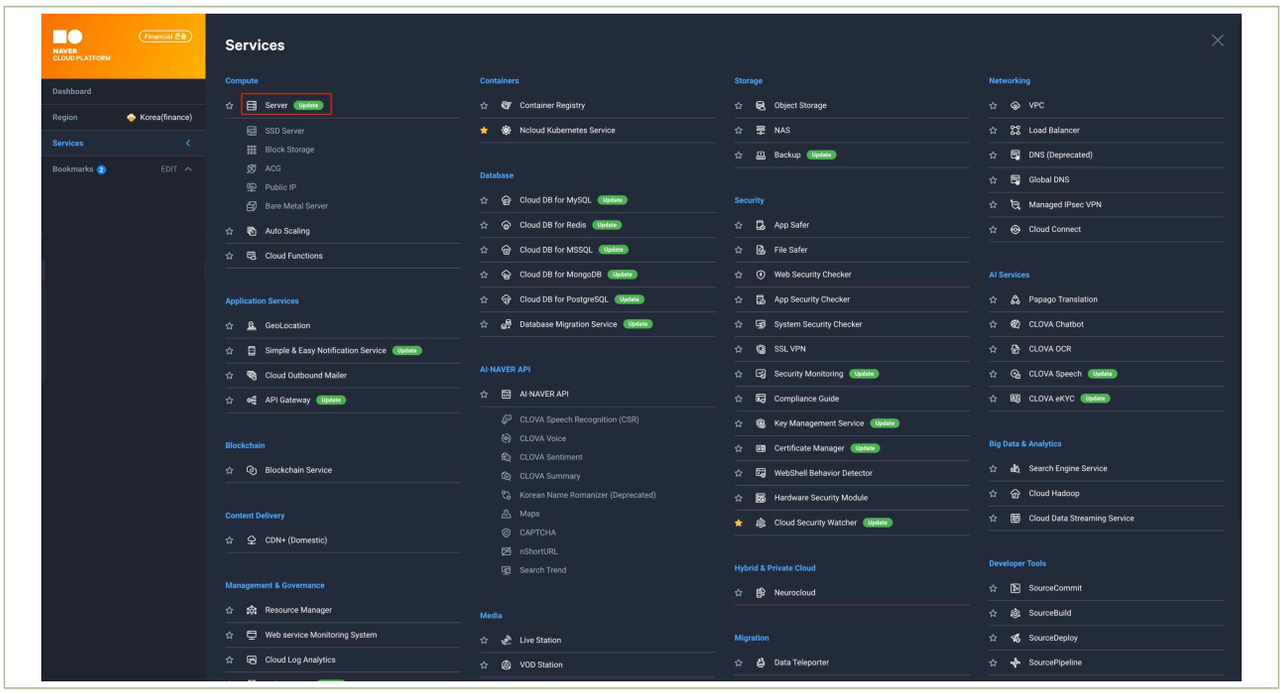
    1) 클라우드의 키 관리 서비스를 통해 CSP 사업자의 관리형 Key로 암호화
    2) 클라우드의 키 관리 서비스를 통해 이용자 관리형 Key로 암호화
    3) 이용자가 직접 관리하는 Key로 암호화 등

3 우수 사례

- 네이버 클라우드 플랫폼의 Key Management Service는 암호화 운용 및 구현을 위해 필수 요소인 암호 키를 관리할 수 있는 상품입니다. 사용자는 Key Management Service 상품을 통해 생성한 암호화 키를 이용하여 Object Storage의 버킷을 암호화할 수 있고, Server, Cloud DB와 같은 가상자원의 스토리지를 NCP 관리형 암호화 키로 암호화하여 사용자의 가상자산을 안전하게 보호할 수 있습니다.

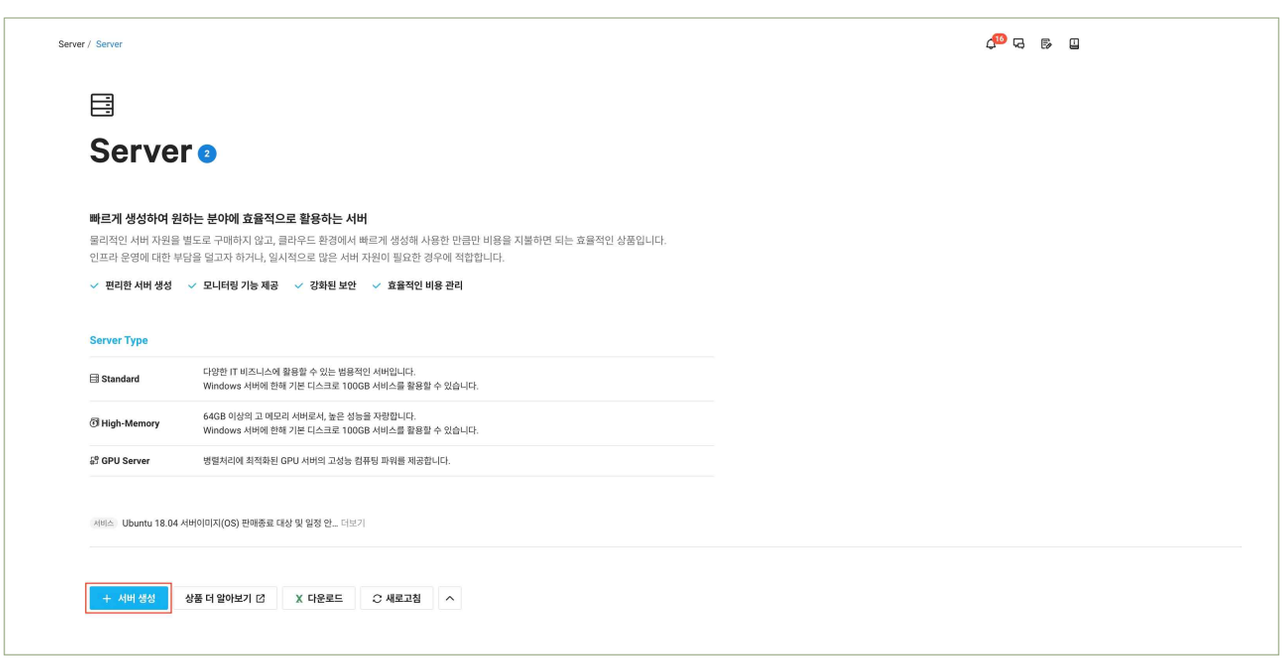
Server 스토리지 암호화 적용

① **(가상자원관리시스템)** ‘Services’ → ‘Server’ 상품을 선택합니다.



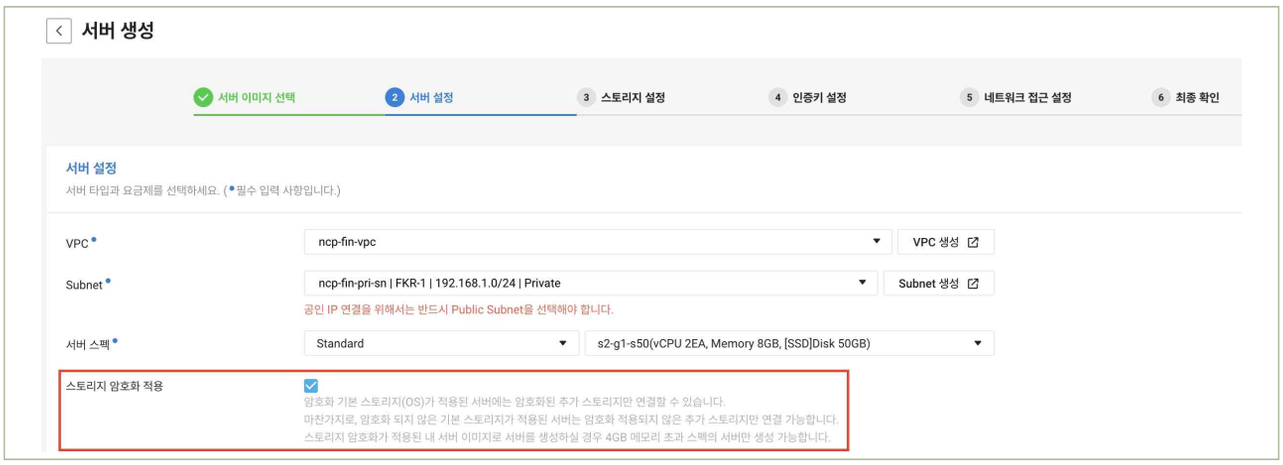
| 그림 4-1-1 | Server 상품 선택

② **(가상자원관리시스템)** ‘Server’ → ‘+ 서버 생성’을 클릭하여 가상자원(Server)를 생성합니다.



| 그림 4-1-2 | Server 생성

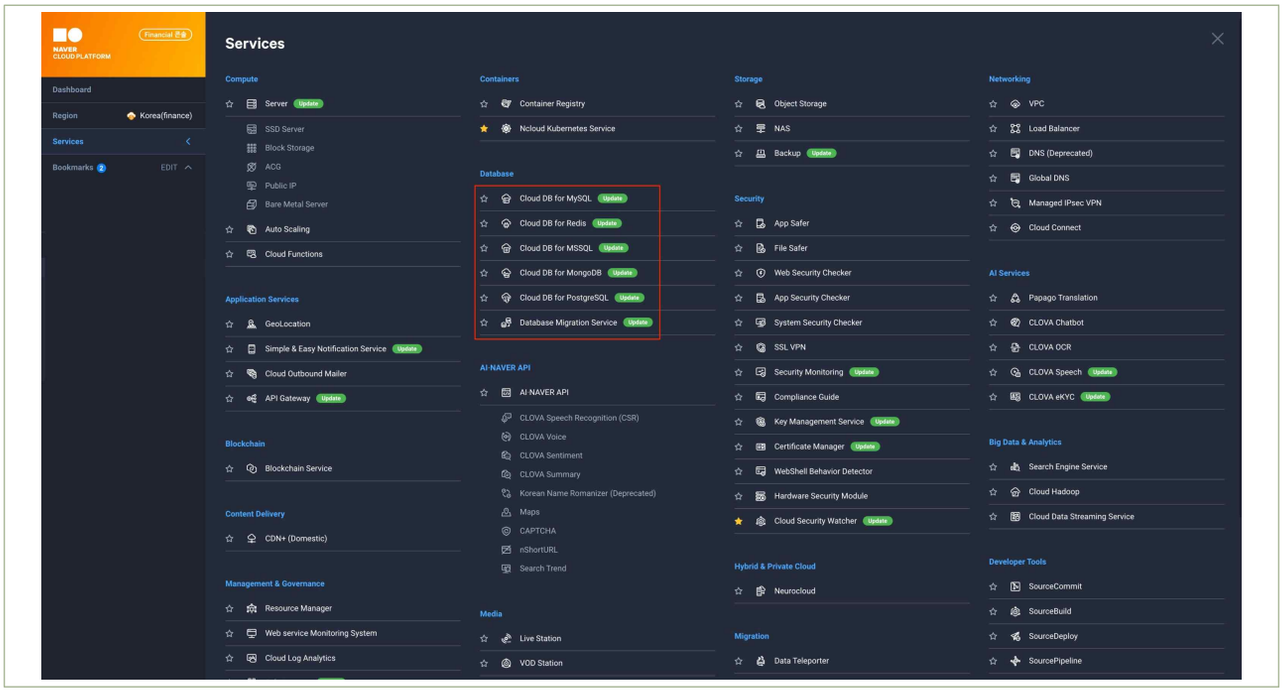
③ **(가상자원관리시스템)** 서버 설정 단계에서 '스토리지 암호화 적용'을 활성화하여 Server에 마운트되는 스토리지에 대해 암호화를 적용합니다.



| 그림 4-1-3 | Server 생성 시 스토리지 암호화 적용 예시

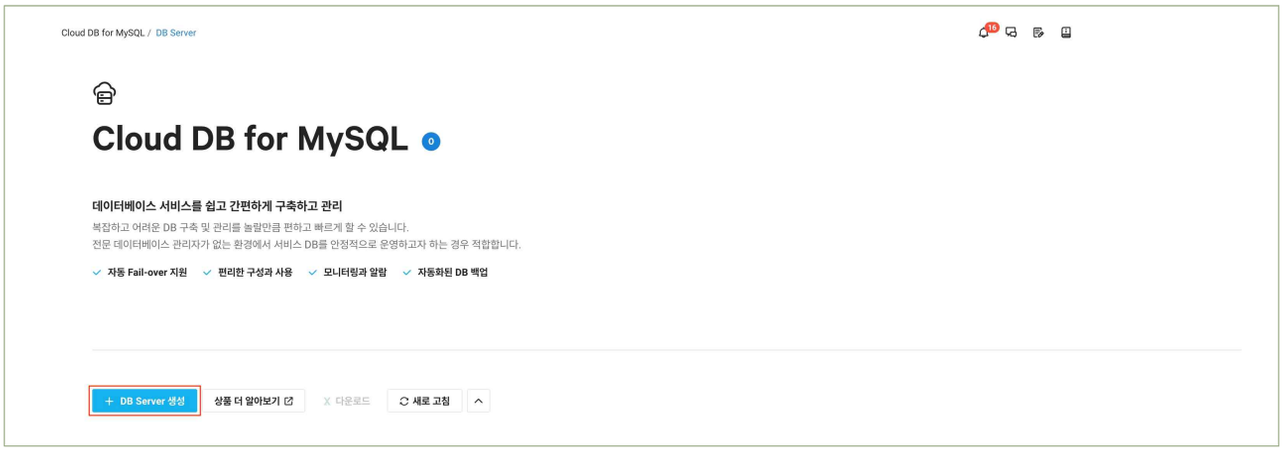
Cloud DB 스토리지 암호화 적용

① **(가상자원관리시스템)** 'Services' → 'Cloud DB' 상품을 선택합니다.



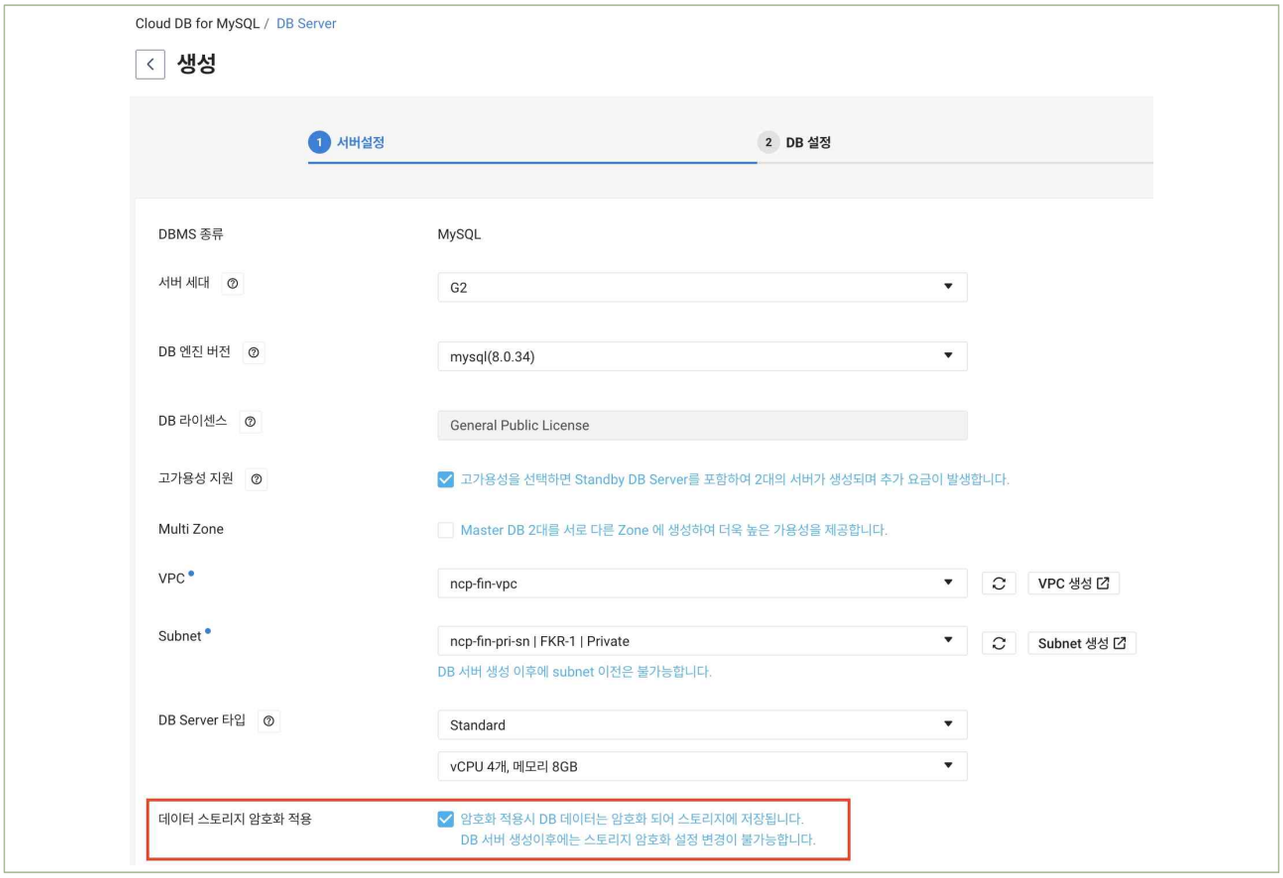
| 그림 4-1-4 | Cloud DB 상품 선택

② **(가상자원관리시스템)** ‘DB Server’ → ‘+DB Server 생성’을 클릭하여 가상자원(Cloud DB)를 생성합니다.



| 그림 4-1-5 | Cloud DB 신규 생성

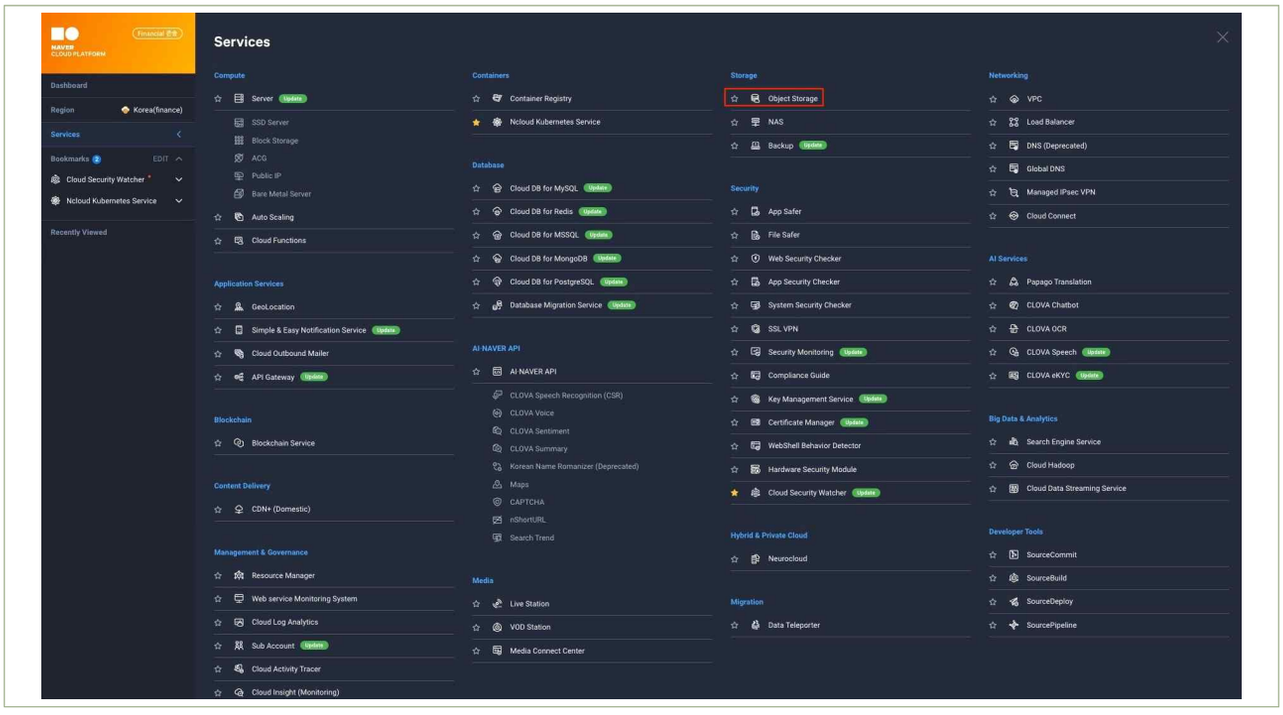
③ **(가상자원관리시스템)** Cloud DB 서버 설정 단계에서 ‘데이터 스토리지 암호화 적용’을 활성화하여 Cloud DB에 마운트되는 스토리지에 대해 암호화를 적용합니다.



| 그림 4-1-6 | Cloud DB 생성 시 스토리지 암호화 적용 예시

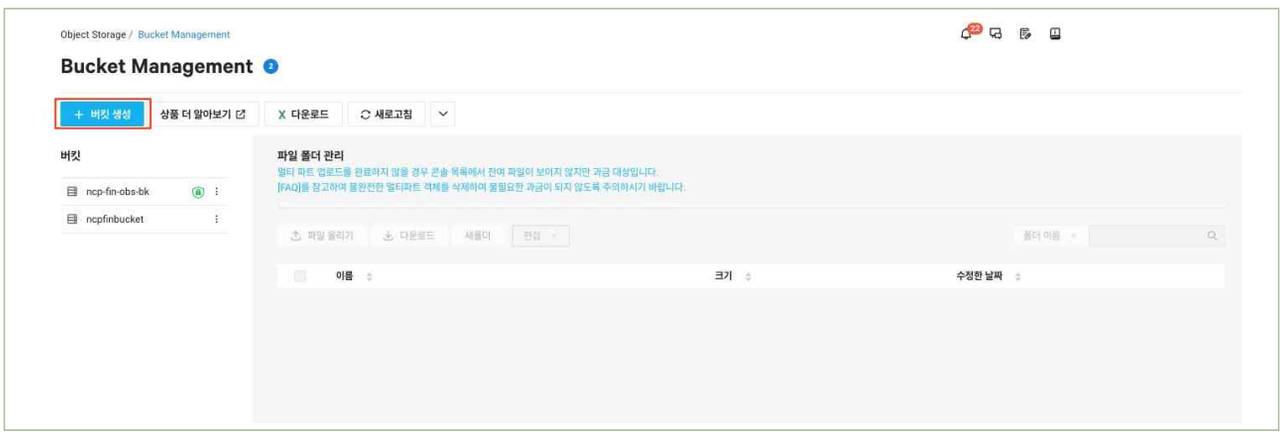
Object Storage 암호화 적용

① **(가상자원관리시스템)** ‘Services’ → ‘Object Storage’ 상품을 선택합니다.



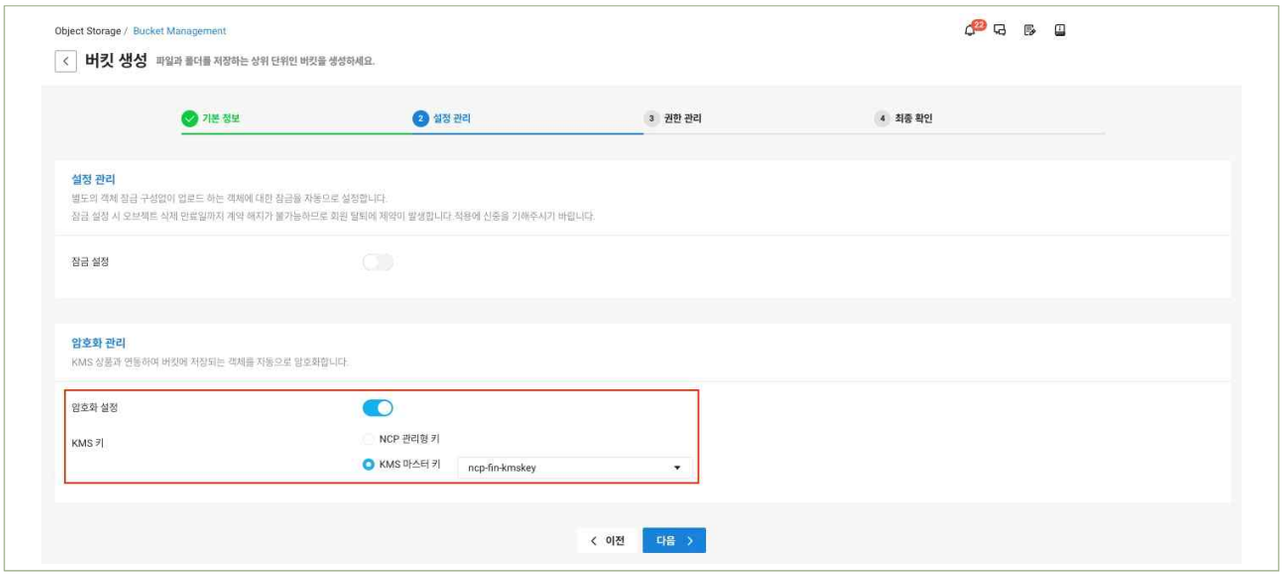
| 그림 4-1-7 | Object Storage 상품 선택

② **(가상자원관리시스템)** ‘Bucket Management’ → ‘+ 버킷 생성’을 클릭합니다.



| 그림 4-1-8 | Object Storage 버킷 생성

- **(가상자원관리시스템)** 버킷 설정 관리 단계에서 '암호화 설정'의 활성화를 통해 NCP 관리형 키 또는 Key Management Service를 통해 사전에 생성한 암호화 키를 사용하여 스토리지 암호화를 적용합니다.



| 그림 4-1-9 | 버킷 생성 시 스토리지 암호화 적용 예시

- **API를 통한 Server 스토리지 암호화 적용**

① **(API(CLI))** 'createServerInstances' API를 통해 Server 생성 시, 'isEncryptedBaseBlock StorageVolume' 파라미터를 통해 블록 스토리지 암호화를 적용합니다.

- 요청 예시

```
GET https://fin-ncloud.apigw.fin-ntruss.com/vserver/v2/createServerInstances
?regionCode=FKR
&serverImageProductCode=SW.VSVR.OS.LNX64.CNTOS.0703.B050
&vpcNo=***04
&subnetNo=***43
&serverProductCode=SVR.VSVR.STAND.C002.M004.NET.SSD.B050.G001
&feeSystemTypeCode=MTRAT
&serverCreateCount=1
&serverName=test-***
&networkInterfaceList.1.networkInterfaceOrder=0
&networkInterfaceList.1.accessControlGroupNoList.1=***63
&placementGroupNo=***61
&isProtectServerTermination=false
&initScriptNo=***44
&loginKeyName=test-***
&associateWithPublicIp=true
& isEncryptedBaseBlockStorageVolume=ture
```

| 그림 4-1-10 | Server 스토리지 암호화 적용

API를 통한 Cloud DB 스토리지 암호화 적용

① **(API(CLI))** 'createCloudMysqlInstance' API를 통해 Cloud DB 생성 시 isStorageEncryption 파라미터를 사용하여 스토리지 암호화를 적용합니다.

- 요청 예시

```
GET {API_URL}/createCloudMysqlInstance
?regionCode=FKR
&vpcNo=****83
&cloudMysqlImageProductCode=SW.VDBAS.DBAAS.LNX64.CNTOS.0708.MYSQL.8025.B050
&cloudMysqlProductCode=SVR.VDBAS.STAND.C002.M008.NET.HDD.B050.G002
&dataStorageTypeCode=SSD
&isHa=true
&isMultiZone=true
&isStorageEncryption=true
&isBackup=true
&backupFileRetentionPeriod=10
&backupTime=02:00
&isAutomaticBackup=false
&cloudMysqlServiceName=test-****
&cloudMysqlServerNamePrefix=test-****
&cloudMysqlUserName=test-****
&cloudMysqlUserPassword=********
&hostIp=192.168.0.%
&cloudMysqlPort=13306
&cloudMysqlDatabaseName=test-****
&subnetNo=****91
&standbyMasterSubnetNo=****93
```

- 응답 예시

```
{
  "createCloudMysqlInstanceResponse": {
    "requestId": "ae758cc2-006c-4df5-8ad2-aeef4ecfa8bf",
    "returnCode": "0",
    "returnMessage": "success",
    "totalRows": 1,
    "cloudMysqlInstanceList": [
      {
        "cloudMysqlInstanceNo": "****890",
        "cloudMysqlServiceName": "test-****",
        "cloudMysqlInstanceStatusName": "creating",

                                ~ 중략 ~

            "isStorageEncryption": true,
            "dataStorageSize": 10737418240,
            "cpuCount": 2,
            "memorySize": 8589934592,
            "createDate": "2021-05-27T18:00:00+0900"
          }
        ]
      }
    ]
  }
}
```

| 그림 4-1-11 | API를 통한 Cloud DB 스토리지 암호화 적용 예시

4 참고 사항

- [참고1] Server 생성 가이드
- [참고2] Cloud DB 생성 가이드
- [참고3] Object Storage 버킷 생성 가이드
- [참고4] Server 생성 API 사용 가이드
- [참고5] Cloud DB 생성 API 사용 가이드

1 기준

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

2 설명

- 암호화 기능 이용 시 암호키 관리 방안을 수립하여야 한다.

  - 예시

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

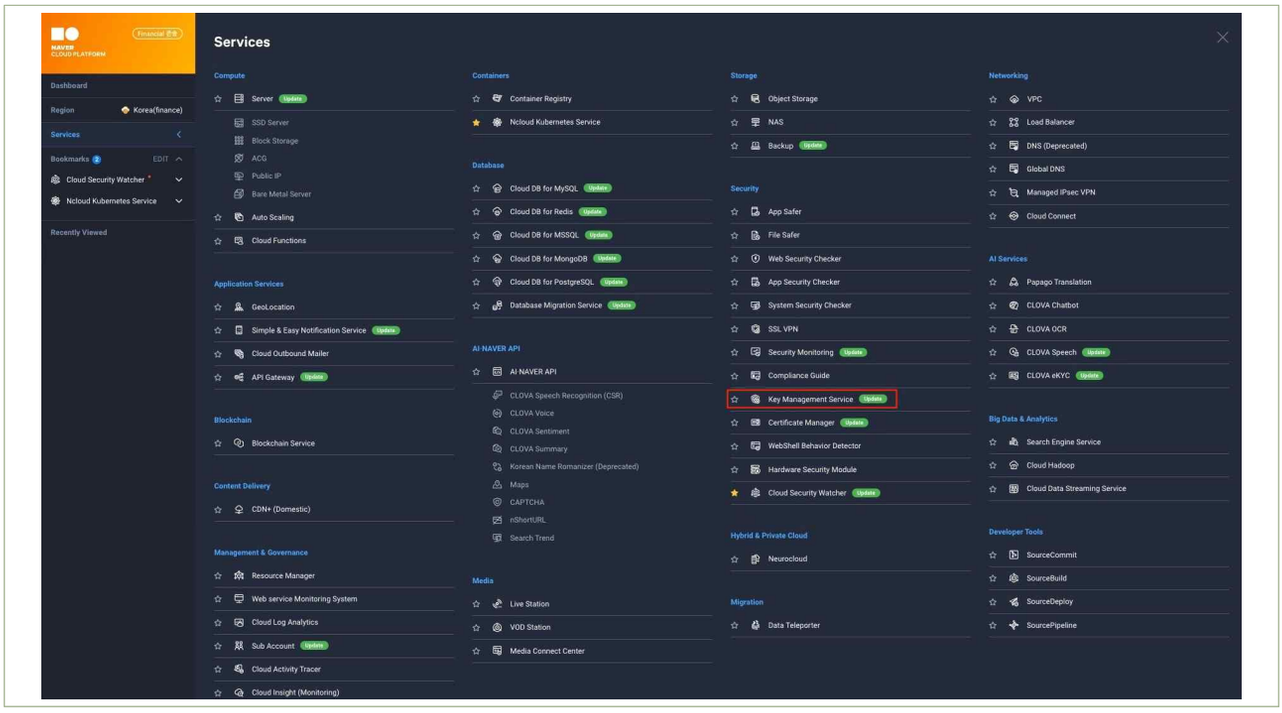
3 우수 사례

- 네이버 클라우드 플랫폼의 Key Management Service는 암호화 키의 유출 등 보안 사고에 사용자가 대응할 수 있도록 암호화 키의 비활성화, 삭제, 자동 암호화 키 갱신 등의 다양한 기능을 제공하고 있습니다. 만약, 사용중인 암호화 키의 유출 등 보안사고가 발생되었을 경우 사용 중인 암호화 키에 대해 즉시 비활성화를 수행하거나 암호화 키를 삭제하여야 합니다. 암호화 키 비활성화의 경우 사용자의 선택에 따라 언제든지 재 활성화가 가능하며, 암호화 키 삭제의 경우 72시간 후 영구 삭제되며 삭제 예약중인 상태에서는 암호화 키 사용이 제한됩니다.

  위와 같은 보안사고를 예방하기 위하여 네이버 클라우드 플랫폼에서는 암호화 키 자동 회전 적용을 권장하고 있습니다. 암호화 키 자동 회전은 기본 90일 자동 회전되며, 1~730일 범위 내에 사용자가 직접 회전 주기를 정의할 수도 있습니다.

암호화 키 비활성화

① **(가상자원관리시스템)** ‘Services’ → ‘Key Management Service’ 상품을 선택합니다.



| 그림 4-2-1 | Key Management Service 상품 선택

② **(가상자원관리시스템)** 비활성화 대상 암호화 키를 선택하고 ‘키 비활성화’를 클릭합니다.

| 그림 4-2-2 | 암호화 키 비활성화

③ **(가상자원관리시스템)** 비 활성화된 암호화 키의 ‘사용중지’ 상태를 확인합니다.

| 그림 4-2-3 | 암호화 키의 비활성화 적용 예시

암호화 키 삭제

① **(가상자원관리시스템)** ‘Services’ → ‘Key Management Service’ 상품을 선택합니다.

| 그림 4-2-4 | Key Management Service 상품 선택

② **(가상자원관리시스템)** 삭제 대상 암호화 키를 선택하고 ‘키 삭제요청’을 클릭합니다.

| 그림 4-2-5 | 암호화 키 삭제

③ **(가상자원관리시스템)** 암호화 키의 '삭제예정' 상태를 확인합니다. 삭제예정 상태의 암호화 키는 72시간 후 영구적으로 삭제됩니다.

| 그림 4-2-6 | 암호화 키의 삭제 예시

암호화 키 자동 회전 적용

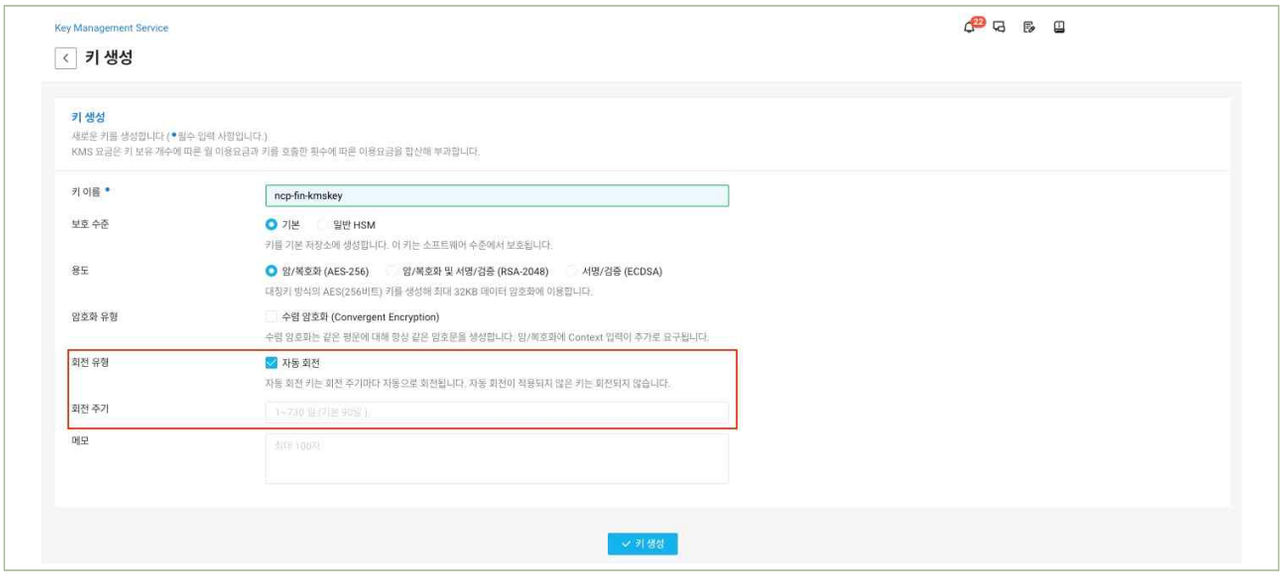
① **(가상자원관리시스템)** 'Services' → 'Key Management Service' 상품을 선택합니다.

| 그림 4-2-7 | Key Management Service 상품 선택

② **(가상자원관리시스템)** 새로운 암호화 키 생성을 위해 '+ 키 생성'을 클릭합니다.

| 그림 4-2-8 | 암호화 키 생성

③ **(가상자원관리시스템)** 키 생성 단계에서 암호화 키 자동 회전을 활성화하여 정의한 회전 주기에 따라 암호화 키의 갱신을 자동화 합니다.



| 그림 4-2-9 | 암호화 키 자동 회전 적용 예시

API를 통한 암호화 키 생성

① **(API(CLI))** 'createCustomKey' API를 통해 Key Management Service 암호화 키를 생성합니다.

- 요청 예시

```
POST https://kms.apigw.fin-ntruss.com/keys/v2/{keyTag}/createCustomKey
```

- 요청 예시 (Body)

```
{
  "requestPlainKey" : ture,
  "bits" : 256
}
```

| 그림 4-2-10 | API를 통한 암호화 키 생성 예시

4 참고 사항

- [참고1] Key Management Service 사용 가이드
- [참고2] Key Management Service API 사용 가이드
- [참고3] 암호화 키 생성 API 사용 가이드

1 기준

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

2 설명

- 클라우드 환경 내 암호키 관리 서비스(ex. KMS) 이용 시 암호키 서비스 관리자 권한을 적절하게 통제하여야 한다.

  - 예시

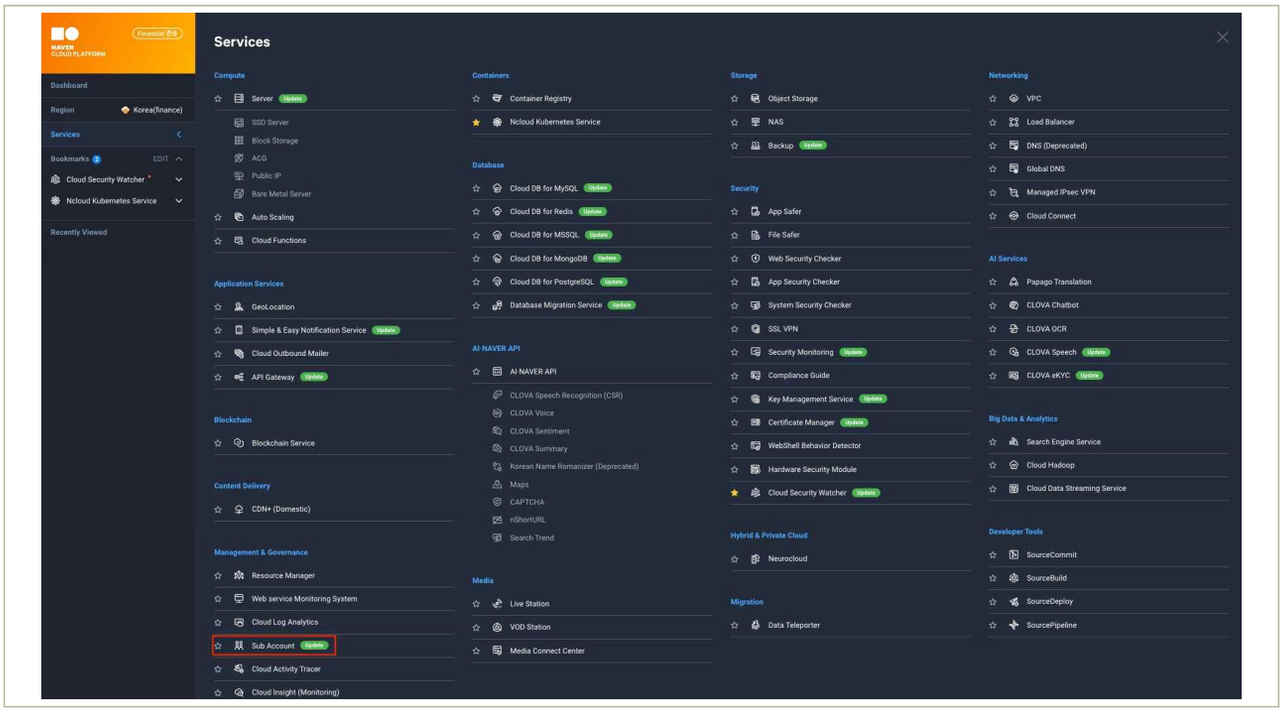
    1) 암호키 관리 서비스 관리자 권한은 최소인원에게 부여하고 부여현황에 대해 상시모니터링 수행
    2) 사용자가 생성하는 각 키에 대해서는 관리자를 별도 지정할 수 있어야 하며, 각 조건에 따라 최소한의 권한 부여 등

3 우수 사례

- 네이버 클라우드 플랫폼의 Key Management Service는 계정 관리 상품인 Sub Account를 사용하여 암호화 키 접근 권한을 다양하게 설정할 수 있습니다. Sub Account는 관리 및 운영 권한 설정을 위해 관리형(System Managed) 정책과 사용자 정의(User Created) 정책을 제공하며, 관리자 권한을 최소한의 서브 계정에게 부여하고자 하는 경우, 사용자 정의 정책을 통해 특정 암호화 키의 관리자 권한을 특정 서브 계정에게만 부여할 수 있습니다.
  이처럼, 특정 서브 계정에게 부여된 관리자 권한은 Key Management Service의 '키 이력 보기'를 통해 암호화 키 호출 이력을 모니터링 할 수 있습니다.

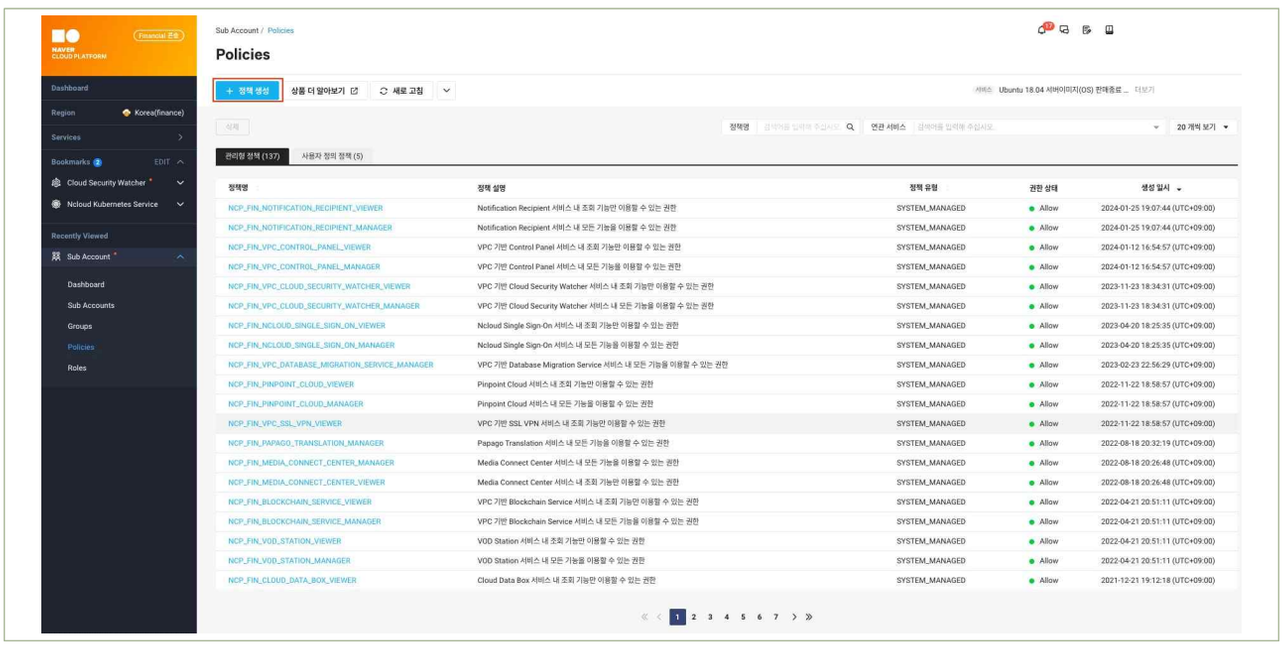
암호화 키 별 관리자 지정

① **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ 상품을 선택합니다.



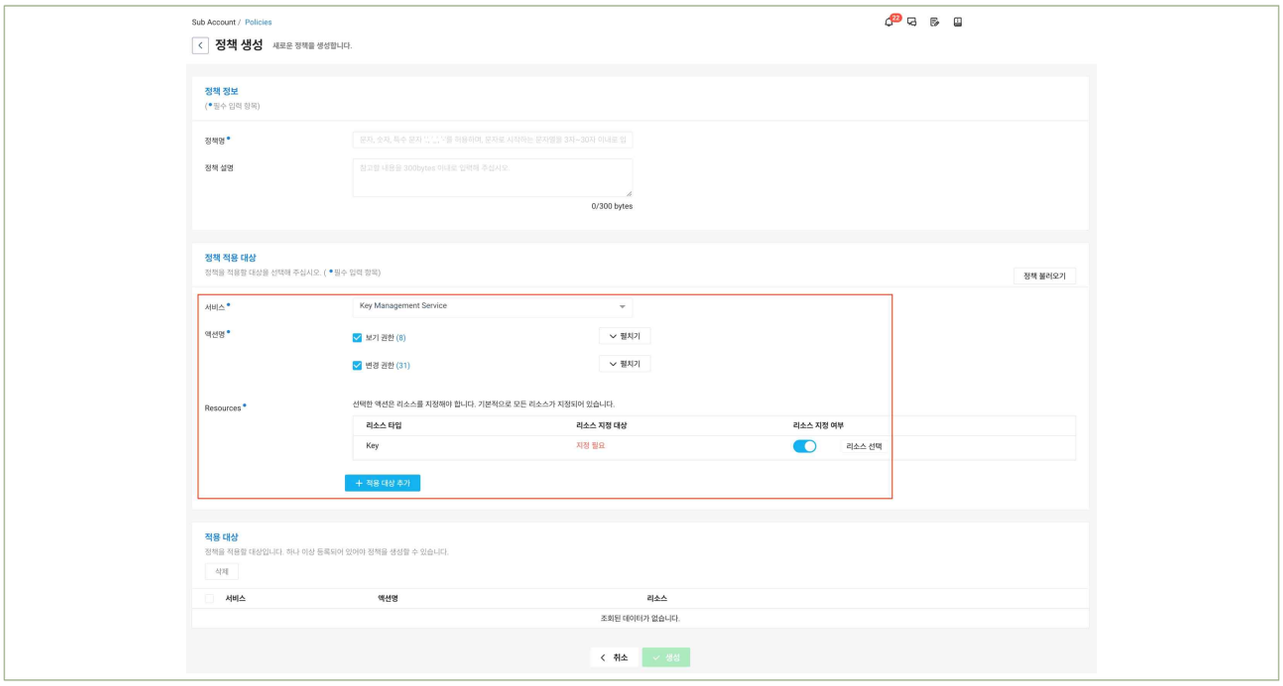
| 그림 4-3-1 | Sub Account 상품 선택

② **(가상자원관리시스템)** 사용자 정의 정책 생성을 위해 ‘Policies’ → ‘+ 정책 생성’버튼을 클릭합니다.



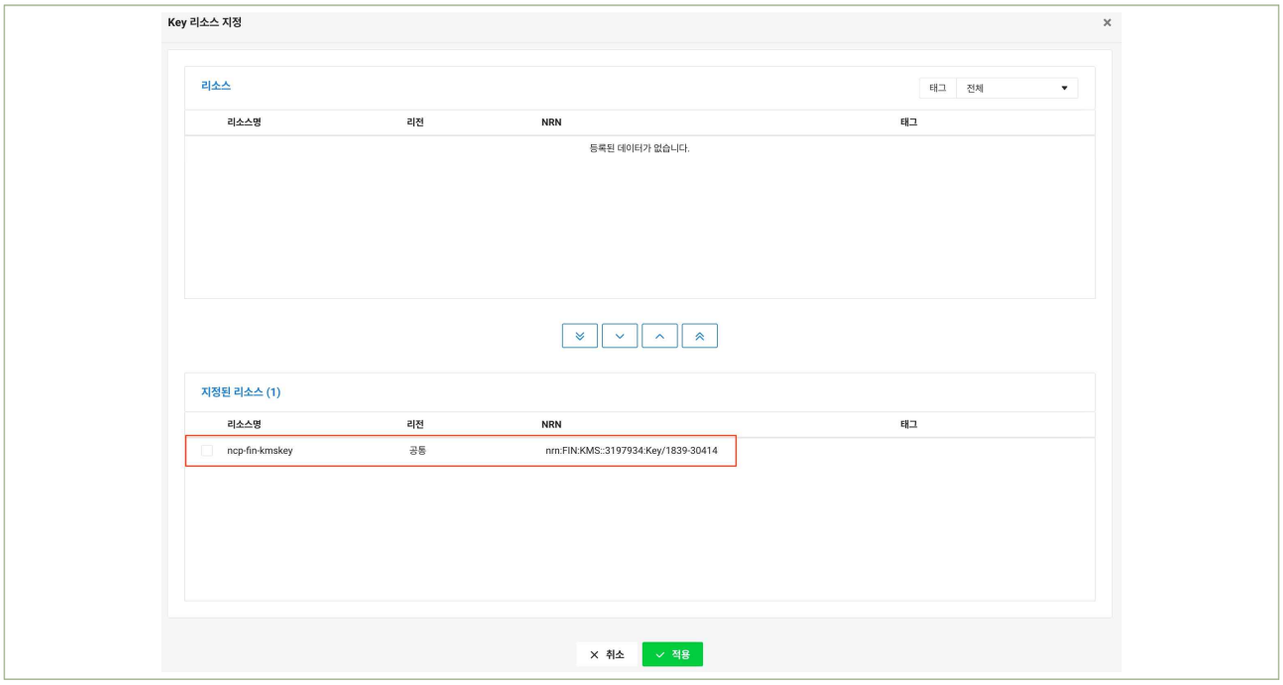
| 그림 4-3-2 | 사용자 정의 정책 생성

③ **(가상자원관리시스템)** 정책 적용 대상 서비스에 Key Management Service를 선택하고, 관리자 권한 범위에 해당하는 액션을 선택합니다. 다음, 리소스 지정 여부 토글을 활성화하고 '리소스 선택' 버튼을 클릭합니다.



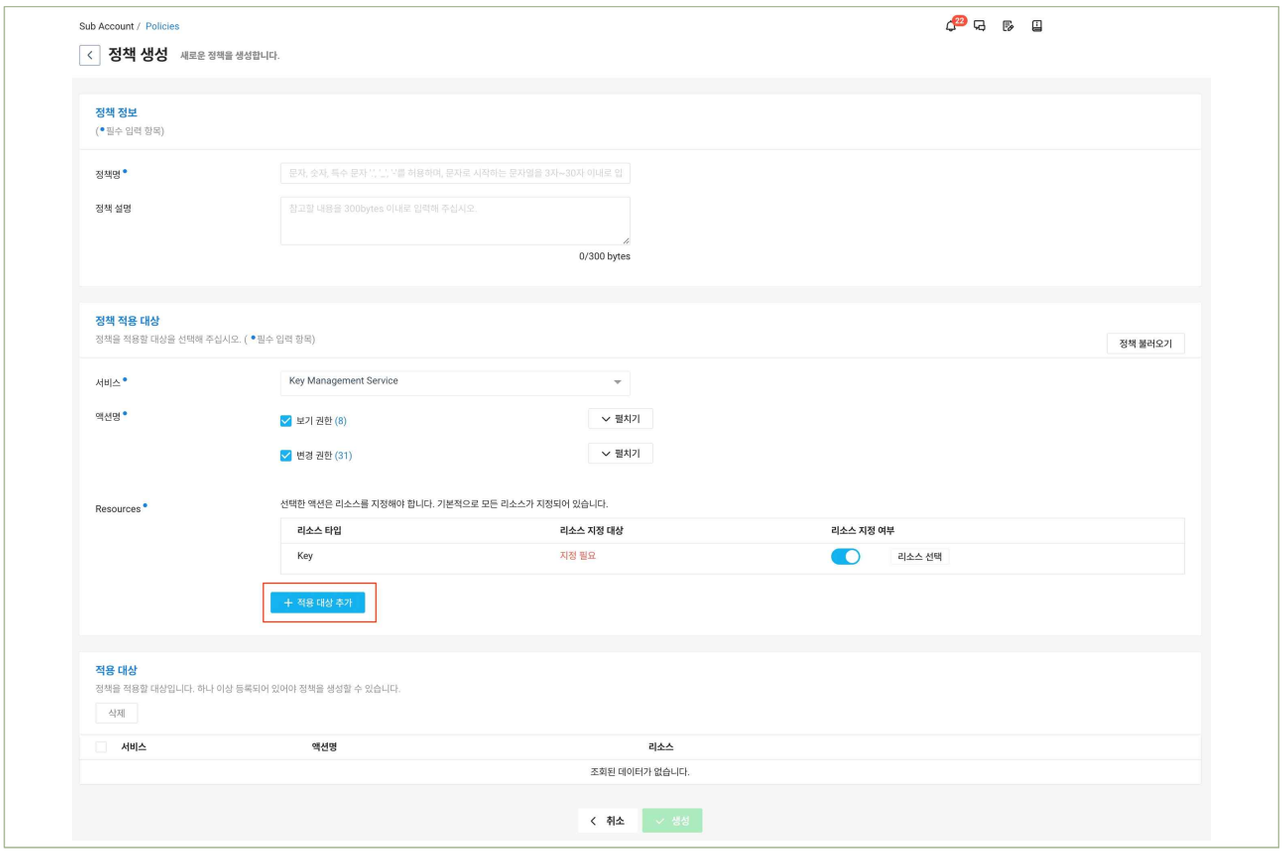
| 그림 4-3-3 | 암호화 키 관리자 권한 범위 설정 예시

④ **(가상자원관리시스템)** 특정 암호화 키에 대한 관리자 권한 부여를 위해 암호화 키 리소스 목록에서 특정 암호화 키만 지정합니다.



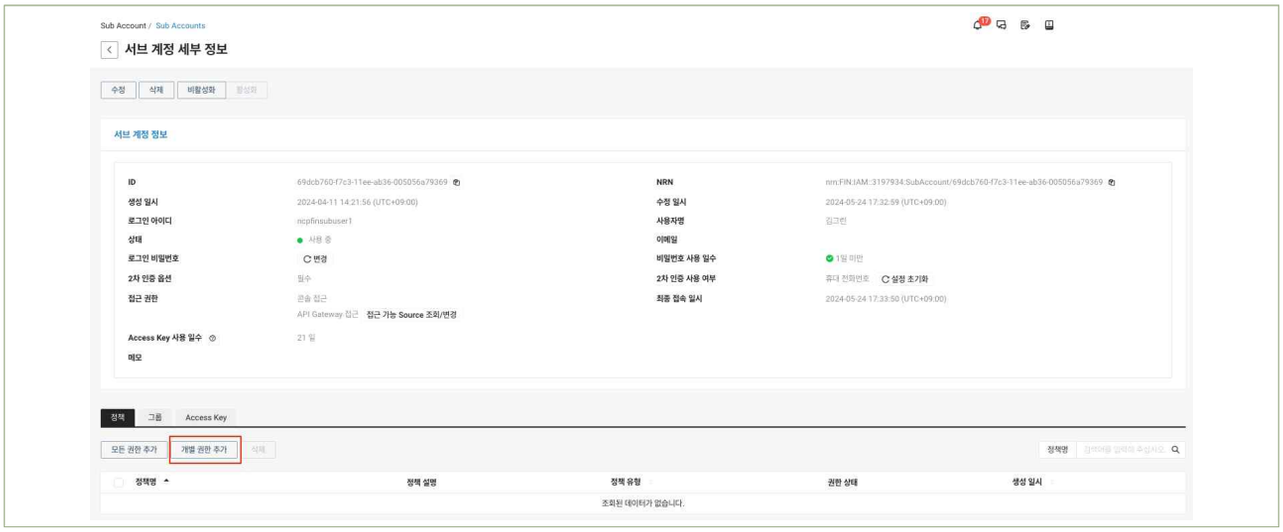
| 그림 4-3-4 | 특정 암호화 키 대상 지정 예시

⑤ **(가상자원관리시스템)** '+적용 대상 추가' 버튼을 클릭한 후 사용자 정의 정책을 생성합니다.



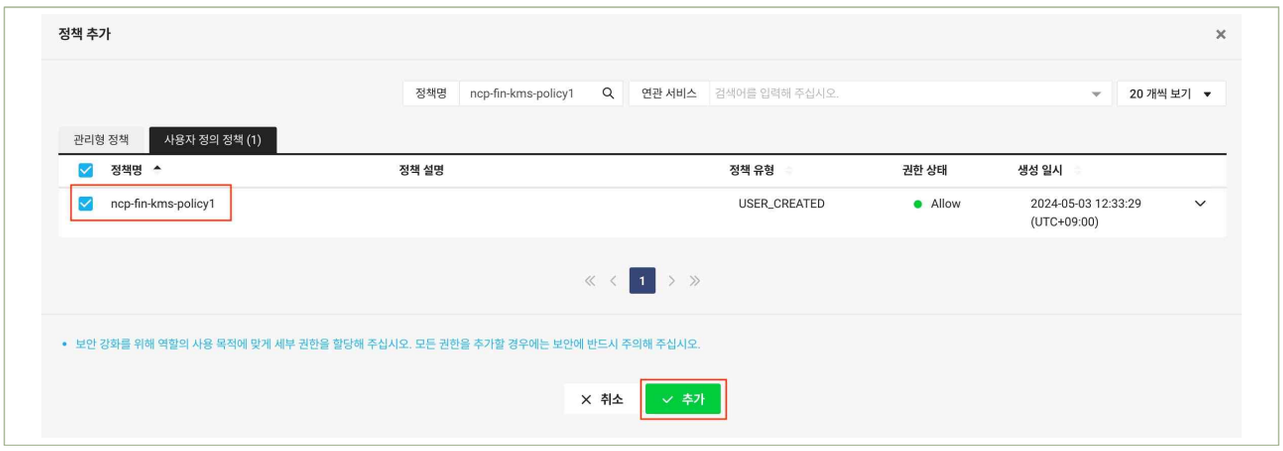
| 그림 4-3-5 | 특정 암호화 키 대상 지정 예시

⑥ **(가상자원관리시스템)** 'Services' → 'Sub Account' → 'Sub Accounts'에서 사용자 정의 정책을 부여할 서브 계정을 선택하고, '개별 권한 추가'를 클릭합니다.



| 그림 4-3-6 | 서브 계정 별 개별 권한 추가

⑦ **(가상자원관리시스템)** 앞서 정의한 사용자 정의 정책을 서브계정에 추가합니다.

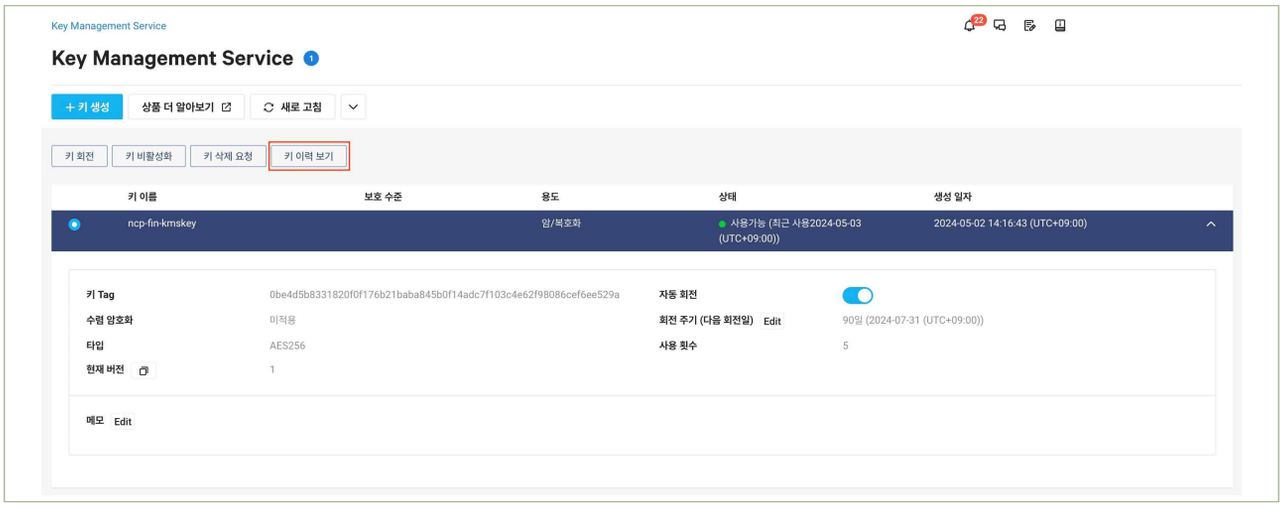


| 그림 4-3-7 | 서브 계정 별 개별 권한 추가

⑧ **(가상자원관리시스템)** 'Services' → 'Key Management Service' 상품을 선택합니다.

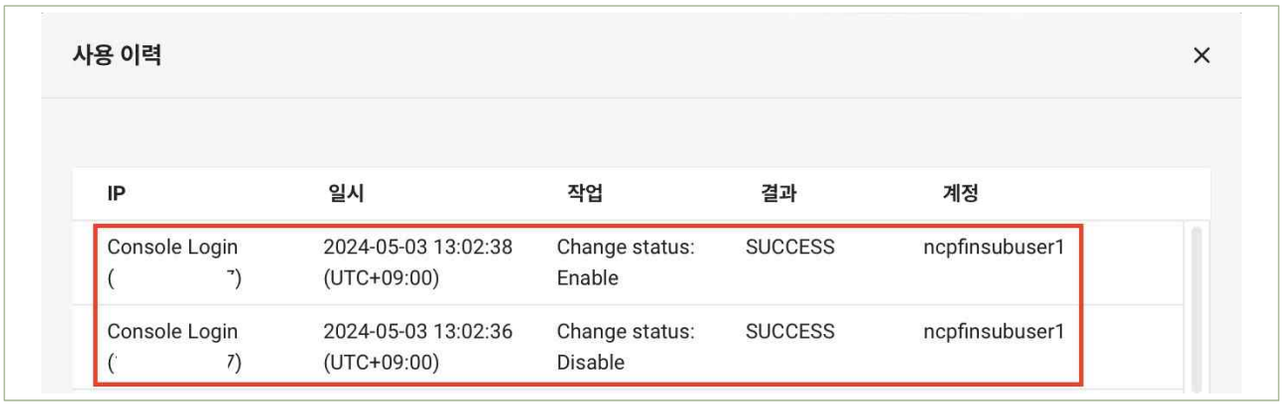
| 그림 4-3-8 | Key Management Service 상품 선택

⑨ **(가상자원관리시스템)** ‘키 이력 보기’ 버튼을 클릭합니다.



| 그림 4-3-9 | 암호화 키 이력 보기 예시

⑩ **(가상자원관리시스템)** 특정 암호화 키의 사용 이력을 모니터링합니다.



| 그림 4-3-10 | 암호화 키 사용 이력 모니터링 예시

API를 통한 사용자 정의 정책 생성 및 연결

① **(API(CLI))** 'polices' API를 통해 암호화 키 관리자 권한에 대한 사용자 정의 정책을 생성합니다.

- 요청 예시

```
POST https://subaccount.apigw.fin-ntruss.com/api/v1/policies
```

- 요청 예시 (Body)

```
{
  "policyName": "string",
  "description": "string",
  "permissions": [
    {
      "effect": "string",
      "targets": [
        {
          "product": "string",
          "actions": [
            "string"
          ],
          "resourceNrns": [
            "string"
          ]
        }
      ]
    }
  ]
}
```

- 응답 예시 (성공)

```
{
  "policyId": "string",
  "policyName": "string",
  "description": "string",
  "validationResult": {
    "details": [
      {
        "code": "string",
        "location": "string",
        "message": "string",
        "type": "ERROR"
      }
    ],
    "success": true
  }
}
```

| 그림 4-3-11 | API를 통한 사용자 정의 정책 생성 예시

② **(API(CLI))** ‘polices’ API를 통해 서브 계정 별 암호화 키에 대한 관리자 권한 사용자 정의 정책을 할당합니다.

- 요청 예시

```
POST https://subaccount.apigw.fin-ntruss.com/api/v1/sub-accounts/{subAccountId}/policies
```

- 요청 예시 (Body)

```
{
  "policyIdList": [
    "string"
  ]
}
```

- 응답 예시

```
[
  {
      "id": "policyId1",
      "success": true
  }
]
```

| 그림 4-3-12 | API를 통한 서브 계정 별 사용자 정의 정책 할당 예시

4 참고 사항

- [참고1] Key Management Service 권한 관리 가이드
- [참고2] 사용자 정의 정책 생성 가이드
- [참고3] 사용자 정의 정책 생성 API 사용 가이드
- [참고4] 서브계정에 정책 할당 API 사용 가이드

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

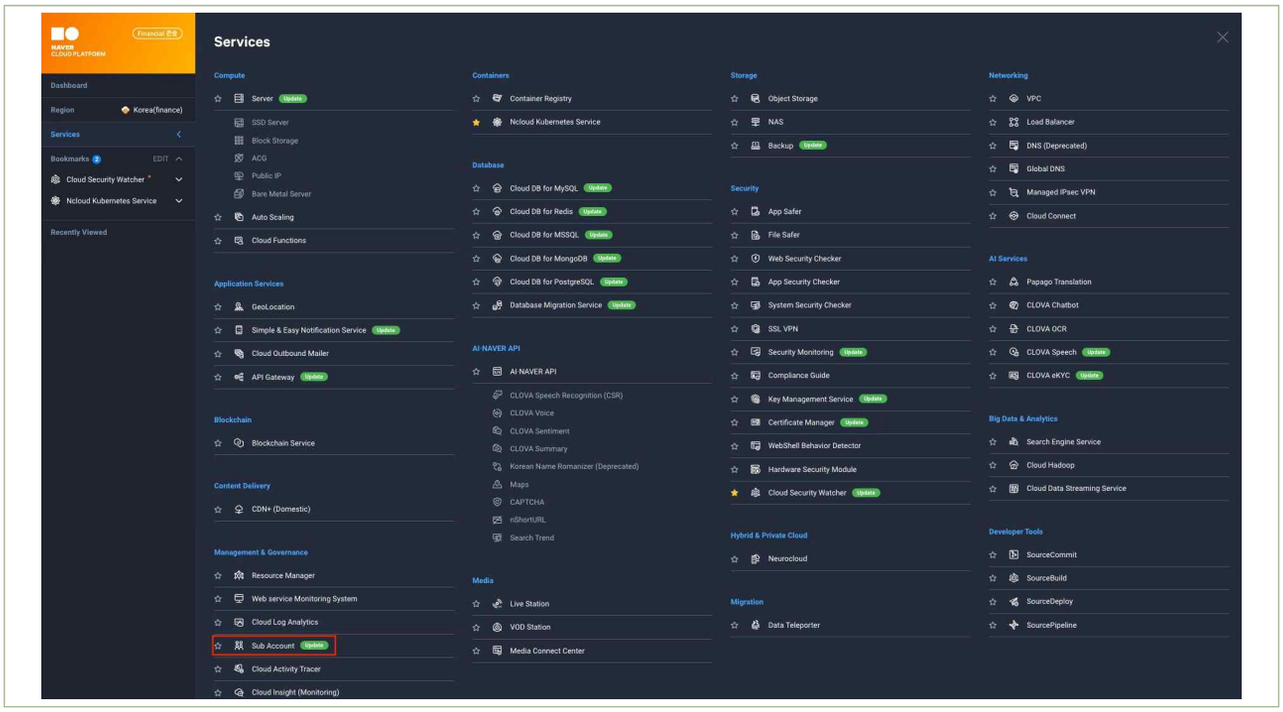
    2) 암호키 호출 권한 현황에 대한 모니터링 및 주기적 검토 수행

3 우수 사례

- 네이버 클라우드 플랫폼의 계정 관리 상품인 Sub Account를 사용하여 Key Management Service의 암호화 키에 대한 접근권한을 다양하게 설정할 수 있습니다. 사용자는 Sub Account의 사용자 정의(User Created) 정책을 통해 서브 계정 별 암호화 키 호출 목적에 따라 상세 권한을 부여할 수 있습니다. 또한, 서브 계정에게 부여된 암호화 키의 권한은 Key Management Service의 '키 이력 보기'를 통해 암호화, 복호화 등의 암호화 키 호출 이력을 모니터링 할 수 있습니다.

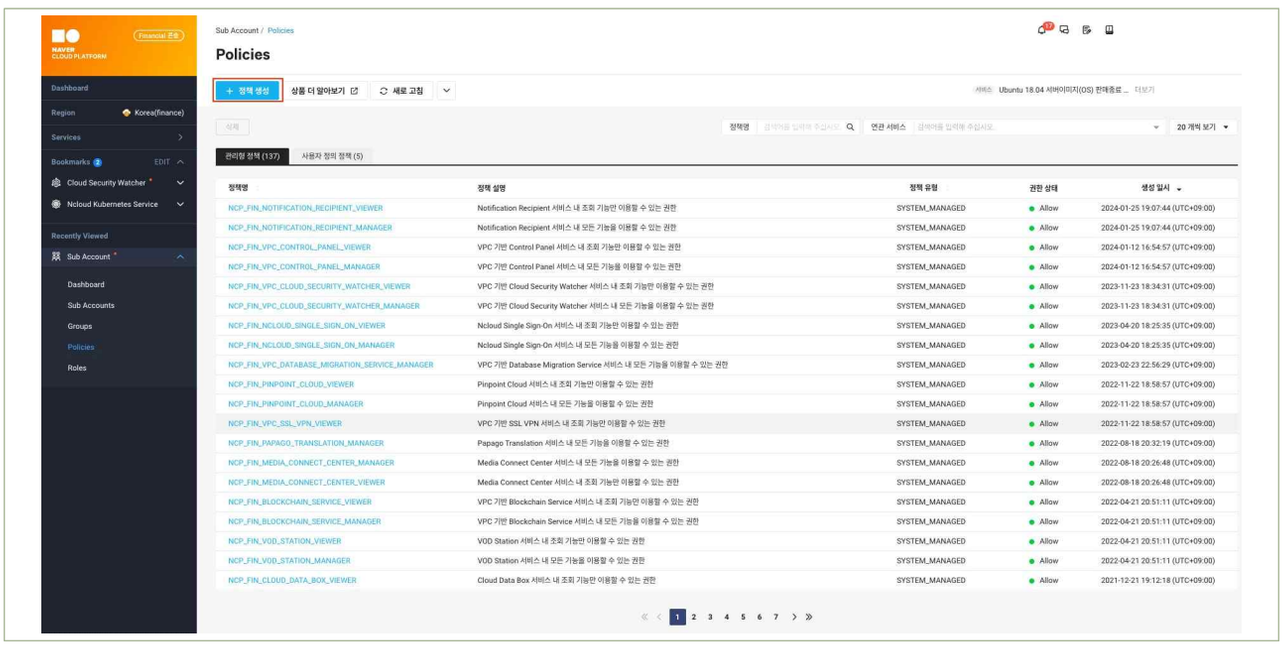
서브계정 별 암호화 키 상세 권한 지정

① **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ 상품을 선택합니다.



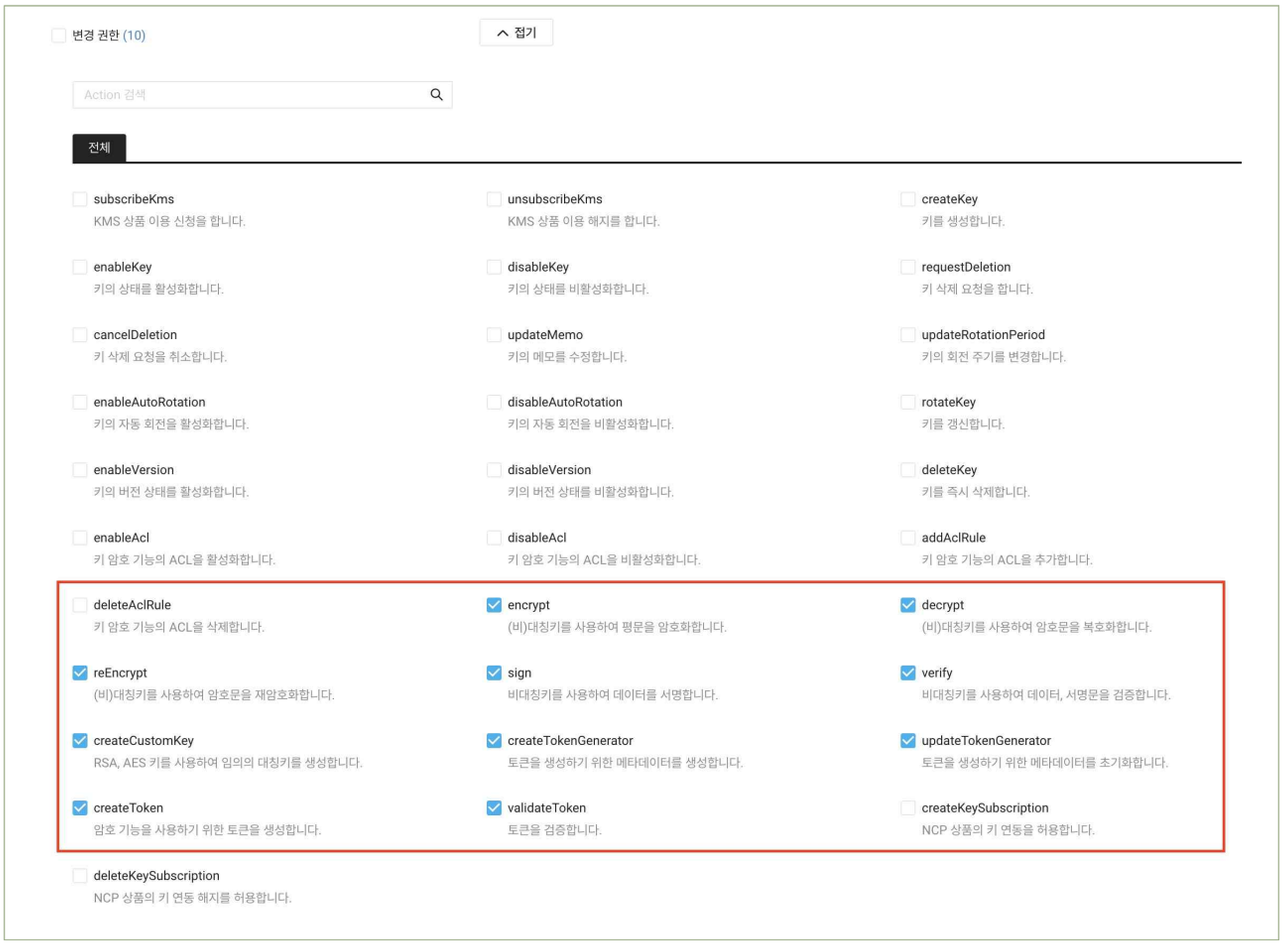
| 그림 4-4-1 | Sub Account 상품 선택

② **(가상자원관리시스템)** 사용자 정의 정책 생성을 위해 ‘Policies’ → ‘+ 정책 생성’버튼을 클릭합니다.



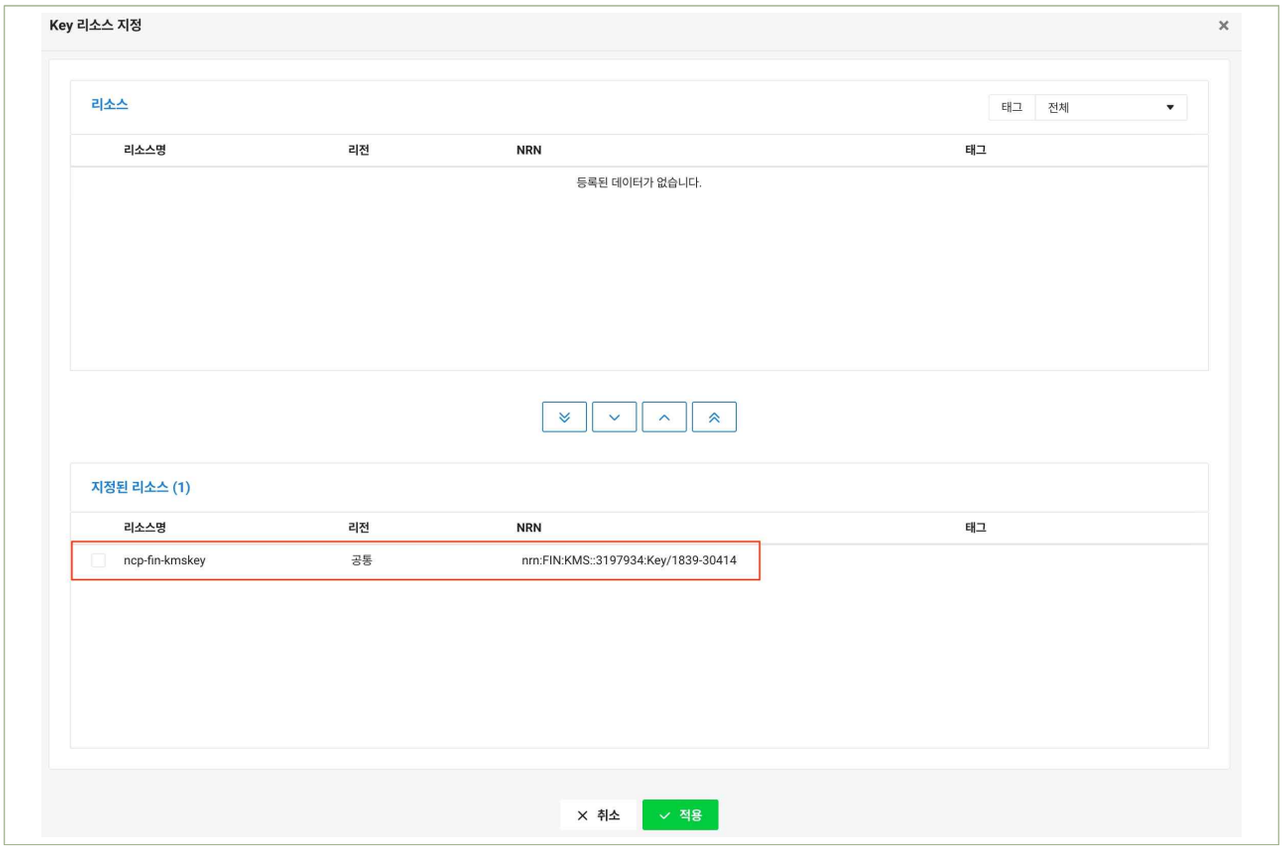
| 그림 4-4-2 | 사용자 정의 정책 생성

③ **(가상자원관리시스템)** 정책 적용 대상 서비스에 Key Management Service를 선택하고, 사용자 업무에 따라 권한 범위에 해당하는 액션을 선택합니다.



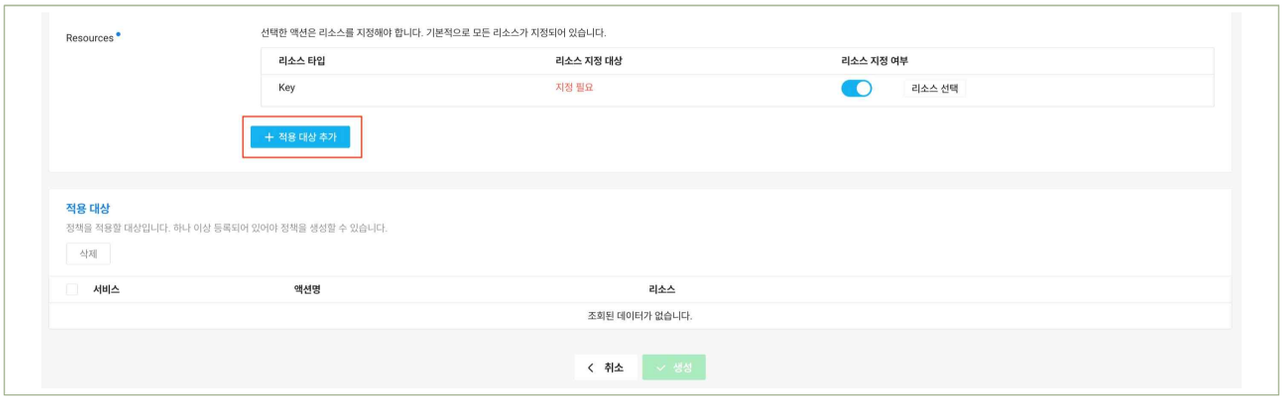
| 그림 4-4-3 | 암호화 키 상세 권한 사용자 정의 정책 생성 예시

④ **(가상자원관리시스템)** 특정 암호화 키에 대한 관리자 권한 부여를 위해 암호화 키 리소스 목록에서 특정 암호화 키만 지정합니다.



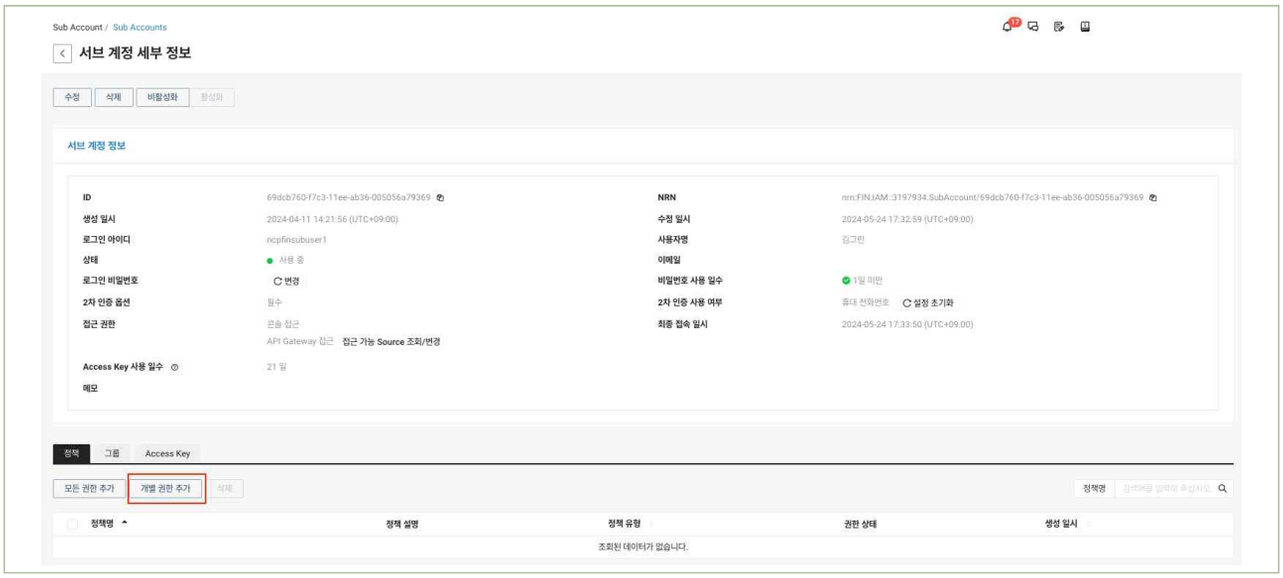
| 그림 4-4-4 | 특정 암호화 키 대상 지정 예시

⑤ **(가상자원관리시스템)** '+적용 대상 추가' 버튼을 클릭한 후 사용자 정의 정책을 생성합니다.



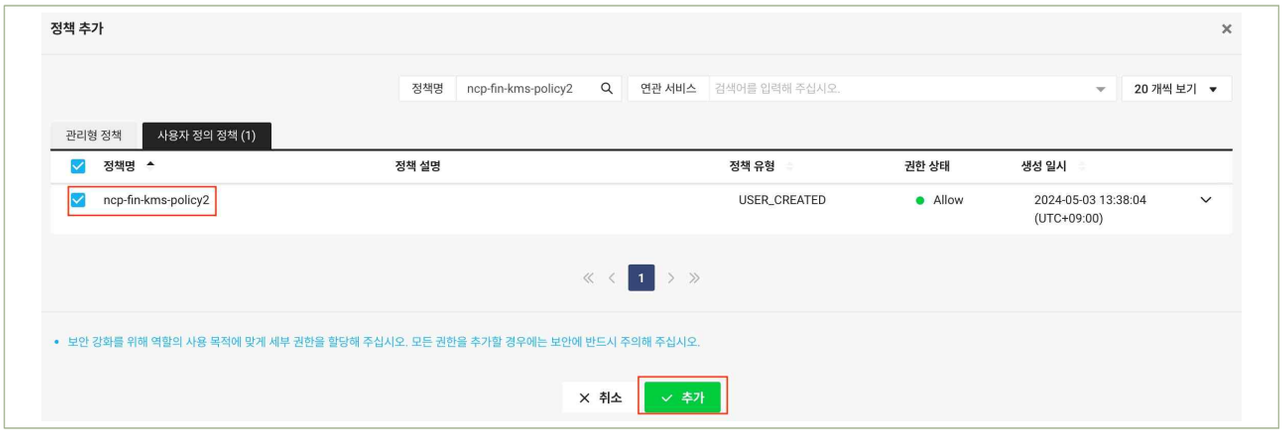
| 그림 4-4-5 | 특정 암호화 키 대상 지정 예시

⑥ **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ → ‘Sub Accounts’에서 사용자 정의 정책을 부여할 서브 계정을 선택하고, ‘개별 권한 추가’를 클릭합니다.



| 그림 4-4-6 | 서브 계정 별 개별 권한 추가

⑦ **(가상자원관리시스템)** 앞서 정의한 사용자 정의 정책을 서브계정에 추가합니다.



| 그림 4-4-7 | 서브 계정 별 개별 권한 추가

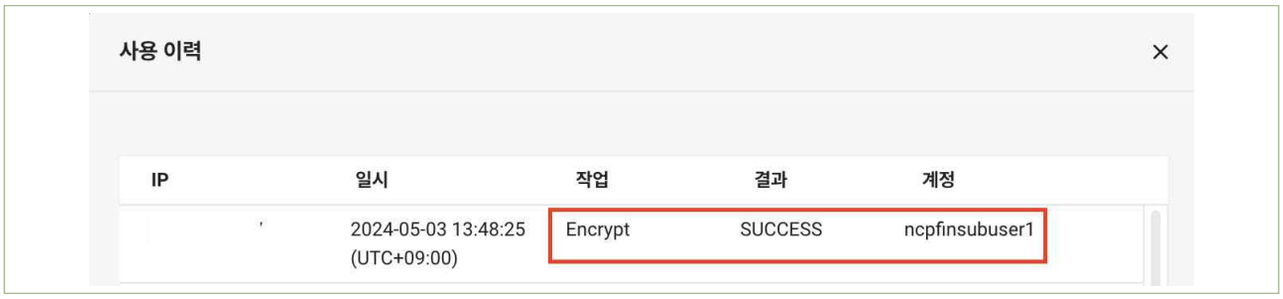
⑧ **(가상자원관리시스템)** ‘Services’ → ‘Key Management Service’ 상품을 선택합니다.

| 그림 4-4-8 | Key Management Service 상품 선택

⑨ **(가상자원관리시스템)** ‘키 이력 보기’ 버튼을 클릭합니다.

| 그림 4-4-9 | 암호화 키 이력 보기 예시

⑩ **(가상자원관리시스템)** 특정 암호화 키의 사용 이력을 모니터링합니다.



| 그림 4-4-10 | 암호화 키 사용 이력 모니터링 예시

API를 통한 사용자 정의 정책 생성 및 연결

① **(API(CLI))** 'polices' API를 통해 암호화 키 상세 권한에 대한 사용자 정의 정책을 생성합니다.

- 요청 예시

```
POST https://subaccount.apigw.fin-ntruss.com/api/v1/policies
```

- 요청 예시 (Body)

```
{
  "policyName": "string",
  "description": "string",
  "permissions": [
    {
      "effect": "string",
      "targets": [
        {
          "product": "string",
          "actions": [
            "string"
          ],
          "resourceNrns": [
            "string"
          ]
        }
      ]
    }
  ]
}
```

- 응답 예시 (성공)

```
{
  "policyId": "string",
  "policyName": "string",
  "description": "string",
  "validationResult": {
```

```
    "details": [
      {
        "code": "string",
        "location": "string",
        "message": "string",
        "type": "ERROR"
      }
    ],
    "success": true
  }
}
```

| 그림 4-4-11 | API를 통한 사용자 정의 정책 생성 예시

② **(API(CLI))** 'polices' API를 통해 서브 계정 별 암호화 키에 대한 상세 권한 사용자 정의 정책을 할당합니다.

- 요청 예시

```
POST https://subaccount.apigw.fin-ntruss.com/api/v1/sub-accounts/{subAccountId}/policies
```

- 요청 예시 (Body)

```
{
  "policyIdList": [
    "string"
  ]
}
```

- 응답 예시

```
[
  {
      "id": "policyId1",
      "success": true
  }
]
```

| 그림 4-4-12 | API를 통한 서브 계정 별 사용자 정의 정책 할당 예시

4 참고 사항

- [참고1] Key Management Service 권한 관리 가이드
- [참고2] 사용자 정의 정책 생성 가이드
- [참고3] 사용자 정의 정책 생성 API 사용 가이드
- [참고4] 서브계정에 정책 할당 API 사용 가이드

1 기준

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

2 설명

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

3 우수 사례

- 네이버 클라우드 플랫폼의 Key Management Service는 사용자가 '금융부문 암호기술 활용 가이드' 등 국내외 전문기관(NIST, KISA 등)에서 발표한 암호화 알고리즘을 적정 준수할 수 있도록 지원하고 있습니다. Key Management Service 상품에서 제공하는 암호화 키 종류별 암호화 알고리즘은 다음과 같습니다.
  - 암/복호화 키 : AES-256
  - 암/복호화 및 서명/검증 키 : RSA-2048
  - 서명/검증 키 : ECDSA

암호화 키 종류 별 알고리즘 확인

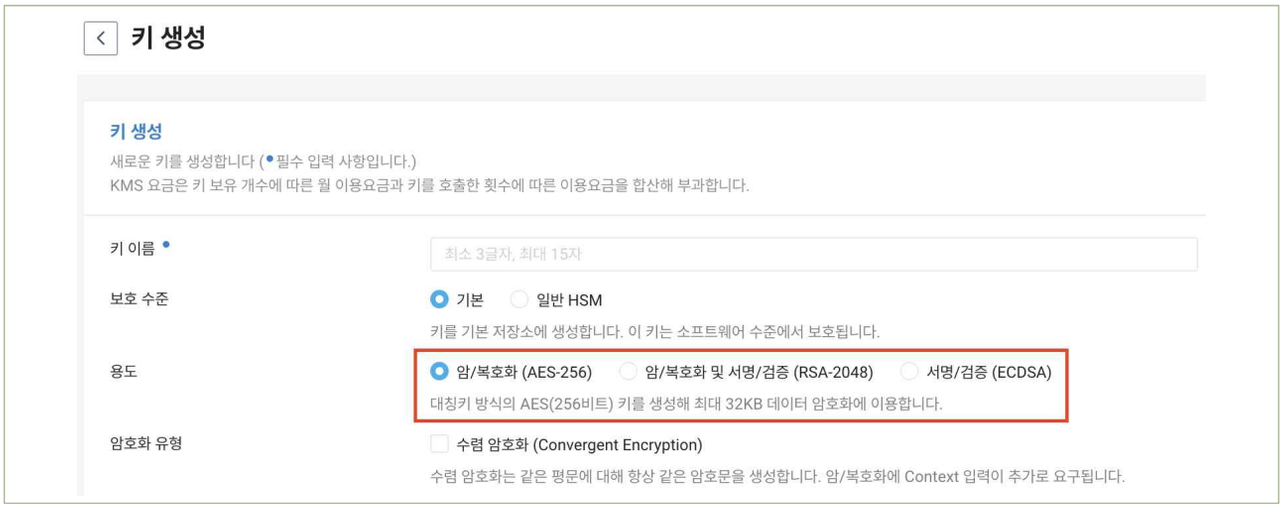
① **(가상자원관리시스템)** ‘Services’ → ‘Key Management Service’ 상품을 선택합니다.

| 그림 4-5-1 | Key Management Service 상품 선택

② **(가상자원관리시스템)** 암호화 키 생성을 위해 ‘+ 키 생성’ 버튼을 클릭합니다.

| 그림 4-5-2 | 암호화 키 신규 생성

③ **(가상자원관리시스템)** 암호화 키 용도에 따라 안전한 암호화 알고리즘이 적용된 암호화 키를 선택합니다.



| 그림 4-5-3 | 암호화 키의 암호화 알고리즘 예시

4 참고 사항

- [참고1] 암호화 키 생성 가이드

5. 로깅 및 모니터링 관리

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

5 로깅 및 모니터링 관리

1 기준

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

2 설명

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

  - 예시

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

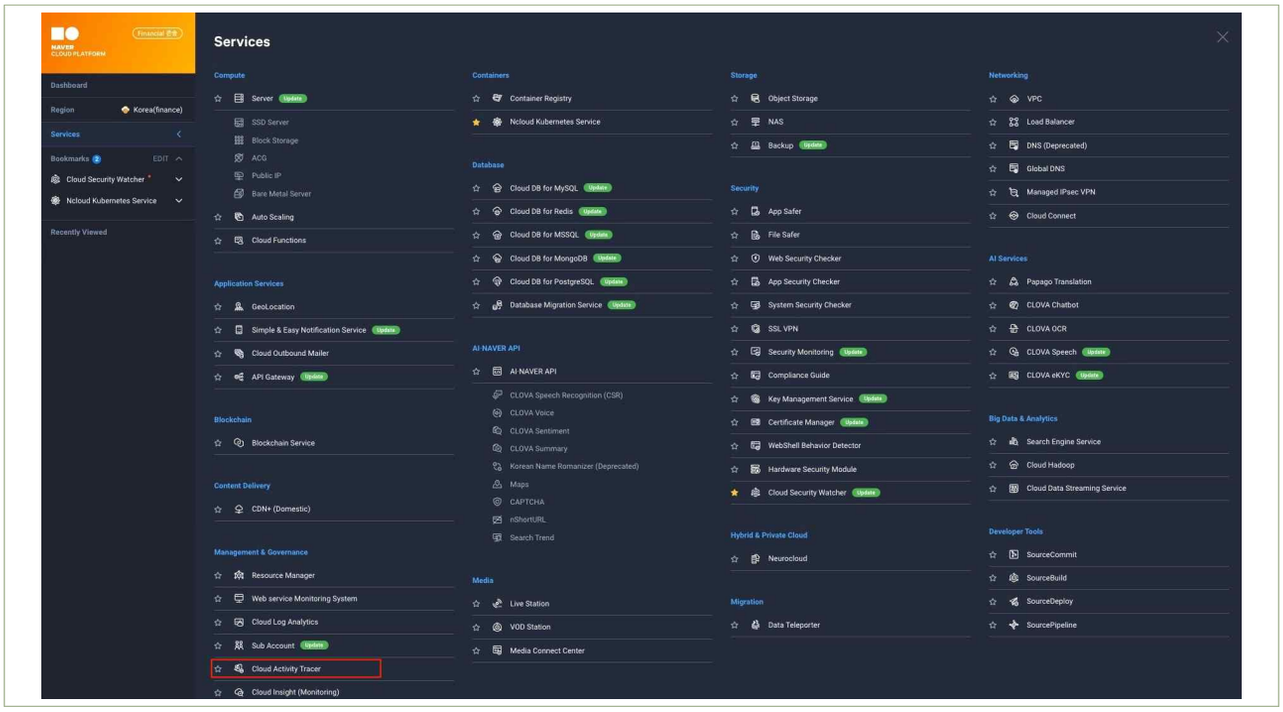
3 우수 사례

- 네이버 클라우드 플랫폼은 메인 계정과 서브 계정의 활동 로그를 수집하고 조회하는 Cloud Activity Tracer 상품을 통해 가상자원관리시스템(클라우드 콘솔) 및 API 사용에 대한 접근 시간, 접근ID, 작업 내용 등을 상세히 기록하여 1년간 보존합니다. 사용자는 이를 통해 언제든지 가상자원관리시스템(클라우드 콘솔)에서 메인 계정과 서브 계정의 활동 기록을 간편하게 열람할 수 있으며, 전자금융감독규정 제13조(전산자료 보호대책) 등에 따라 계정 활동의 장기보존을 위해 Object Storage 상품을 연동하여 안전하게 보관할 수 있습니다.

- 또한, 리소스 현황 식별, 자산 변경 감시 등 클라우드 보안 형상 관리를 수행하는 Cloud Security Watcher 보안 상품을 통해 보다 더 세밀한 계정 활동, 리소스 변경 현황 등을 모니터링할 수 있으며, 이 외에도 가상자원(서버)의 이상행위 탐지를 통해 위협을 식별하거나, 가상자원의 로그인 이력을 보존하고 모니터링할 수 있습니다.

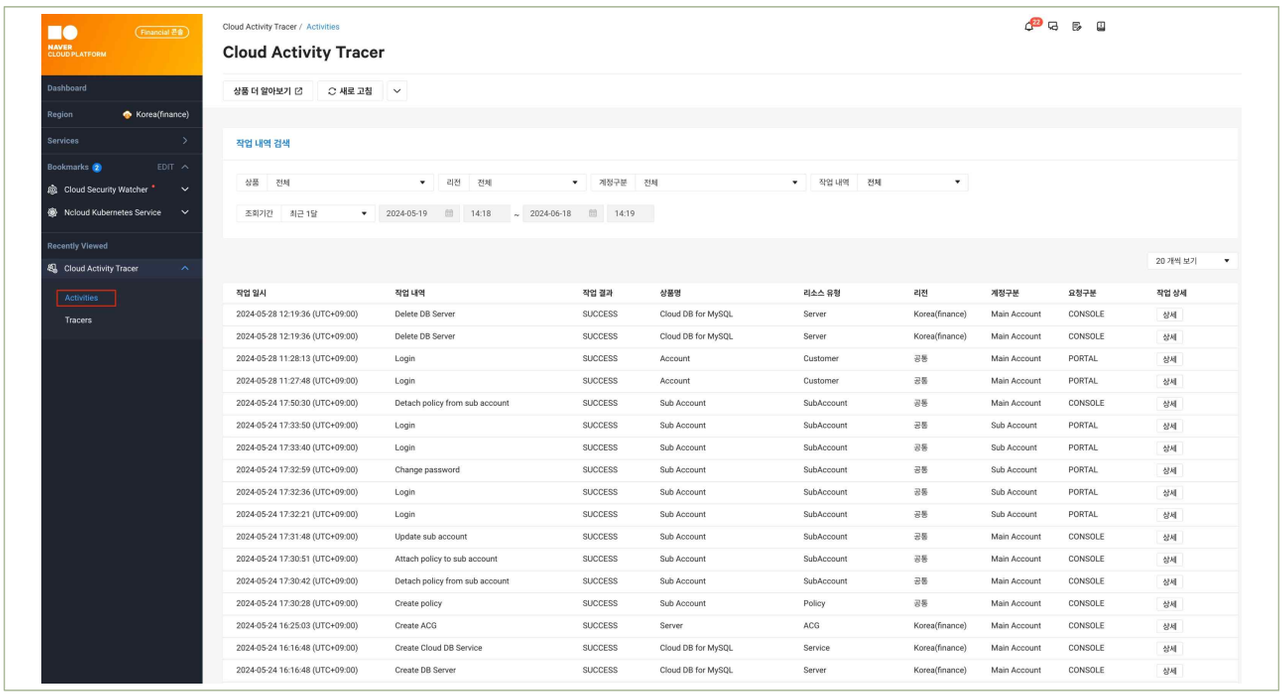
- **보존된 계정 활동 이력 확인**

  ① **(가상자원관리시스템)** 'Services' → 'Cloud Activity Tracer' 상품을 선택합니다.



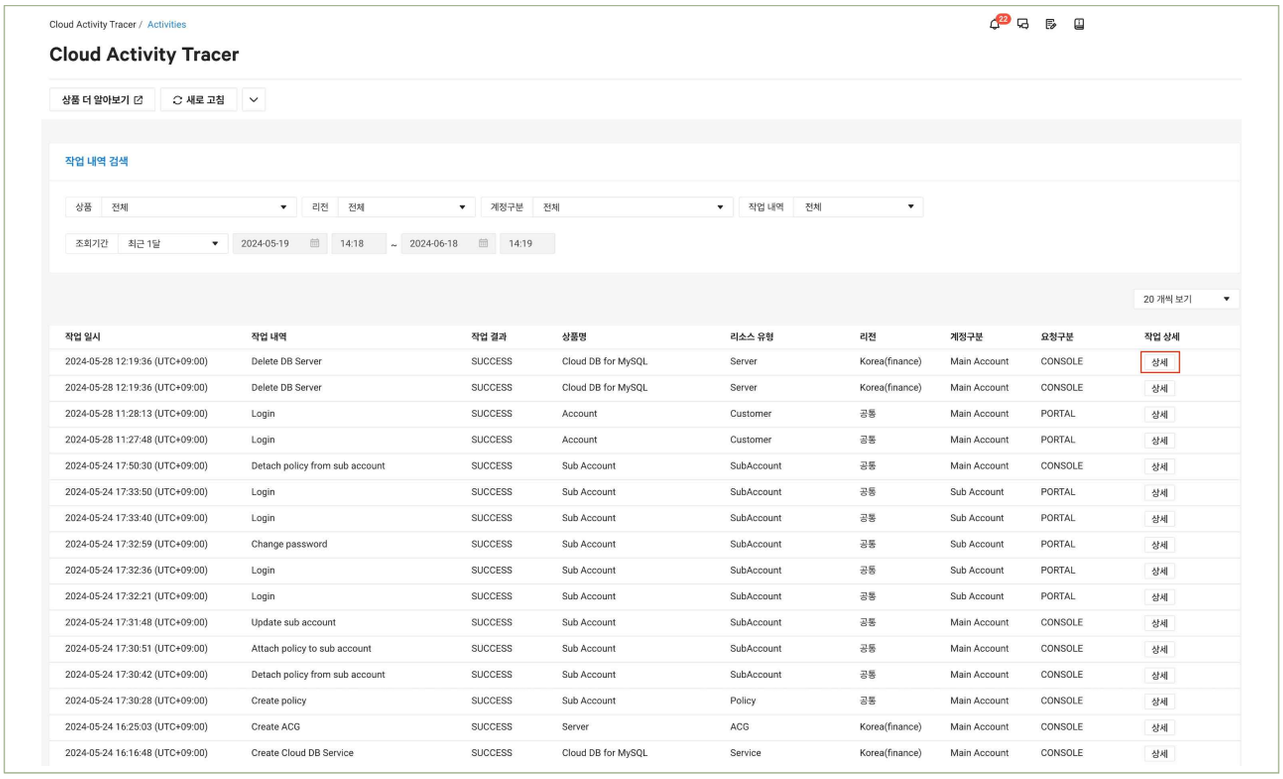
| 그림 5-1-1 | Cloud Activity Tracer 상품 선택

② **(가상자원관리시스템)** ‘Activities’를 통해 보존된 메인 계정, 서브 계정의 계정 활동 이력 목록을 확인합니다.



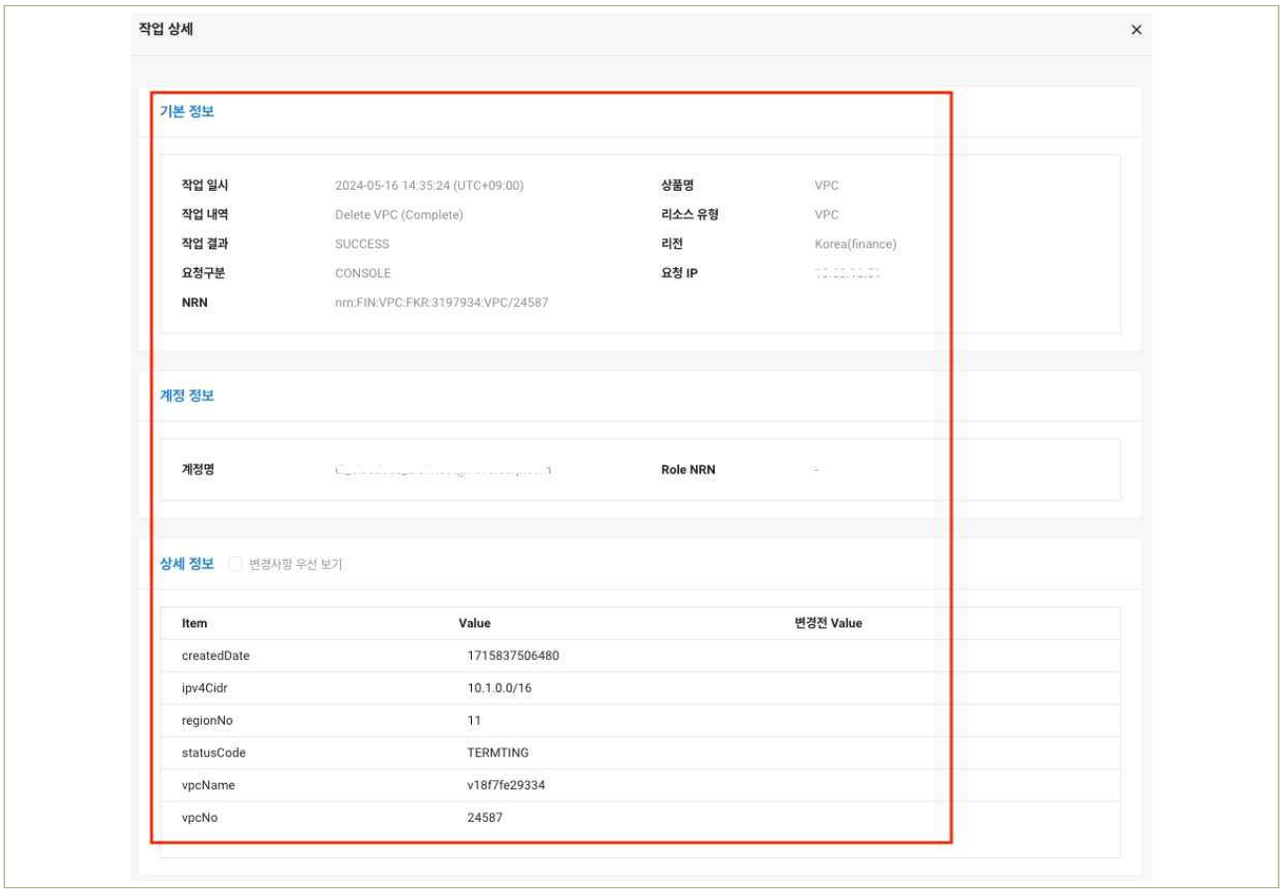
| 그림 5-1-2 | 계정 활동 이력 예시

③ **(가상자원관리시스템)** 계정 활동 이력에 대한 세부 내용을 확인을 위해 ‘상세’ 버튼을 클릭합니다.



| 그림 5-1-3 | 계정 활동 이력 예시

④ **(가상자원관리시스템)** 상세 계정 활동 이력을 확인합니다.



| 그림 5-1-4 | 상세 계정 활동 이력 예시

API를 통한 계정 활동 이력 확인

① **(API(CLI))** Cloud Activity Tracer의 'activities' API를 통해 메인계정 및 서브 계정의 활동 이력을 확인합니다.

- 요청 예시

```
POST https://cloudactivitytracer.apigw.fin-ntruss.com/api/v1/activities
```

- 요청 예시 (Body)

```
{
  "fromEventTime": "integer",
  "toEventTime": "integer",
  "nrn": "string",
  "pageIndex": "integer",
  "pageSize": "integer"
}
```

- 응답 예시 (성공)

```
{
  "historyId": "662625720e28854c967b05ba",
  "nrn": "nrn:FIN:IAM::3******:SubAccount/69dcb760-f7c3-11ee-ab36-005056a79369",
  "eventTime": 1713775985981,
  "platformType": "BOTH",
  "productName": "IAM",
  "productDisplayName": "Sub Account",
  "regionCode": "",
  "regionDisplayName": "Global",
  "resourceType": "SubAccount",
  "resourceId": "69dcb760-f7c3-11ee-ab36-005056a79369",
  "resourceName": "ncpfinsubuser1",
  "actionDisplayName": "Attach policy to sub account",
  "actionResultType": "SUCCESS",
  "actionUserType": "Customer",
  "sourceType": "CONSOLE",
  "sourceIp": "10.***.***.*7",
  "productData": {
      "subAccountNo": "69dcb760-f7c3-11ee-ab36-005056a79369",
      "subAccountId": "ncpfinsubuser1",
      "name": "김그린",
      "loginUrl": "c******",
      "canConsoleAccess": "true",
      "canProgramAccess": "false",
      "useConsolePermitIp": "false",
      "needDgr2Auth": "true",
      "needPasswordReset": "true",
      "createTime": "1712812916000",
      "dgr2Yn": "N",
      "policies[0].policyNo": "9d1a94b0-0085-11ef-8682-246e96591a38",
      "policies[0].policyName": "ncp-fin-bucket-policy",
      "policies[0].type": "USER_CREATED",
      "policies[0].createTime": "1713775933000"
    }
}
```

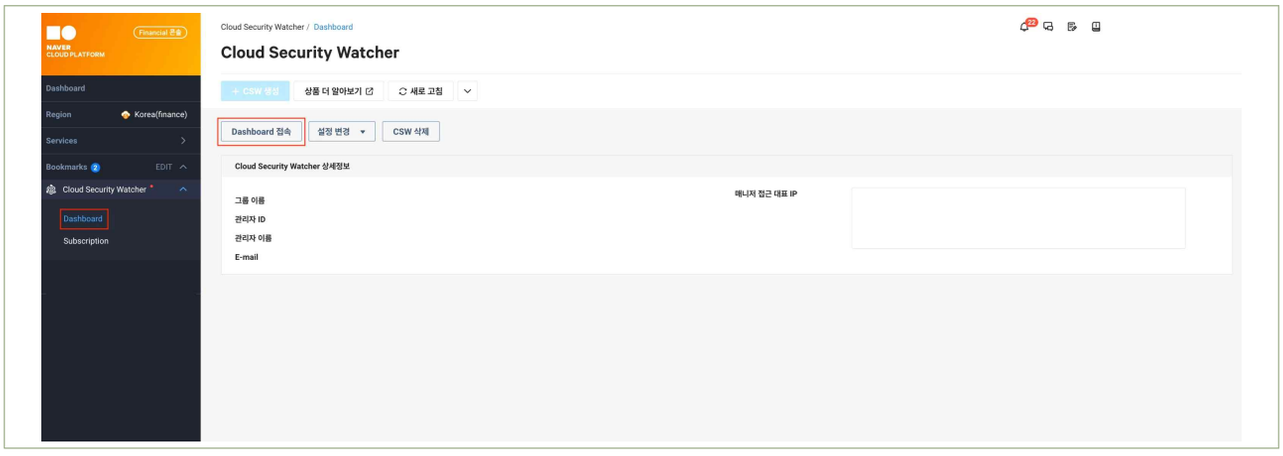
| 그림 5-1-5 | API를 통한 클라우드 계정 활동 이력 확인 예시

가상자원(서버) 로그인 이력 확인

① **(가상자원관리시스템)** ‘Services’ → ‘Cloud Security Watcher’ 상품을 선택합니다.

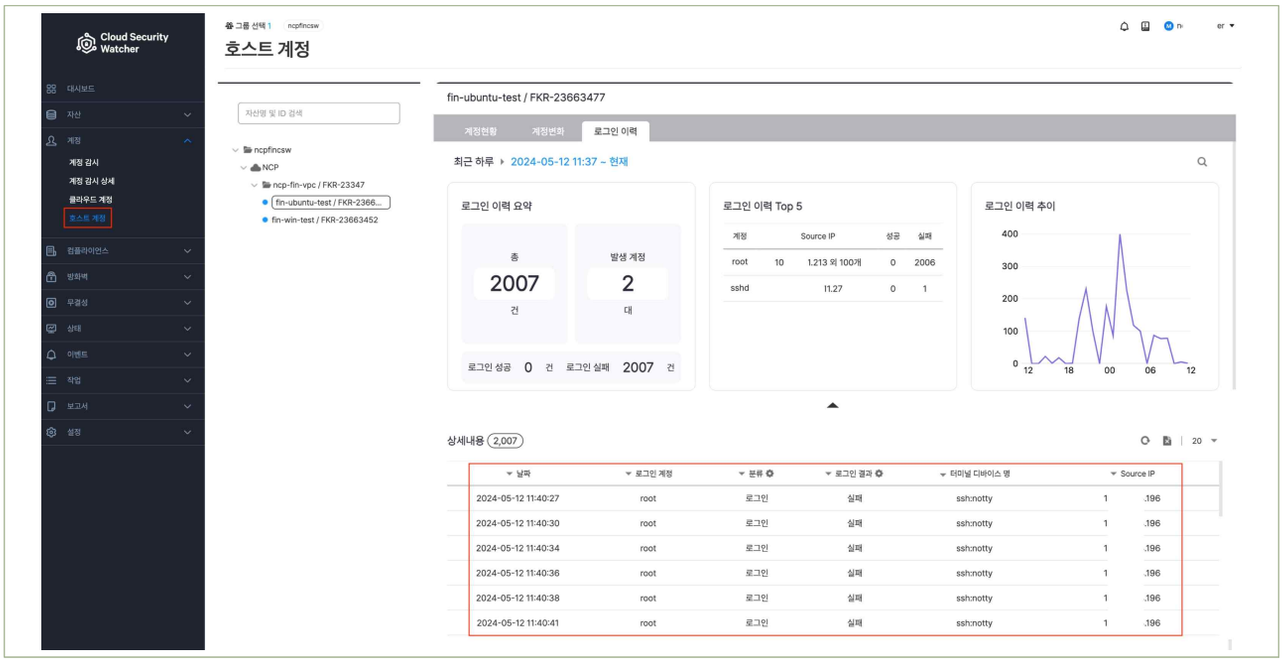
| 그림 5-1-6 | Cloud Security Watcher 상품 선택

② **(가상자원관리시스템)** ‘Dashboard’ → ‘Dashboard 접속’ 버튼을 클릭하여 Cloud Security Watcher 콘솔에 접속합니다.



| 그림 5-1-7 | Cloud Security Watcher 콘솔 접속

③ **(가상자원관리시스템)** '계정' → '호스트 계정'에서 가상자원(서버)의 로그인 이력 보존 현황을 확인합니다.



| 그림 5-1-8 | 가상자원(서버) 로그인 이력 예시

4 참고 사항

- [참고1] Cloud Activity Tracer 사용 가이드
- [참고2] Cloud Security Watcher 사용 가이드
- [참고3] Cloud Activity Tracer 이력 호출 API 사용 가이드

1 기준

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

2 설명

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

  - 예시

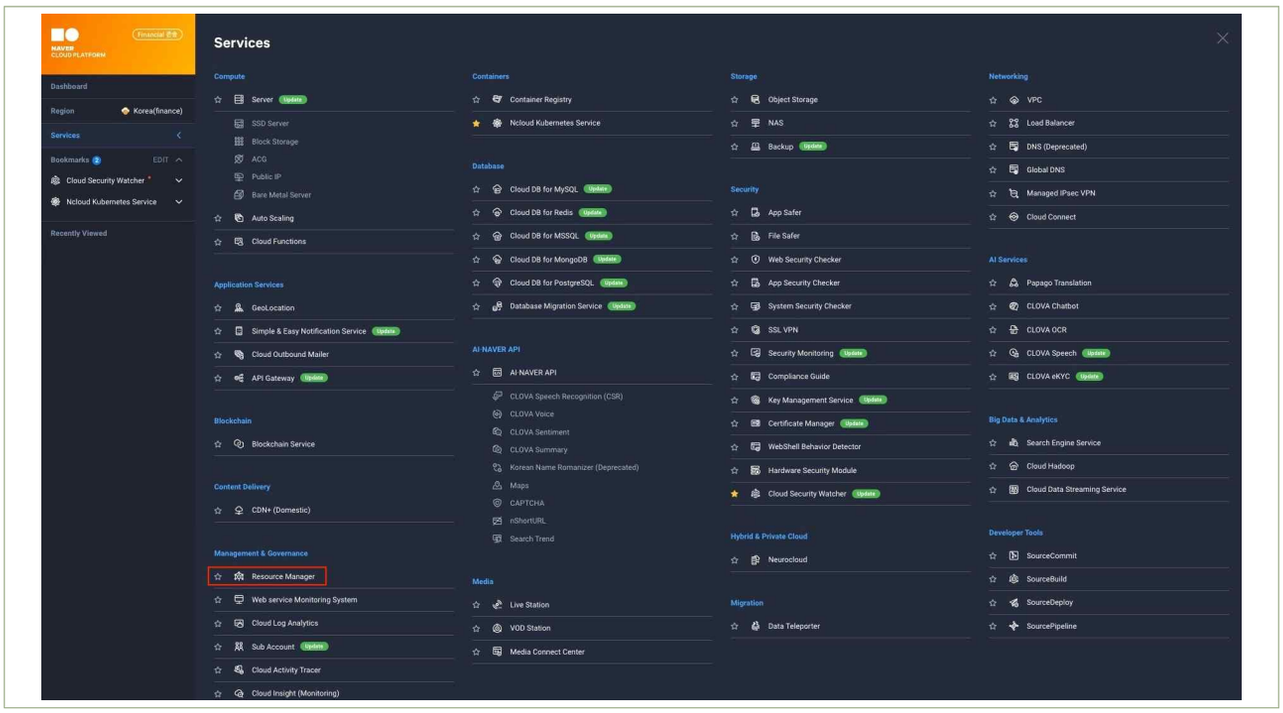
    1) 클라우드 가상자원 이용에 관한 행위추적성 증적(ex. 감사로그 등)에 대한 상시 모니터링 수행
    2) 금융회사 내부규정등 관련 규정을 통해 수립된 검토 기간에 맞추어 클라우드 가상자원 이용에 관한 행위추적성 증적에 대한 주기적 검토 수행

3 우수 사례

- 네이버 클라우드 플랫폼은 가상자원을 통합적으로 관리할 수 있는 Resource Manager를 통해 전체 리소스 현황을 한 번에 확인할 수 있습니다. Resource Manager에서 개별 리소스에 대한 태그(Tag)를 설정하여 논리적인 검색 및 관리를 수행할 수 있으며, Observer 기능을 통해 가상자원 변경 등 가상자원의 상태를 감시하여 SMS 또는 E-mail 알람을 받을 수 있도록 구성할 수 있습니다.
  또한, 리소스 현황 식별, 자산 변경 감시 등 클라우드 보안 형상 관리를 수행하는 Cloud Security Watcher 보안 상품을 활용하여 가상자원의 상태 변경에 대한 모니터링과 알림 조건을 더욱 상세히 설정할 수 있습니다.

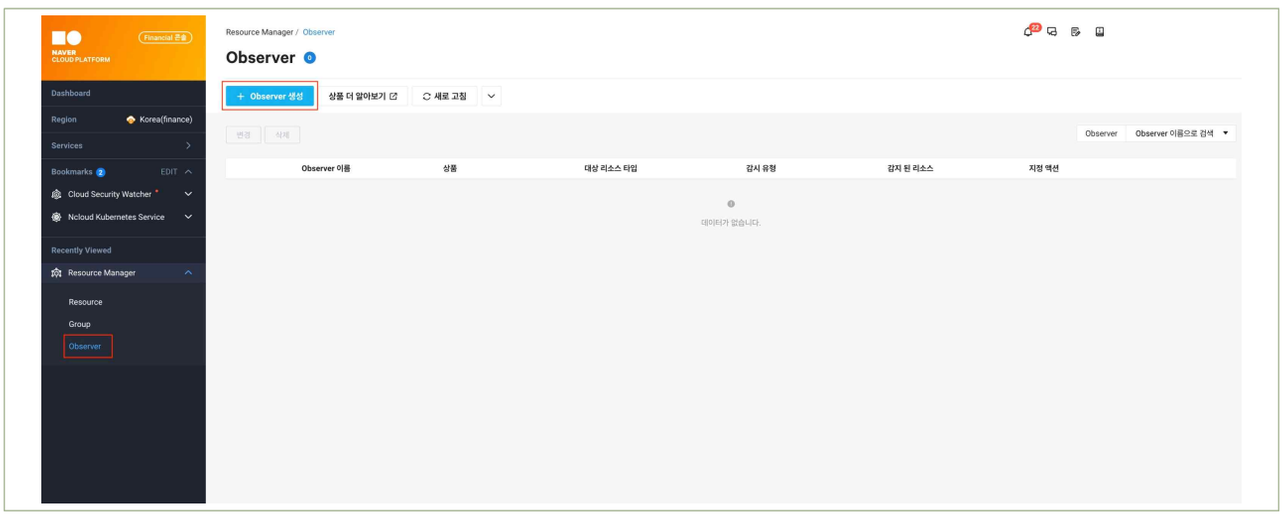
Resource Manager를 통한 가상자원 상태변경에 대한 모니터링

① **(가상자원관리시스템)** ‘Services’ → ‘Resource Manager’ 상품을 선택합니다.



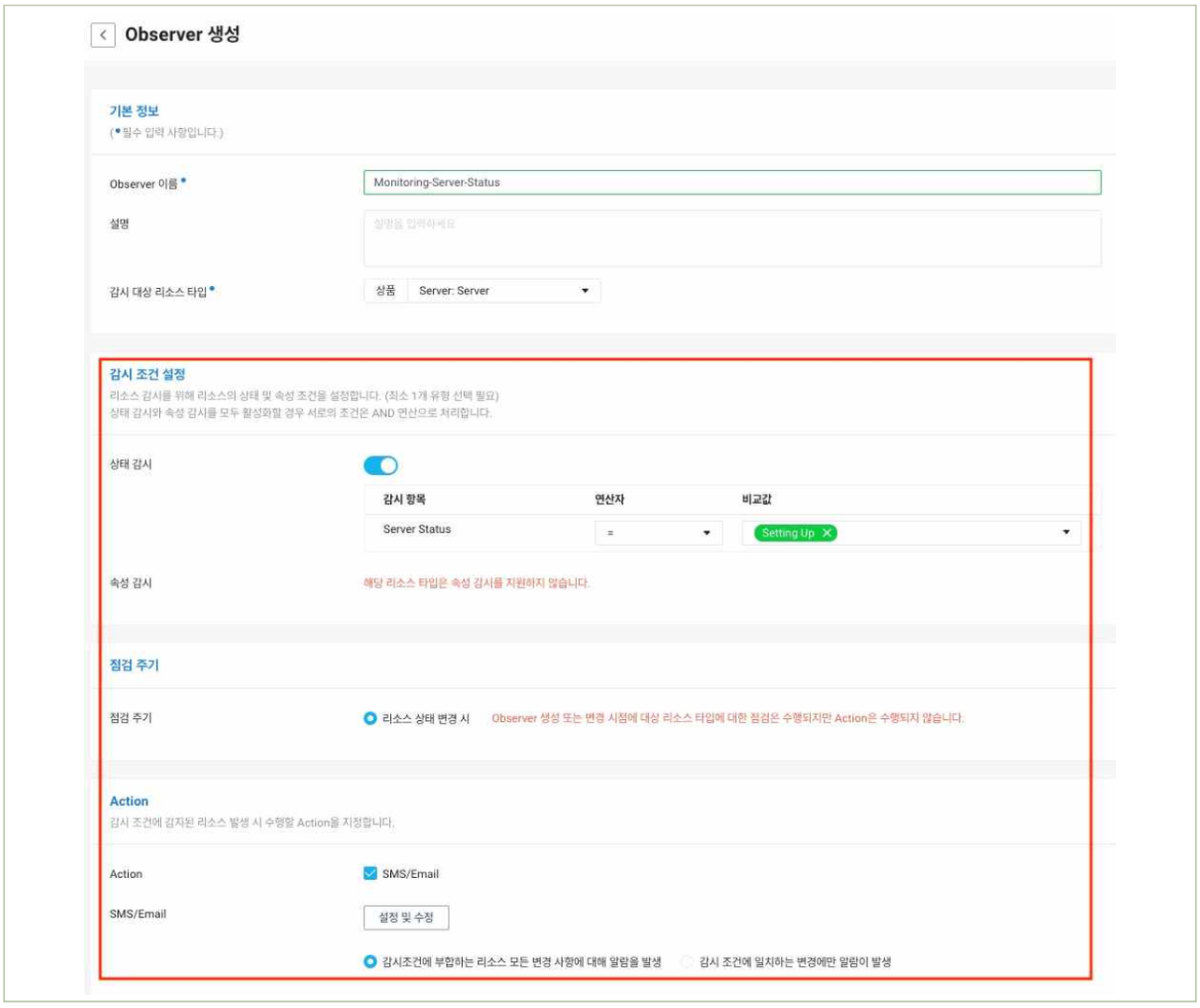
| 그림 5-2-1 | Resource Manager 상품 선택

② **(가상자원관리시스템)** ‘Observer’ → ‘+ Observer 생성’을 클릭합니다.



| 그림 5-2-2 | Observer 생성

③ **(가상자원관리시스템)** 가상자원에 대한 상태변경 감시 조건과 알림 대상을 설정합니다.



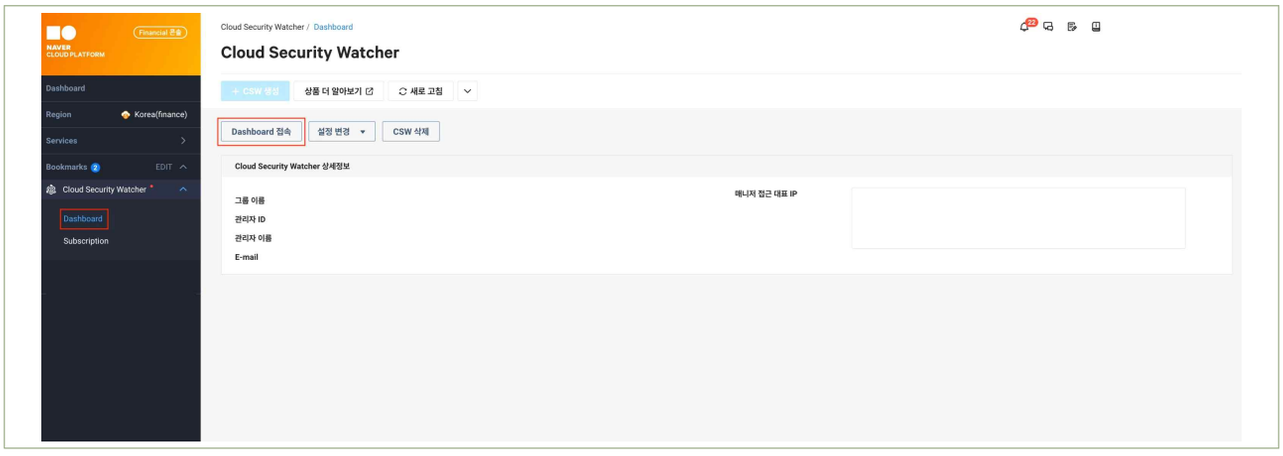
| 그림 5-2-3 | Observer를 통한 가상자원 상태변경 감시 설정 예시

Cloud Security Watcher를 통한 가상자원 상태변경에 대한 모니터링

① **(가상자원관리시스템)** ‘Services’ → ‘Cloud Security Watcher’ 상품을 선택합니다.

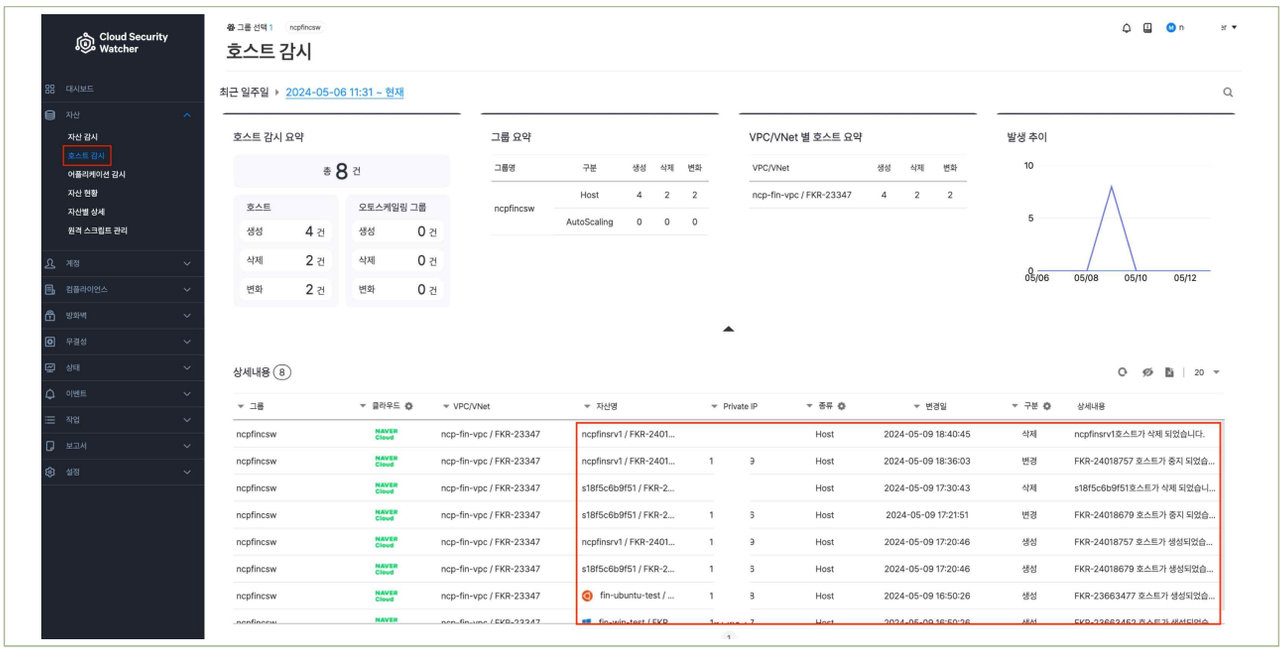
| 그림 5-2-4 | Cloud Security Watcher 상품 선택

② **(가상자원관리시스템)** ‘Dashboard’ → ‘Dashboard 접속’ 버튼을 클릭하여 Cloud Security Watcher 콘솔에 접속합니다.



| 그림 5-2-5 | Cloud Security Watcher 콘솔 접속

③ **(가상자원관리시스템)** '자산' → '호스트 감시'를 통해 가상자원의 상태변경 감시를 수행합니다.



| 그림 5-2-6 | Cloud Security Watcher를 통한 가상자원 상태변경 감시 예시

4 참고 사항

- [참고1] Resource Manager 사용 가이드
- [참고2] Cloud Security Watcher를 통한 자산 감시

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

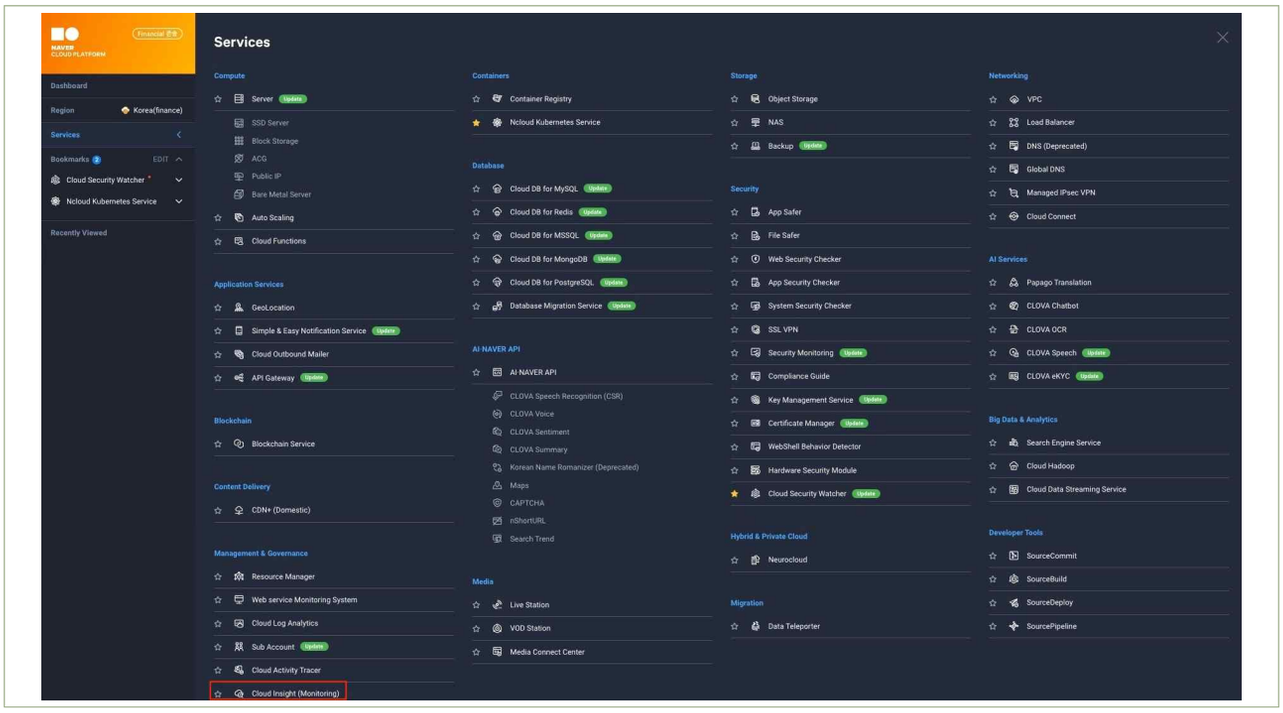
    1) 가상자원 상태 모니터링(사용량, 트래픽 용량 등)
    2) 가상자원 장애 모니터링(장애 발생 시 담당자 공지 등)
    3) 가상자원 장애 발생 시 장애상황기록부 작성 등
    4) 가상자원 네트워크 정책 변경(삭제 등) 모니터링

3 우수 사례

- 네이버 클라우드 플랫폼은 가상자원 및 네이버 클라우드 플랫폼 상품들의 성능 지표를 통합 관리하고, 장애 발생 시 담당자에게 장애 정보를 신속히 전달할 수 있는 모니터링 상품인 Cloud Insight를 통해 가상자원의 CPU, Memory, Disk, Network 등의 상태 모니터링을 지원합니다. 사용자는 Cloud Insight의 Event Rule을 통해 가용성에 대한 임계값 조건을 정의하고 Event 발생 시 장애 대응 담당자가 이를 인지할 수 있도록 알람을 구성할 수 있습니다.
  또한, 리소스 현황 식별, 자산 변경 감시 등 클라우드 보안 형상 관리를 수행하는 Cloud Security Watcher 보안 상품을 통해해서 가상자원 내의 CPU, Memory 사용에 대한 프로세스 정보를 가상자원관리시스템(클라우드 콘솔)을 통해 간편히 모니터링할 수 있습니다.

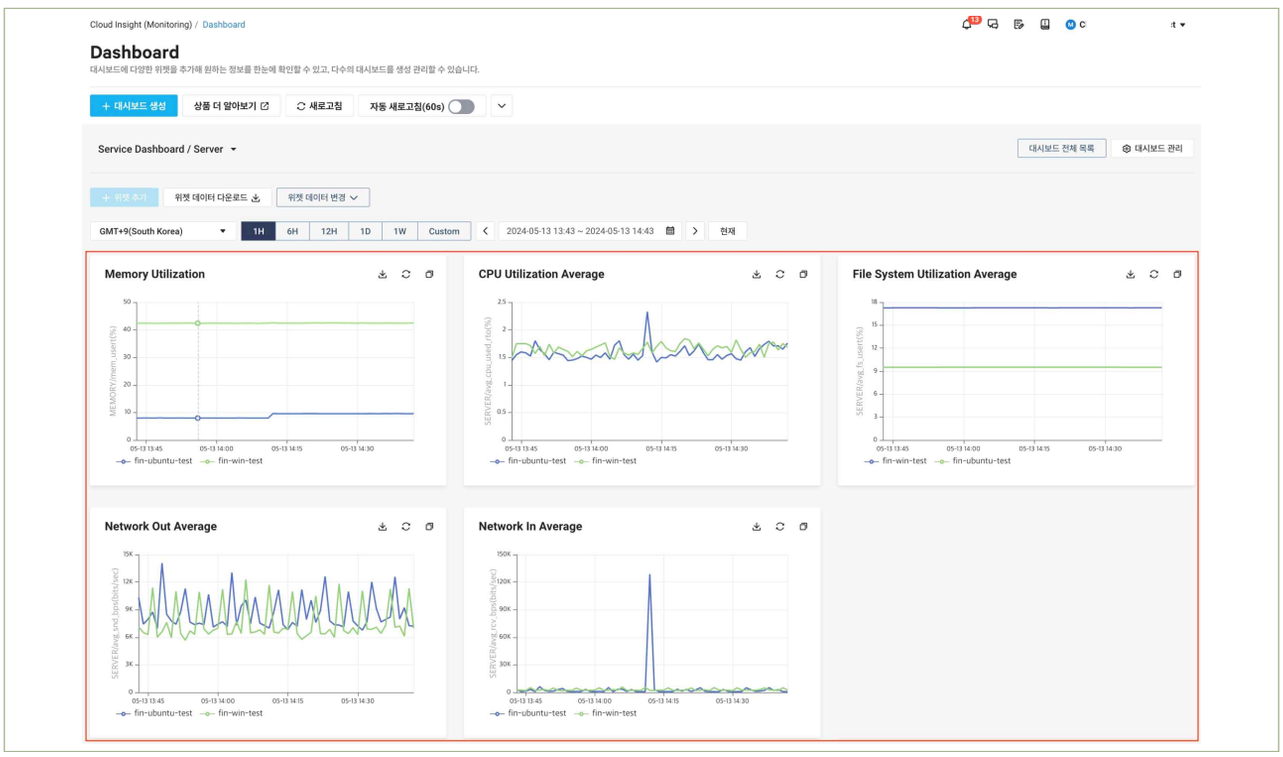
가상자원 운용에 관한 모니터링

① **(가상자원관리시스템)** ‘Services’ → ‘Cloud Insight’ 상품을 선택합니다.



| 그림 5-3-1 | Cloud Insight 상품 선택

② **(가상자원관리시스템)** ‘Dashboard’를 통해 가상자원 상태에 대한 모니터링을 수행합니다.



| 그림 5-3-2 | Cloud Insight를 통한 가상자원 상태 모니터링 예시

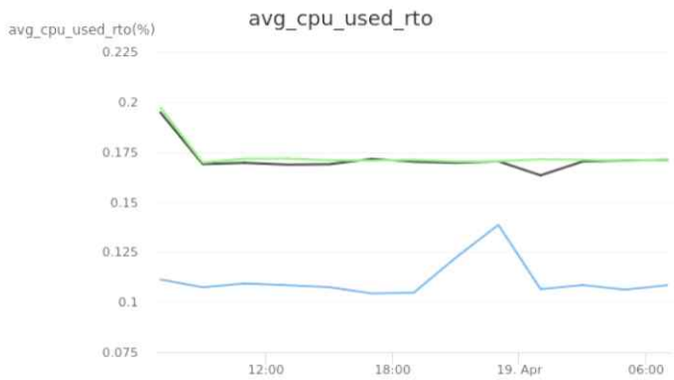
API를 통한 가상자원 운용 모니터링

① **(API(CLI))** 'GetDashboardWidgetImage' API를 통해 Cloud Insight의 모니터링 Widget 이미지를 확인하여 가상자원 상태를 모니터링합니다.

- 요청 예시

```
GET https://cw.apigw.fin-ntruss.com/cw_fea/real/cw/api/chart/dashboard/df_45795842904726323 2/widgets/avg_cpu_used_rto__45795842904726323 2?startTime=1650261600000&endTime=1650358800000
```

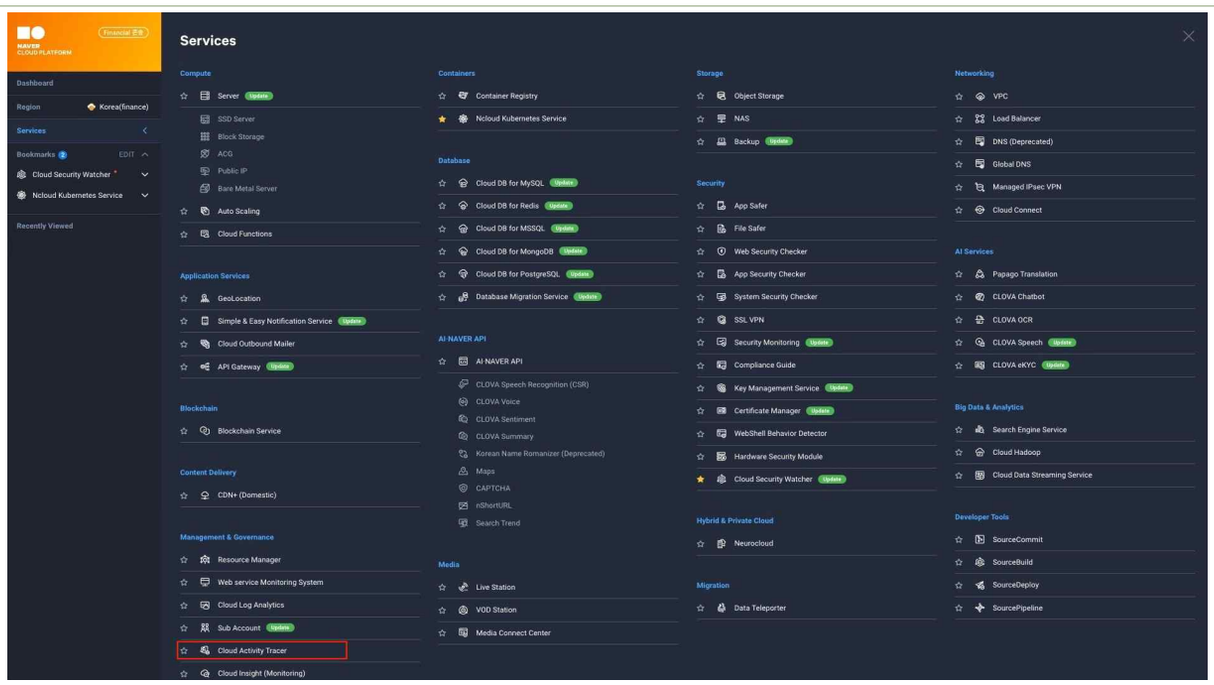
- 응답 예시



| 그림 5-3-3 | API를 통한 가상자원 상태 모니터링 예시

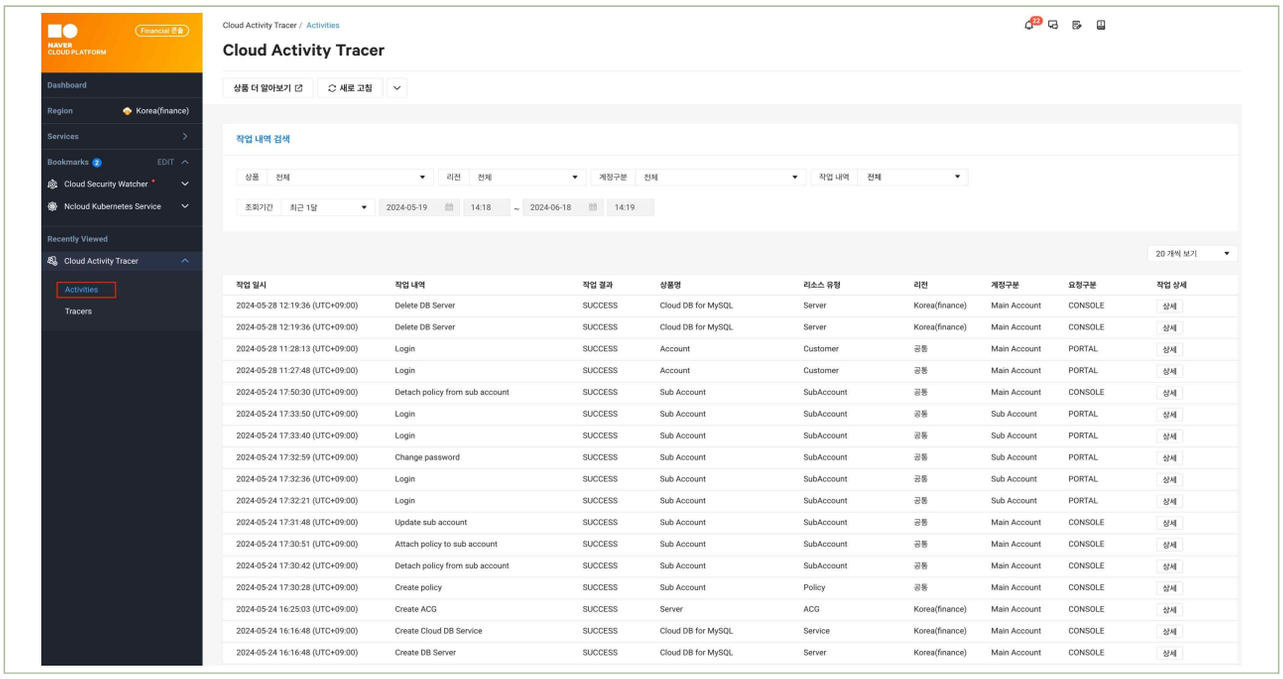
네트워크 정책 변경 모니터링

① **(가상자원관리시스템)** 'Services' → 'Cloud Activity Tracer' 상품을 선택합니다.



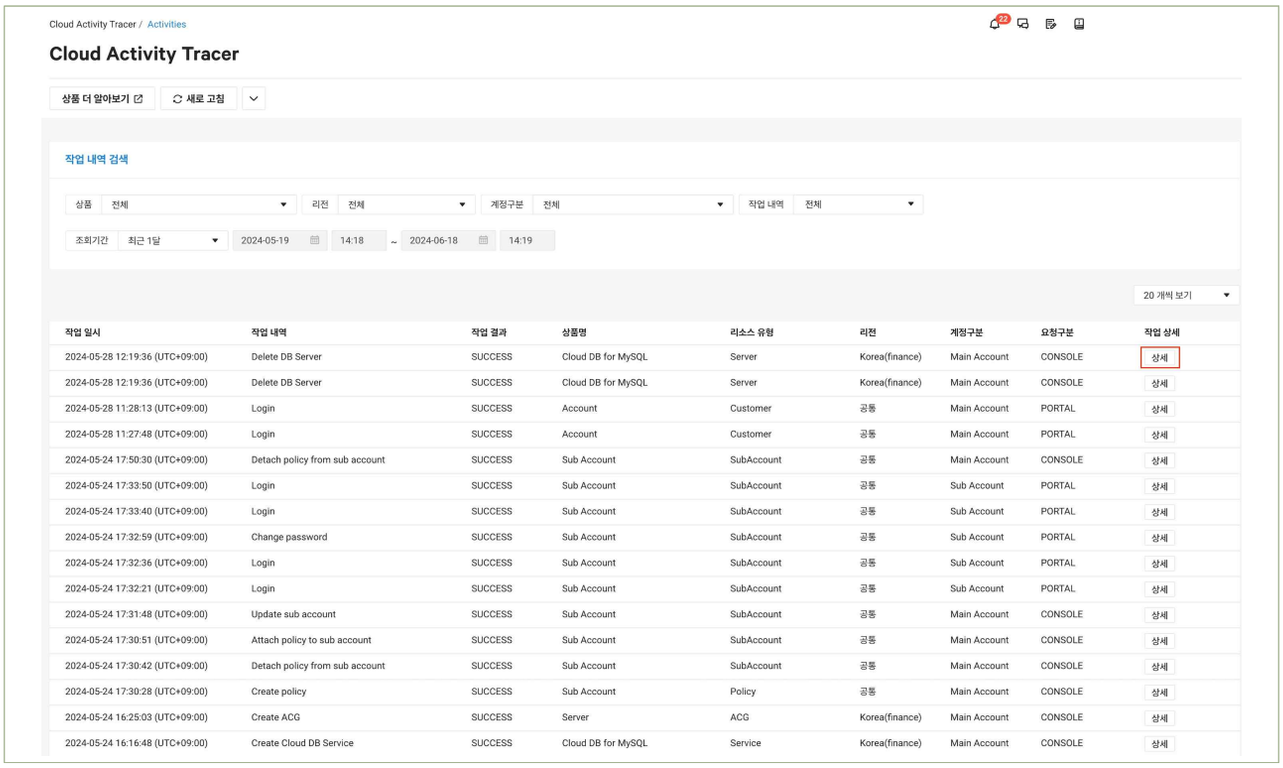
| 그림 5-3-4 | Cloud Activity Tracer 상품 선택

② **(가상자원관리시스템)** ‘Activities’를 통해 보존된 메인 계정, 서브 계정의 계정 활동 이력 목록을 확인합니다.



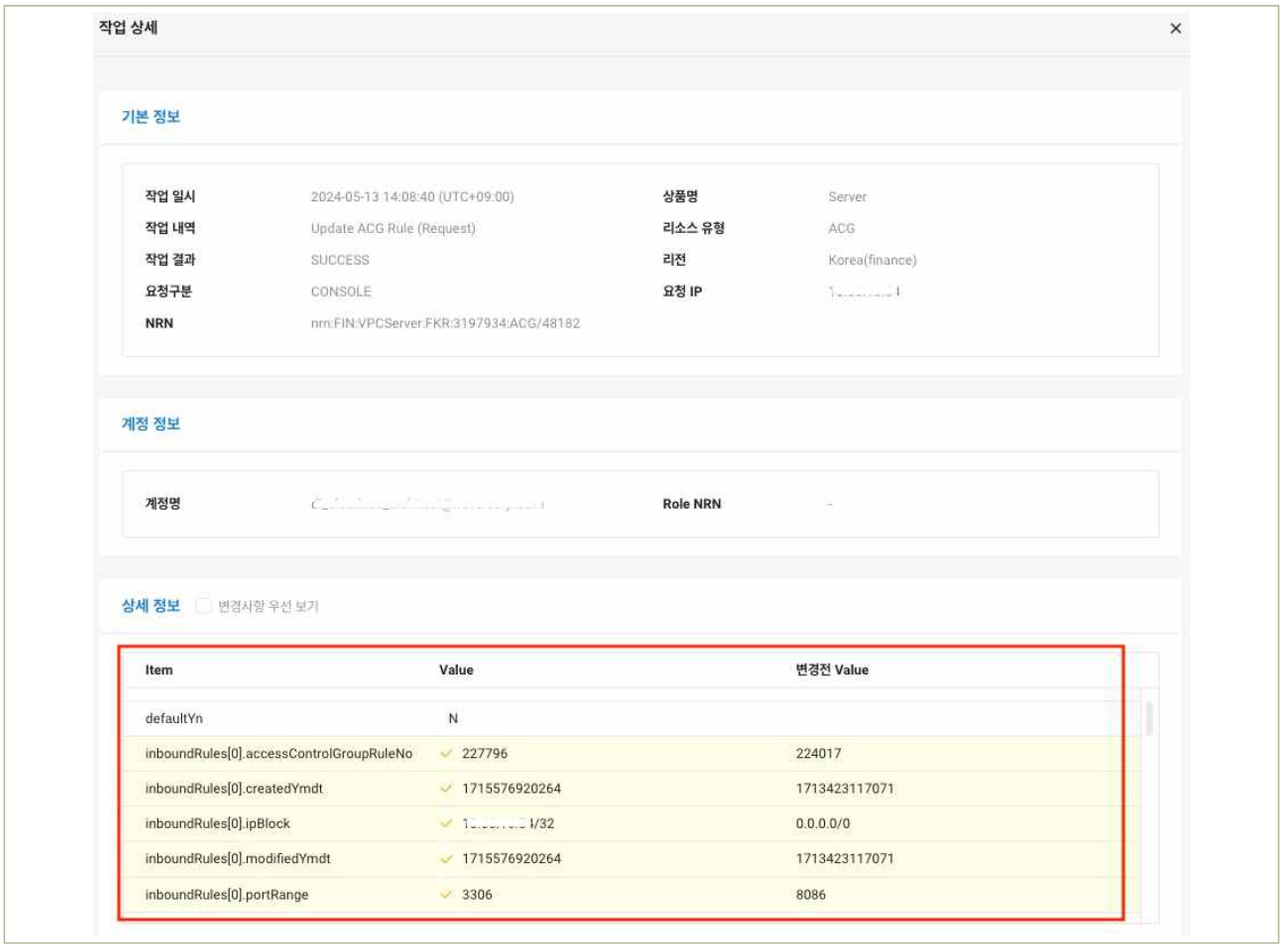
| 그림 5-3-5 | 계정 활동 이력 예시

③ **(가상자원관리시스템)** 계정 활동 이력에 대한 세부내용을 확인을 위해 ‘상세’ 버튼을 클릭합니다.



| 그림 5-3-6 | 계정 활동 이력 예시

④ **(가상자원관리시스템)** 상세 계정 활동 이력을 통해 ACG(Access Control Group), NACL(Network Access Control List) 등 가상자원 네트워크 정책 변경에 대한 모니터링을 수행합니다.



| 그림 5-3-7 | Cloud Activity Tracer를 통한 네트워크 정책 변경 모니터링 예시

API를 통한 계정 활동 이력 확인

① **(API(CLI))** 'activities' API를 통해 네트워크 정책 변경 이력을 확인합니다.

- 요청 예시

```
POST https://cloudactivitytracer.apigw.fin-ntruss.com/api/v1/activities
```

- 요청 예시 (Body)

```
{
  "fromEventTime": "integer",
  "toEventTime": "integer",
  "nrn": "string",
  "pageIndex": "integer",
  "pageSize": "integer"
}
```

- 응답 예시 (성공)

```
{
    "historyId": "664b11f4e1fd0965ef436e8e",
    "nrn": "nrn:FIN:VPCServer:FKR:3******:ACG/4****",
    "eventTime": 1716195828526,
    "platformType": "VPC",
    "productName": "VPCServer",
    "productDisplayName": "Server",
    "regionCode": "FKR",
    "regionDisplayName": "Korea(finance)",
    "resourceType": "ACG",
    "resourceId": "4***8",
    "resourceName": "cloud-mysql-*****",
    "actionDisplayName": "Create ACG",
    "actionResultType": "SUCCESS",
    "actionUserType": "Customer",
    "sourceType": "API",
    "sourceIp": "10.***.***.*9",
    "productData": {
        "defaultYn": "N",
        "vpcName": "ncp-fin-vpc",
        "createdYmdt": "1716195828501",
        "accessControlGroupNo": "4****",
        "outboundRuleCount": "0",
        "accessControlGroupName": "cloud-mysql-*****",
        "memberNo": "3******",
        "modifiedYmdt": "1716195828501",
        "inboundRuleCount": "0",
        "vpcNo": "2****",
        "networkInterfaceCount": "0",
        "statusCode": "RUN"
    }
}
```

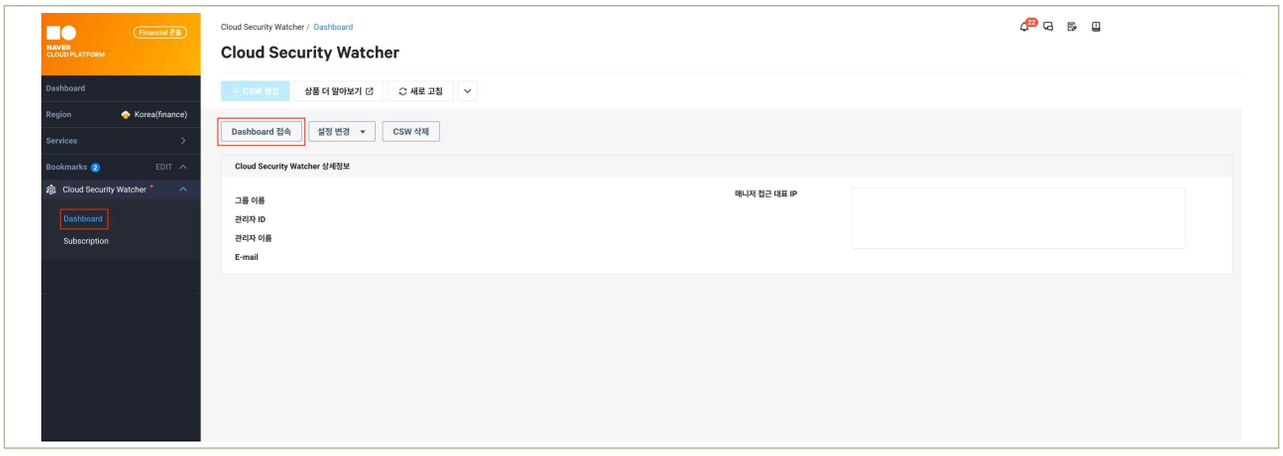
| 그림 5-3-8 | API를 통한 네트워크 정책 변경 이력 확인 예시

Cloud Security Watcher를 통한 가상자원 상태변경에 대한 모니터링

① **(가상자원관리시스템)** 'Services' → 'Cloud Security Watcher' 상품을 선택합니다.

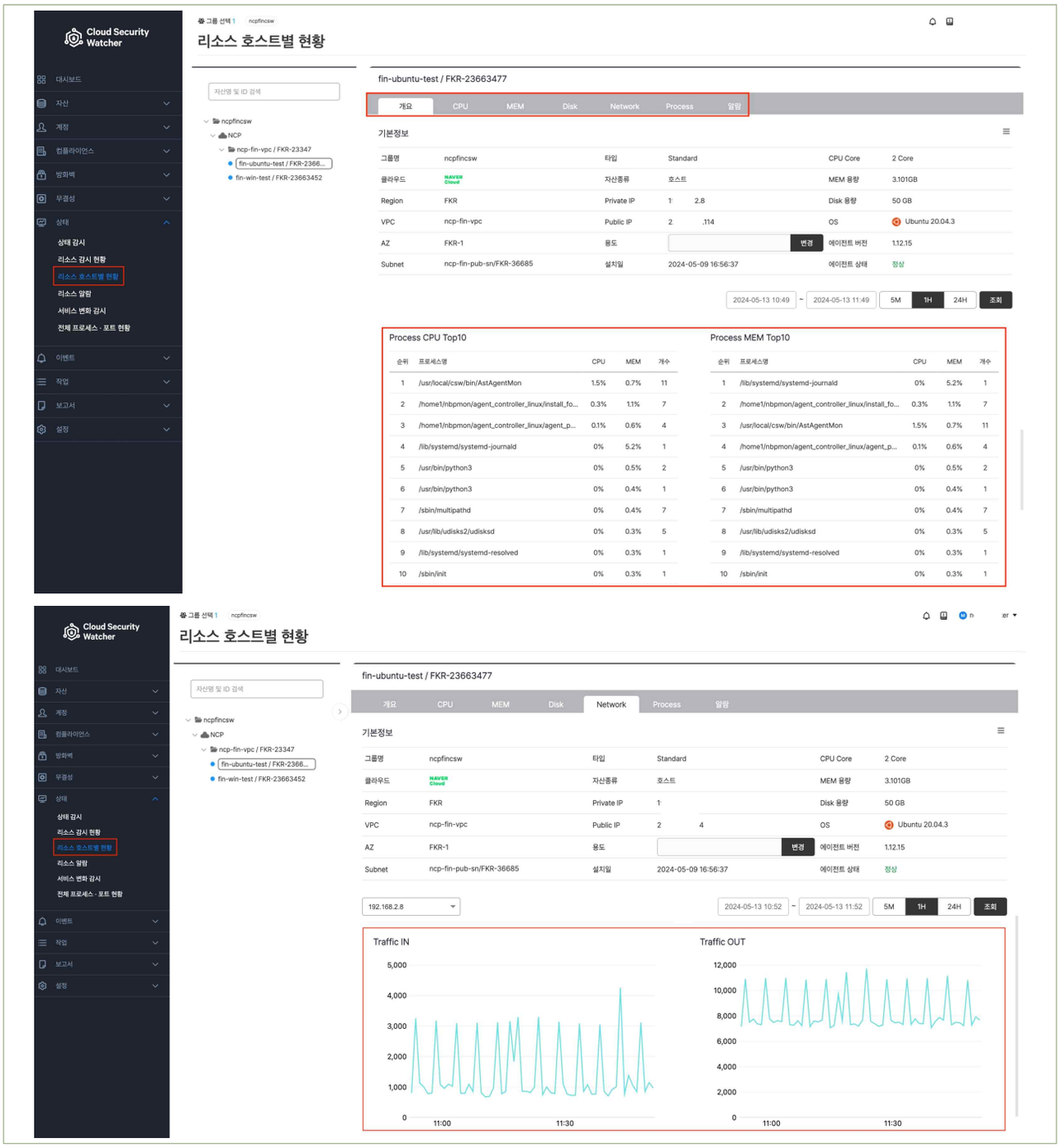
| 그림 5-3-9 | Cloud Security Watcher 상품 선택

② **(가상자원관리시스템)** 'Dashboard' → 'Dashboard 접속' 버튼을 클릭하여 Cloud Security Watcher 콘솔에 접속합니다.



| 그림 5-3-10 | Cloud Security Watcher 콘솔 접속

③ **(가상자원관리시스템)** '상태' → '리소스 호스트별 현황'을 통해 가상자원 상태에 대한 모니터링을 수행합니다.



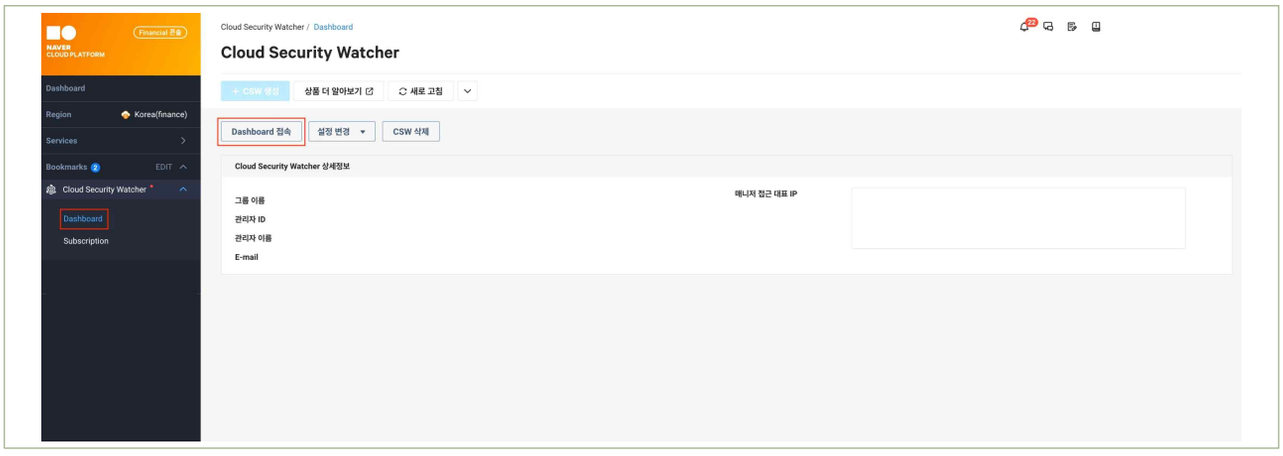
| 그림 5-3-11 | Cloud Security Watcher를 통한 가상자원 상태 모니터링 예시

Cloud Security Watcher를 통한 네트워크 정책 변경 모니터링

① **(가상자원관리시스템)** ‘Services’ → ‘Cloud Security Watcher’ 상품을 선택합니다.

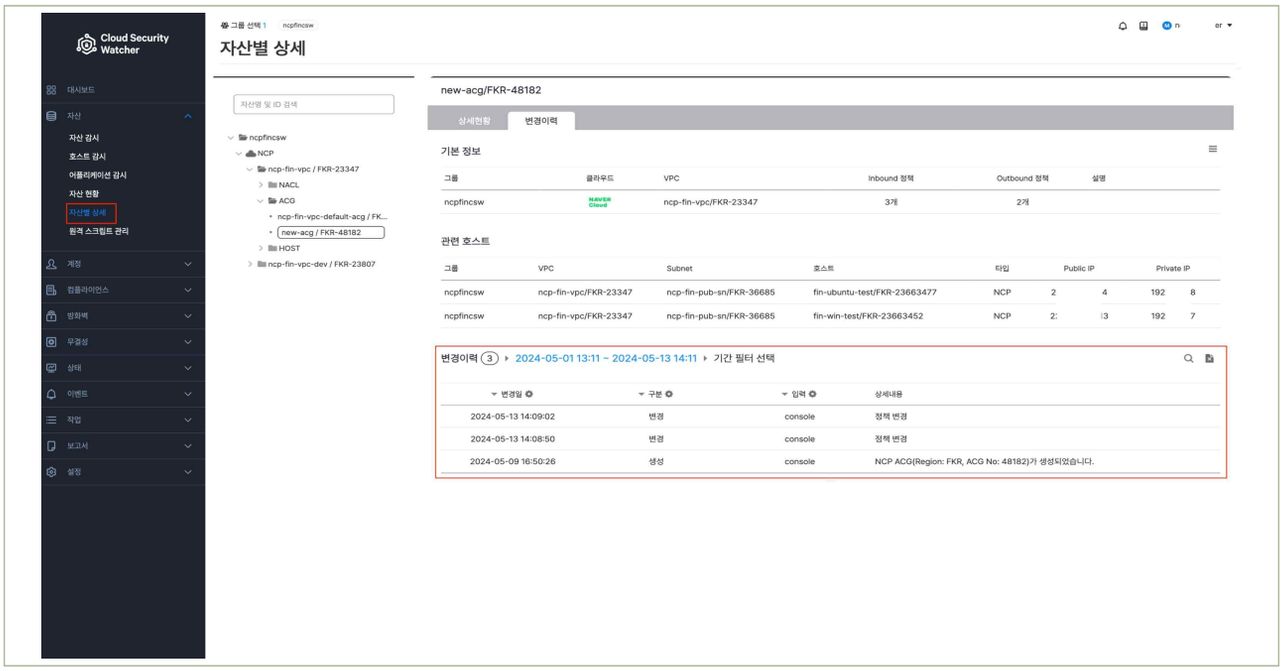
| 그림 5-3-12 | Cloud Security Watcher 상품 선택

② **(가상자원관리시스템)** ‘Dashboard’ → ‘Dashboard 접속’ 버튼을 클릭하여 Cloud Security Watcher 콘솔에 접속합니다.



| 그림 5-3-13 | Cloud Security Watcher 콘솔 접속

③ **(가상자원관리시스템)** '자산' → '자산별 상세'를 통해 ACG(Access Control Group), NACL (Network Access Control List) 등 가상자원 네트워크 정책 변경에 대한 모니터링을 수행합니다.



| 그림 5-3-14 | Cloud Security Watcher를 통한 네트워크 정책 변경 모니터링 예시

4 참고 사항

- [참고1] Cloud Insight 사용 가이드
- [참고2] Cloud Insight 대시보드 사용 가이드
- [참고3] Cloud Security Watcher를 통한 상태감시 가이드
- [참고4] Cloud Insight 위젯이미지 호출 API 사용 가이드
- [참고5] Cloud Activity Tracer 이력 호출 API 사용 가이드

1 기준

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

2 설명

- API 사용 이력에 대한 행위추적성을 확보하여야 한다.

  - 예시 (행위 감사로그)

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

3 우수 사례

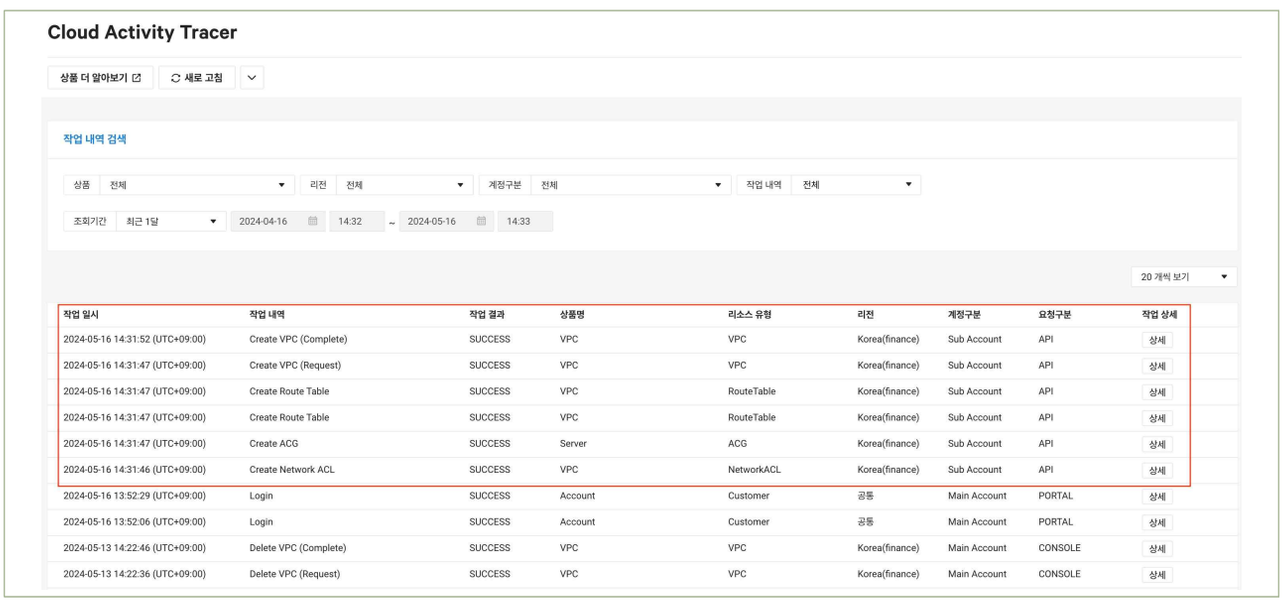
- 네이버 클라우드 플랫폼은 메인 계정과 서브 계정의 활동 로그를 수집하고 조회하는 Cloud Activity Tracer 상품을 통해 가상자원관리시스템(클라우드 콘솔) 및 API 사용에 대한 접근 시간, 접근ID, 작업 내용 등을 상세히 기록하여 1년간 보존합니다. 사용자는 이를 통해 언제든지 가상자원관리시스템(클라우드 콘솔)에서 메인 계정과 서브 계정의 활동 기록을 간편하게 열람할 수 있으며, 전자금융감독규정 제13조(전산자료 보호대책) 등에 따라 계정 활동의 장기보존을 위해 Object Storage 상품을 연동하여 안전하게 보관할 수 있습니다.

API 사용이력의 보존

① **(가상자원관리시스템)** ‘Services’ → ‘Cloud Activity Tracer’ 상품을 선택합니다.

| 그림 5-4-1 | Cloud Activity Tracer 상품 선택

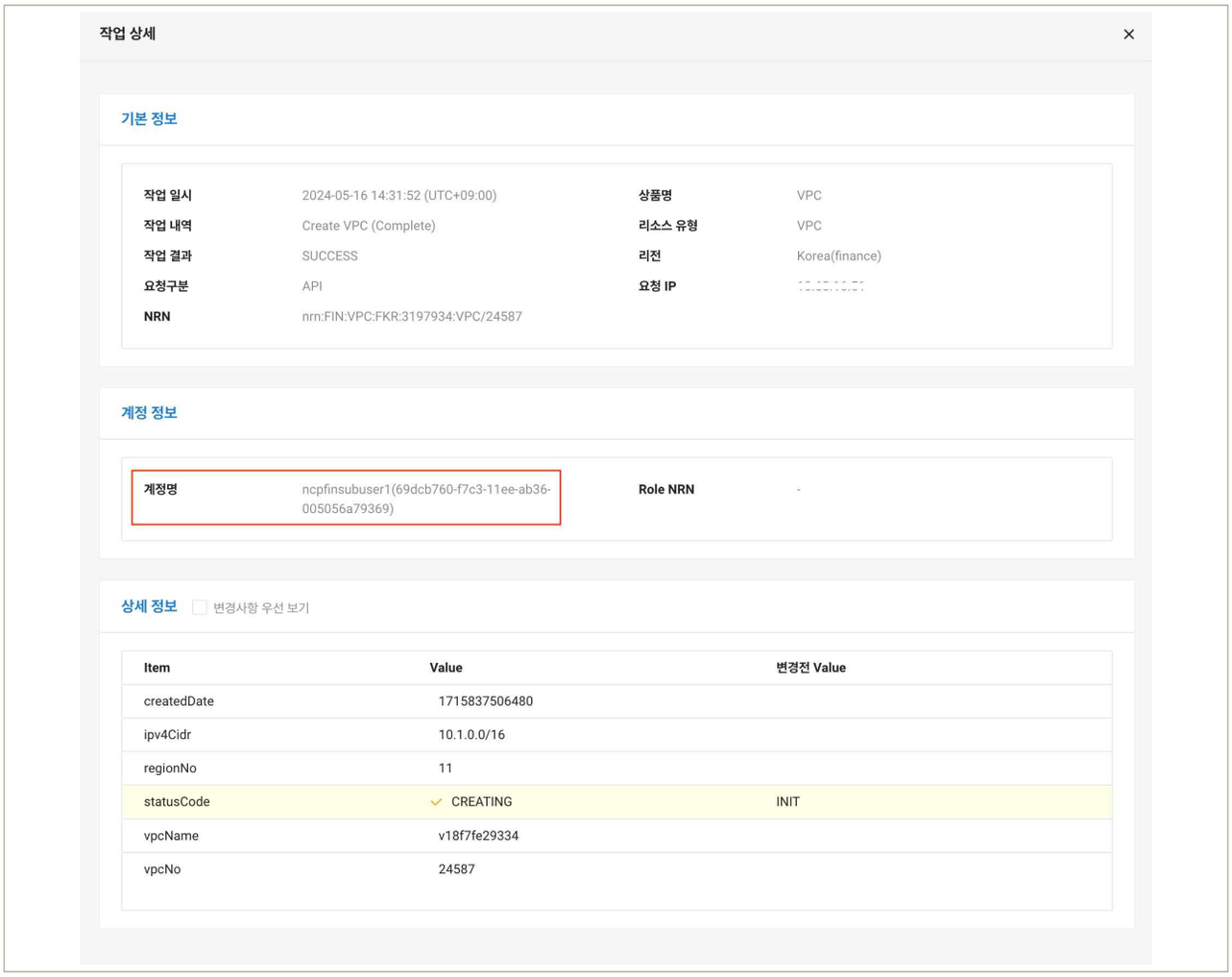
② **(가상자원관리시스템)** ‘Activities’를 통해 기록된 API 사용 이력에 대해 확인합니다.



작업 일시	작업 내역	작업 결과	상품명	리소스 유형	리전	계정구분	요청구분	작업 상세
2024-05-16 14:31:52 (UTC+09:00)	Create VPC (Complete)	SUCCESS	VPC	VPC	Korea(finance)	Sub Account	API	상세
2024-05-16 14:31:47 (UTC+09:00)	Create VPC (Request)	SUCCESS	VPC	VPC	Korea(finance)	Sub Account	API	상세
2024-05-16 14:31:47 (UTC+09:00)	Create Route Table	SUCCESS	VPC	RouteTable	Korea(finance)	Sub Account	API	상세
2024-05-16 14:31:47 (UTC+09:00)	Create Route Table	SUCCESS	VPC	RouteTable	Korea(finance)	Sub Account	API	상세
2024-05-16 14:31:47 (UTC+09:00)	Create ACG	SUCCESS	Server	ACG	Korea(finance)	Sub Account	API	상세
2024-05-16 14:31:46 (UTC+09:00)	Create Network ACL	SUCCESS	VPC	NetworkACL	Korea(finance)	Sub Account	API	상세
2024-05-16 13:52:29 (UTC+09:00)	Login	SUCCESS	Account	Customer	공통	Main Account	PORTAL	상세
2024-05-16 13:52:06 (UTC+09:00)	Login	SUCCESS	Account	Customer	공통	Main Account	PORTAL	상세
2024-05-13 14:22:46 (UTC+09:00)	Delete VPC (Complete)	SUCCESS	VPC	VPC	Korea(finance)	Main Account	CONSOLE	상세
2024-05-13 14:22:36 (UTC+09:00)	Delete VPC (Request)	SUCCESS	VPC	VPC	Korea(finance)	Main Account	CONSOLE	상세

| 그림 5-4-2 | Cloud Activity Tracer를 통한 API 사용 이력 확인 예시

③ **(가상자원관리시스템)** API 사용에 대한 상세 내역 확인을 위해 '상세'버튼을 클릭합니다.



| 그림 5-4-3 | Cloud Activity Tracer를 통한 API 사용 이력 상세 예시

API를 통한 API 사용 이력 확인

① **(API(CLI))** 'activities' API를 통해 메인 계정 및 서브 계정의 API 사용 이력을 확인합니다.

- 요청 예시

```
POST https://cloudactivitytracer.apigw.fin-ntruss.com/api/v1/activities
```

- 요청 예시 (Body)

```
{
  "fromEventTime": "integer",
  "toEventTime": "integer",
  "nrn": "string",
  "pageIndex": "integer",
  "pageSize": "integer"
}
```

- 응답 예시 (성공)


```
{
    "historyId": "66459a48e1fd0965ef3da817",
    "nrn": "nrn:FIN:VPC:FKR:3******:VPC/2****",
    "eventTime": 1715837512529,
    "platformType": "VPC",
    "productName": "VPC",
    "productDisplayName": "VPC",
    "regionCode": "FKR",
    "regionDisplayName": "Korea(finance)",
    "resourceType": "VPC",
    "resourceId": "2****",
    "resourceName": "v18f7fe29334",
    "actionDisplayName": "Create VPC (Complete)",
    "actionResultType": "SUCCESS",
    "actionUserType": "Sub",
    "actionSubAccountNo": 9****,
    "sourceType": "API",
    "sourceIp": "10.***.***.*1",
    "productData": {
        "vpcName": "v18f7fe29334",
        "createdDate": "1715837506480",
        "ipv4Cidr": "10.***.***.0/16",
        "vpcNo": "2****",
        "regionNo": "11",
        "statusCode": "CREATING"
    }
}
```


| 그림 5-4-4 | API를 통한 API 사용 이력 확인 예시

4 참고 사항

- [참고1] 계정활동 이력 조회 가이드
- [참고2] Cloud Activity Tracer 이력 호출 API 사용 가이드

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.

  - 예시 (행위 감사로그)

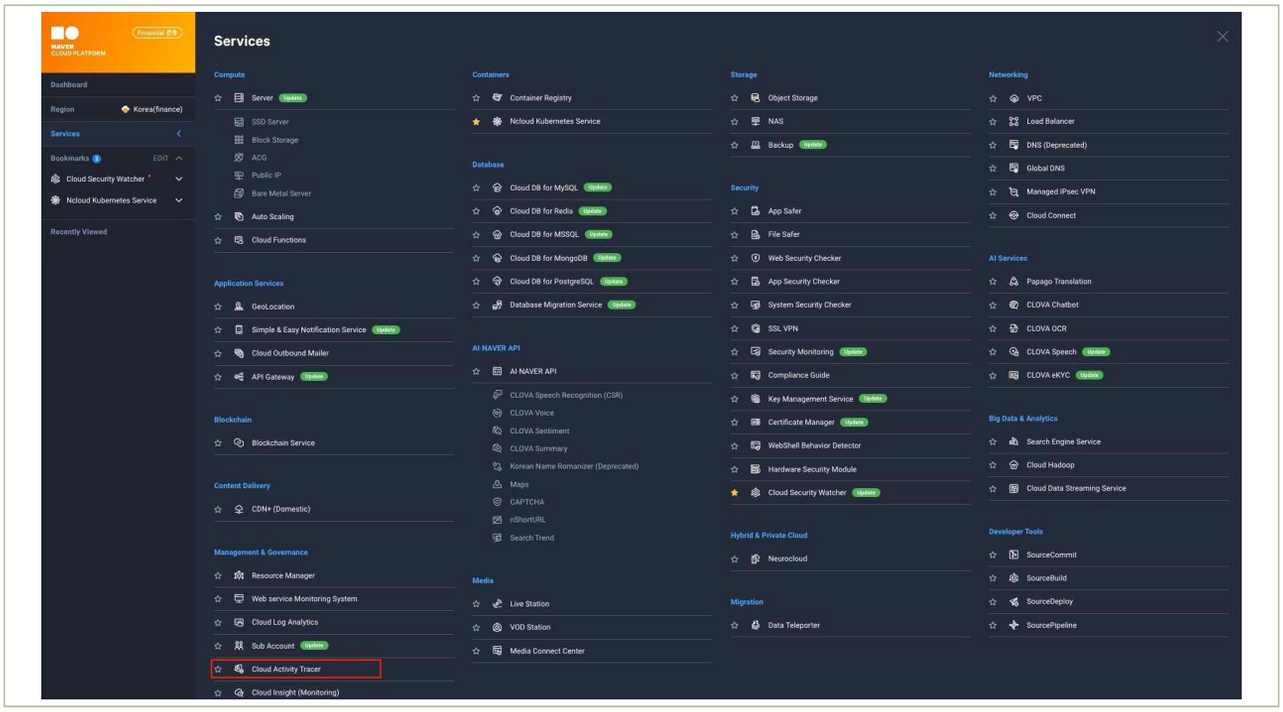
    1) 네트워크 서비스 이용에 관한 사항(VPC, NAT 규칙 생성 및 변경 등) 등

3 우수 사례

- 네이버 클라우드 플랫폼은 메인 계정과 서브 계정의 활동 로그를 수집하고 조회하는 Cloud Activity Tracer 상품을 통해 가상자원관리시스템(클라우드 콘솔) 및 API를 이용한 네트워크 변경 이력에 대하여 접근 시간, 접근ID, 작업 내용 등을 상세히 기록하고 1년간 안전하게 보존합니다. 사용자는 이를 통해 언제든지 가상자원관리시스템(클라우드 콘솔)에서 메인 계정과 서브 계정의 네트워크 변경 기록을 간편하게 열람할 수 있으며, 전자금융감독규정 제13조(전산자료 보호대책) 등에 따라 계정 활동의 장기보존을 위해 Object Storage 상품을 연동하여 안전하게 보관할 수 있습니다.

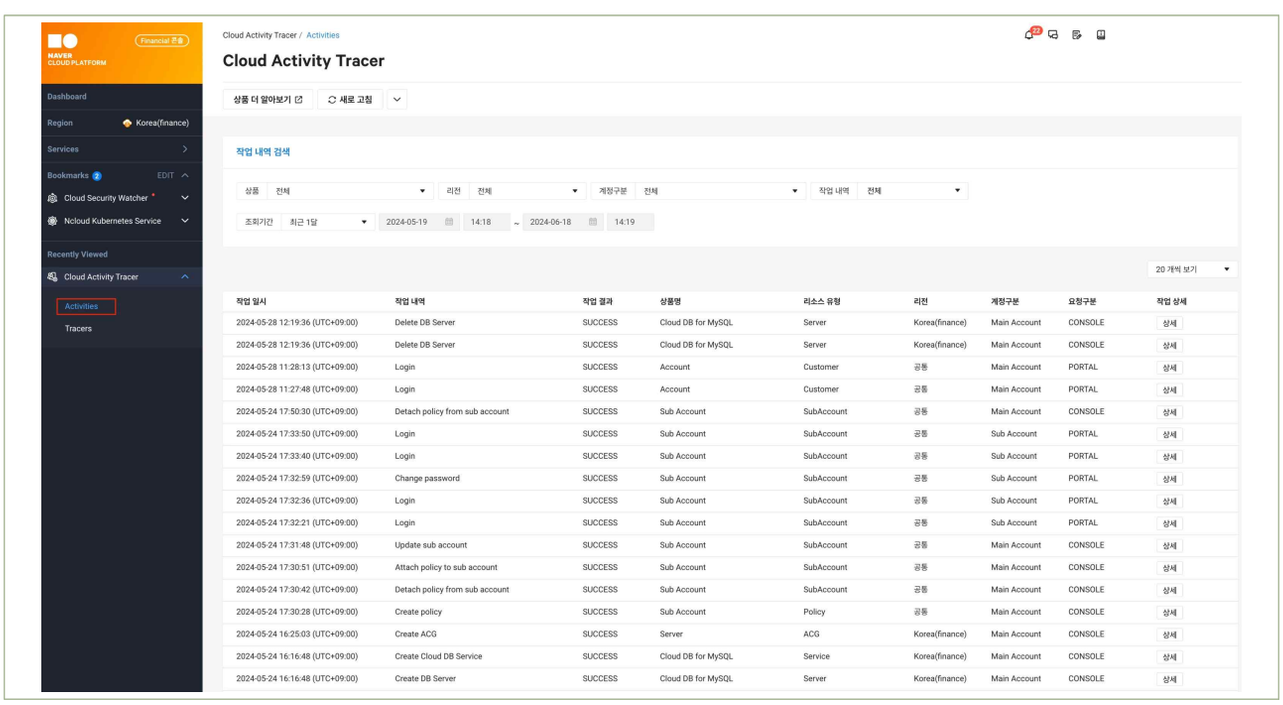
네트워크 변경 이력 확인

① **(가상자원관리시스템)** ‘Services’ → ‘Cloud Activity Tracer’ 상품을 선택합니다.



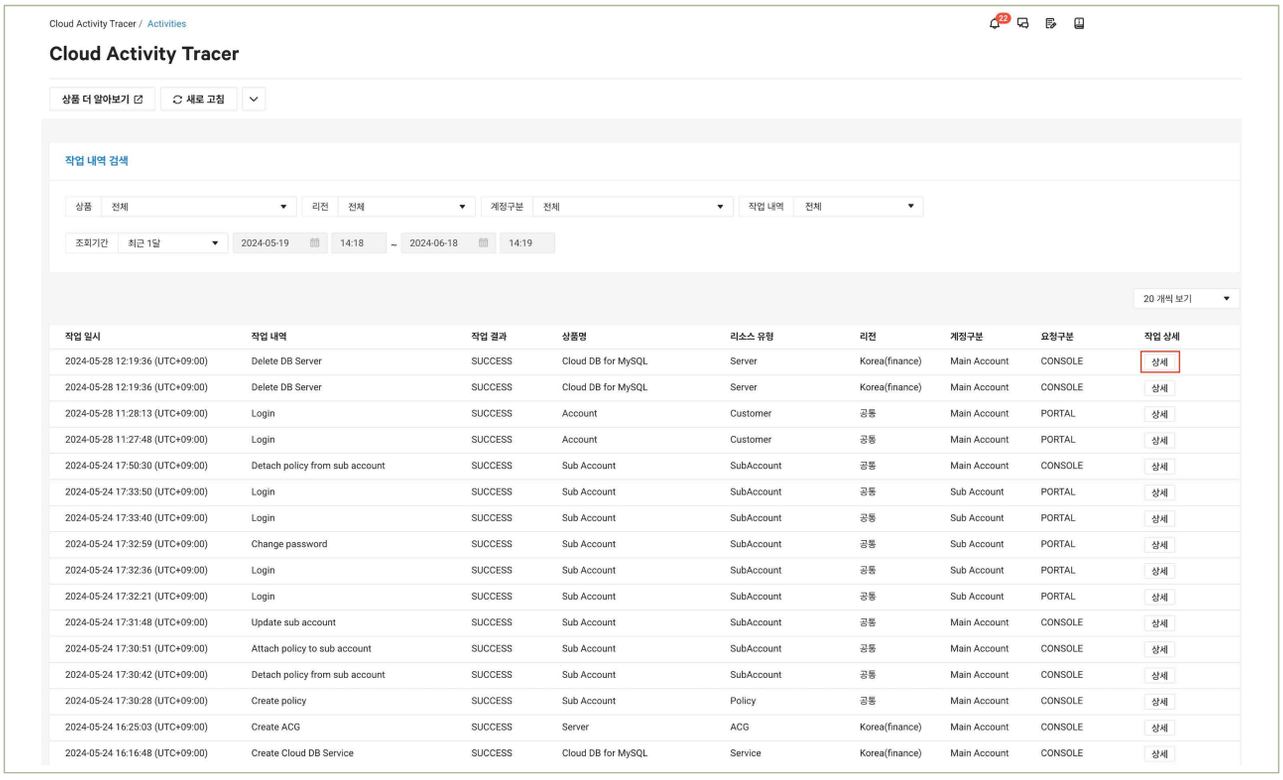
| 그림 5-5-1 | Cloud Activity Tracer 상품 선택

② **(가상자원관리시스템)** ‘Activities’를 통해 보존된 메인 계정, 서브 계정의 계정 활동 이력 목록을 확인합니다.



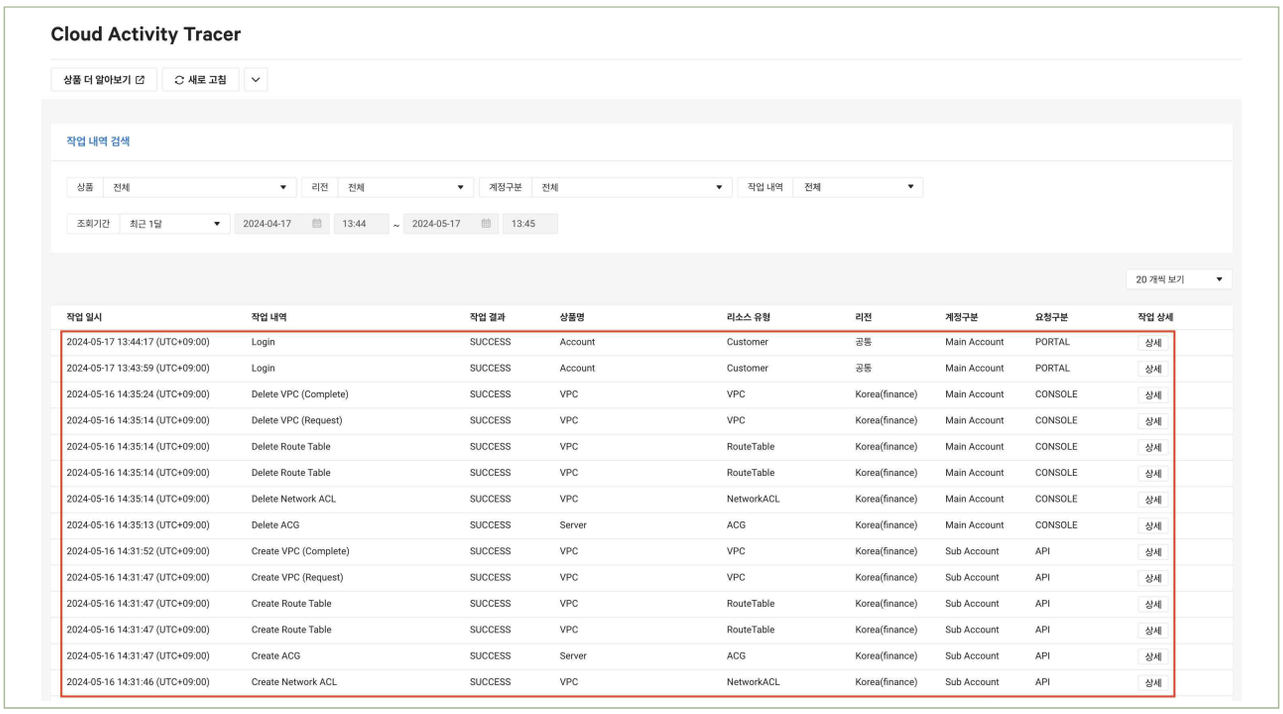
| 그림 5-5-2 | 계정 활동 이력 예시

③ **(가상자원관리시스템)** 계정 활동 이력에 대한 세부내용을 확인을 위해 '상세' 버튼을 클릭합니다.



| 그림 5-5-3 | 계정 활동 이력 예시

④ **(가상자원관리시스템)** 네트워크 변경 이력의 상세 확인을 위해 '상세'버튼을 클릭합니다.



| 그림 5-5-4 | Cloud Activity Tracer를 통한 네트워크 변경 이력 확인 예시

API를 통한 네트워크 변경 이력 확인

① **(API(CLI))** ‘activities’ API를 통해 네트워크 변경 이력을 확인합니다.

- 요청 예시

```
POST https://cloudactivitytracer.apigw.fin-ntruss.com/api/v1/activities
```

- 요청 예시 (Body)

```
{
  "fromEventTime": "integer",
  "toEventTime": "integer",
  "nrn": "string",
  "pageIndex": "integer",
  "pageSize": "integer"
}
```

- 응답 예시 (성공)

```
{
    "historyId": "664b11f4e1fd0965ef436e8e",
    "nrn": "nrn:FIN:VPCServer:FKR:3******:ACG/4****",
    "eventTime": 1716195828526,
    "platformType": "VPC",
    "productName": "VPCServer",
    "productDisplayName": "Server",
    "regionCode": "FKR",
    "regionDisplayName": "Korea(finance)",
    "resourceType": "ACG",
    "resourceId": "4***8",
    "resourceName": "cloud-mysql-*****",
    "actionDisplayName": "Create ACG",
    "actionResultType": "SUCCESS",
    "actionUserType": "Customer",
    "sourceType": "API",
    "sourceIp": "10.***.***.*9",
    "productData": {
        "defaultYn": "N",
        "vpcName": "ncp-fin-vpc",
        "createdYmdt": "1716195828501",
        "accessControlGroupNo": "4****",
        "outboundRuleCount": "0",
        "accessControlGroupName": "cloud-mysql-*****",
        "memberNo": "3******",
        "modifiedYmdt": "1716195828501",
        "inboundRuleCount": "0",
        "vpcNo": "2****",
        "networkInterfaceCount": "0",
        "statusCode": "RUN"
    }
}
```

| 그림 5-5-5 | API를 통한 네트워크 변경 이력 확인 예시

4 참고 사항

- [참고1] 계정활동 이력 조회 가이드
- [참고2] Cloud Activity Tracer 이력 호출 API 사용 가이드

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.
  - 예시 (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

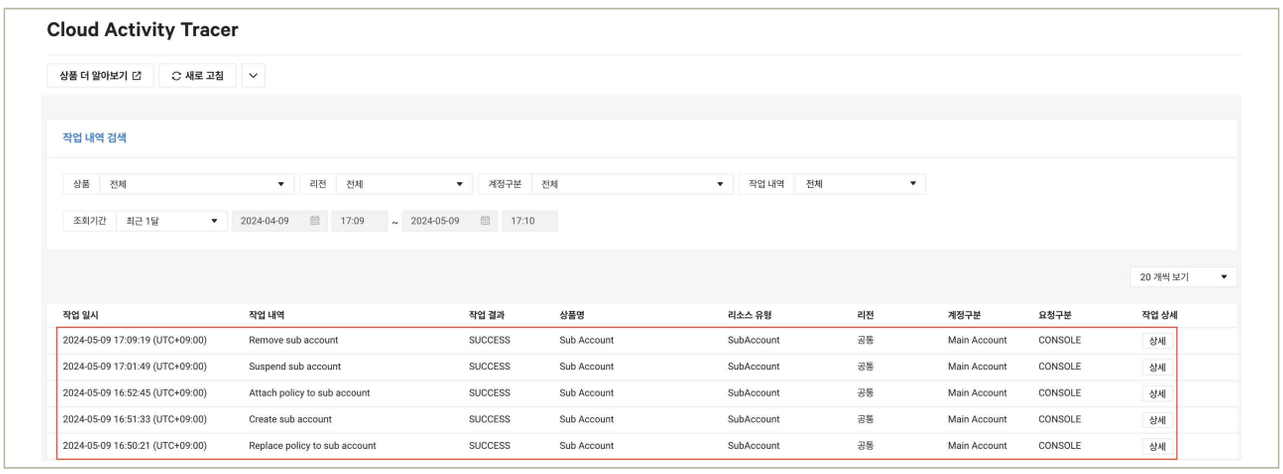
- 네이버 클라우드 플랫폼은 메인 계정과 서브 계정의 활동 로그를 수집하고 조회하는 Cloud Activity Tracer 상품을 통해 가상자원관리시스템(클라우드 콘솔) 및 API를 이용한 메인 계정 및 서브 계정의 변경 이력에 대하여 접근 시간, 접근ID, 작업 내용 등을 상세히 기록하고 1년간 안전하게 보존합니다. 사용자는 이를 통해 언제든지 가상자원관리시스템(클라우드 콘솔)에서 메인 계정과 서브 계정의 변경 기록을 간편하게 열람할 수 있으며, 전자금융감독규정 제13조(전산자료 보호대책) 등에 따라 계정 활동의 장기보존을 위해 Object Storage 상품을 연동하여 안전하게 보관할 수 있습니다.
  또한, 리소스 현황 식별, 자산 변경 감시 등 클라우드 보안 형상 관리를 수행하는 Cloud Security Watcher 보안 상품을 통해해서 가상자원(서버) 접속 계정의 변경에 대한 로그를 확보할 수 있습니다.

클라우드 계정 변경 내역 확인

① **(가상자원관리시스템)** ‘Services’ → ‘Cloud Activity Tracer’ 상품을 선택합니다.

| 그림 5-6-1 | Cloud Activity Tracer 상품 선택

② **(가상자원관리시스템)** ‘Activities’를 통해 클라우드 계정의 변경 이력을 확인합니다.



| 그림 5-6-2 | Cloud Activity Tracer를 통한 클라우드 계정 변경 이력 확인 예시

API를 통한 클라우드 계정 변경 이력 확인

① **(API(CLI))** 'activities' API를 통해 클라우드 계정 변경 이력을 확인합니다.

- 요청 예시

```
POST https://cloudactivitytracer.apigw.fin-ntruss.com/api/v1/activities
```

- 요청 예시 (Body)

```
{
  "fromEventTime": "integer",
  "toEventTime": "integer",
  "nrn": "string",
  "pageIndex": "integer",
  "pageSize": "integer"
}
```

- 응답 예시 (성공)

```
{
  "historyId": "662625720e28854c967b05ba",
  "nrn": "nrn:FIN:IAM::3******:SubAccount/69dcb760-f7c3-11ee-ab36-005056a79369",
  "eventTime": 1713775985981,
  "platformType": "BOTH",
  "productName": "IAM",
  "productDisplayName": "Sub Account",
  "regionCode": "",
  "regionDisplayName": "Global",
  "resourceType": "SubAccount",
  "resourceId": "69dcb760-f7c3-11ee-ab36-005056a79369",
  "resourceName": "ncpfinsubuser1",
  "actionDisplayName": "Attach policy to sub account",
  "actionResultType": "SUCCESS",
  "actionUserType": "Customer",
  "sourceType": "CONSOLE",
  "sourceIp": "10.***.***.*7",
  "productData": {
      "subAccountNo": "69dcb760-f7c3-11ee-ab36-005056a79369",
      "subAccountId": "ncpfinsubuser1",
      "name": "김그린",
      "loginUrl": "c******",
      "canConsoleAccess": "true",
      "canProgramAccess": "false",
      "useConsolePermitIp": "false",
      "needDgr2Auth": "true",
      "needPasswordReset": "true",
      "createTime": "1712812916000",
      "dgr2Yn": "N",
      "policies[0].policyNo": "9d1a94b0-0085-11ef-8682-246e96591a38",
      "policies[0].policyName": "ncp-fin-bucket-policy",
      "policies[0].type": "USER_CREATED",
      "policies[0].createTime": "1713775933000"
  }
}
```

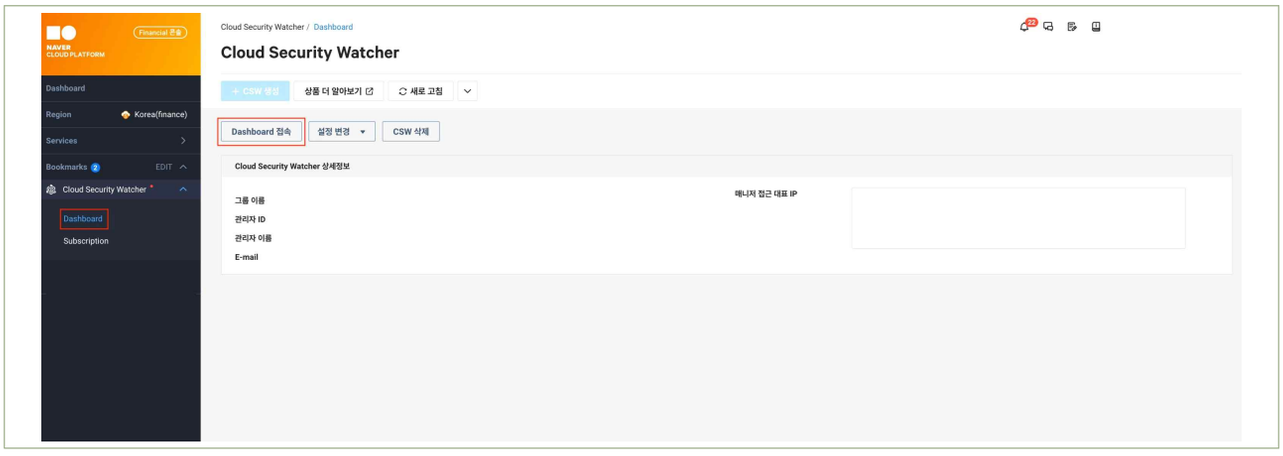
| 그림 5-6-3 | API를 통한 클라우드 계정 변경 이력 확인 예시

Cloud Security Watcher를 통한 가상자원 접속 계정 변경 이력 확인

① **(가상자원관리시스템)** ‘Services’ → ‘Cloud Security Watcher’ 상품을 선택합니다.

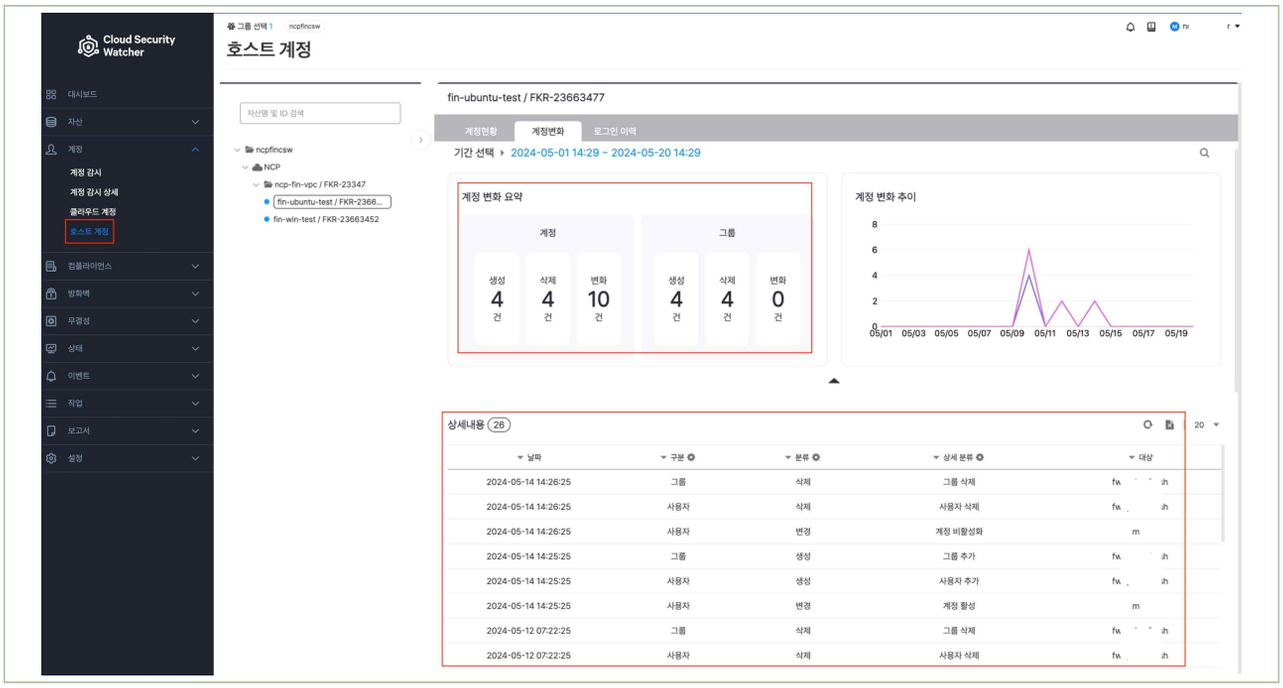
| 그림 5-6-4 | Cloud Security Watcher 상품 선택

② **(가상자원관리시스템)** ‘Dashboard’ → ‘Dashboard 접속’ 버튼을 클릭하여 Cloud Security Watcher 콘솔에 접속합니다.



| 그림 5-6-5 | Cloud Security Watcher 콘솔 접속

③ **(가상자원관리시스템)** '계정' → '호스트 계정'을 통해 클라우드 가상자원 접속 계정의 변경에 대한 이력을 확인합니다.



| 그림 5-6-6 | Cloud Security Watcher를 통한 가상자원 접속 계정 변경 이력 확인 예시

4 참고 사항

- [참고1] 계정활동 이력 조회 가이드
- [참고2] Cloud Security Watcher를 통한 가상자원 접속 계정 변경 이력 조회 가이드
- [참고3] Cloud Activity Tracer 이력 호출 API 사용 가이드

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

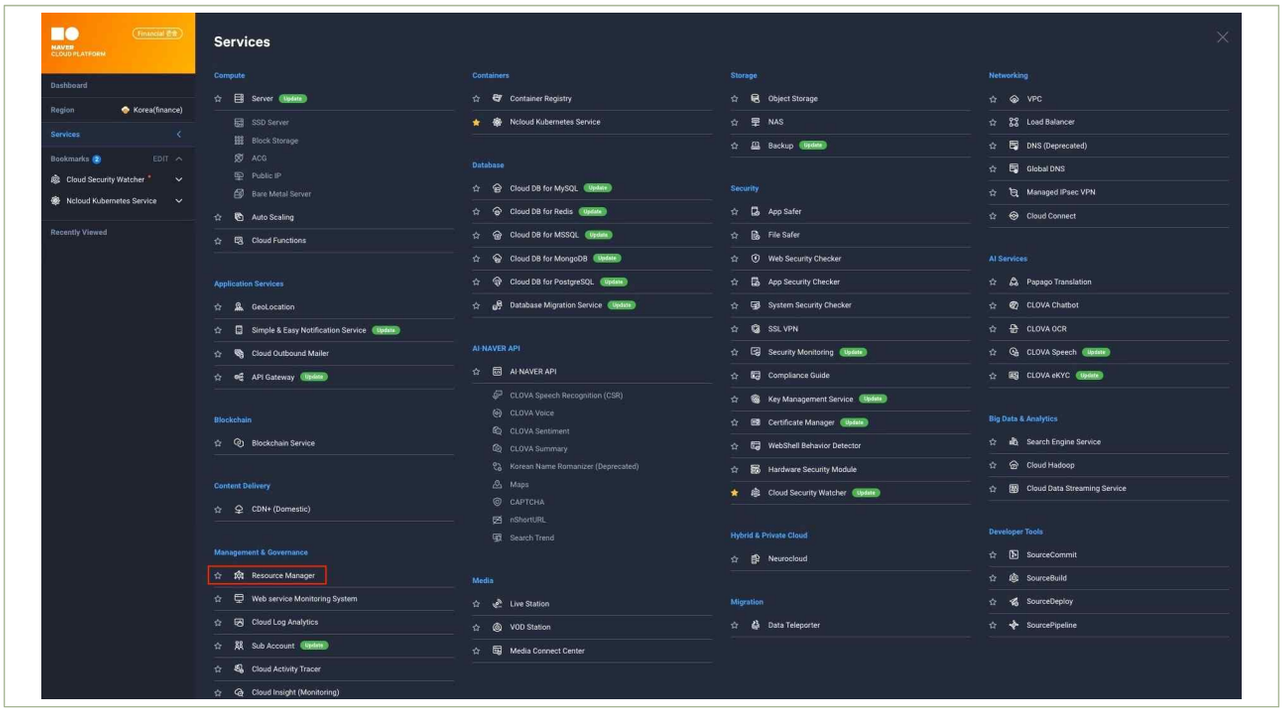
    1) 계정 변경사항에 관한 상시 모니터링 수행
    2) 전자금융감독규정 및 금융회사 내부규정등에 수립된 주기에 맞추어 주기적 검토 수행
    3) 관리자 계정에 대해서는 이중확인 수행 등

3 우수 사례

- 네이버 클라우드 플랫폼은 가상자원을 통합적으로 관리할 수 있는 Resource Manager의 Observer 기능을 통해 클라우드 계정 변경 등의 계정 상태를 감시하여 SMS 또는 E-mail 알람을 받을 수 있도록 구성할 수 있습니다.
  또한, 리소스 현황 식별, 자산 변경 감시 등 클라우드 보안 형상 관리를 수행하는 Cloud Security Watcher 보안 상품을 활용하여 클라우드 계정의 상태 변경에 대한 모니터링과 알림 조건을 더욱 상세히 설정할 수 있습니다.

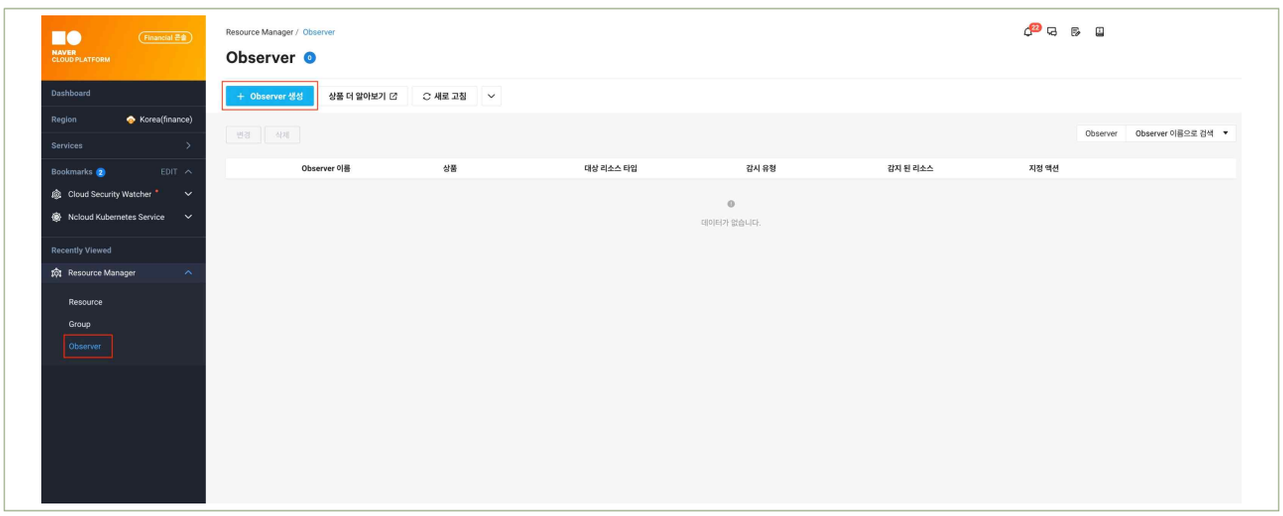
클라우드 계정 변경사항 모니터링

① **(가상자원관리시스템)** ‘Services’ → ‘Resource Manager’ 상품을 선택합니다.



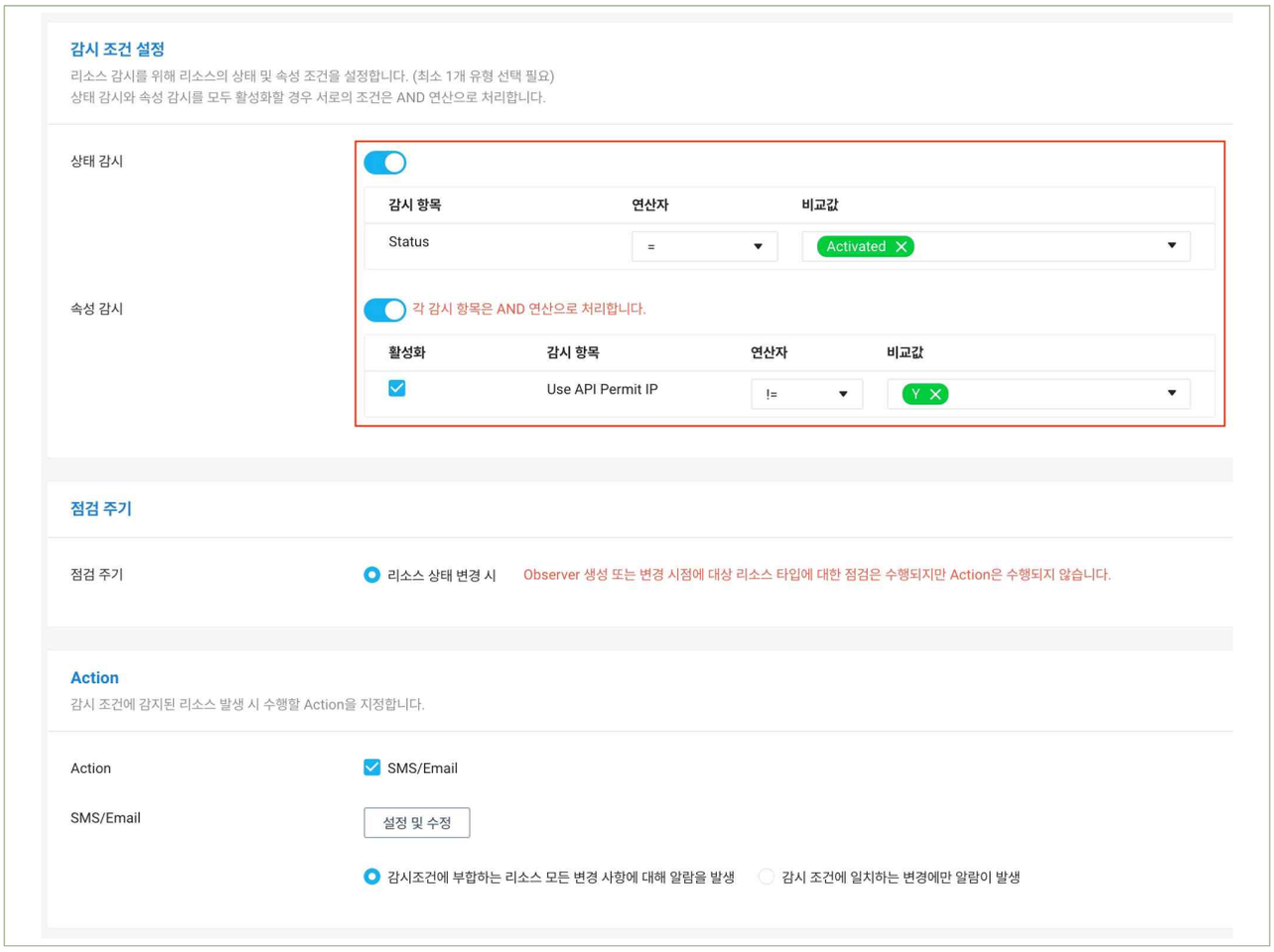
| 그림 5-7-1 | Resource Manager 상품 선택

② **(가상자원관리시스템)** ‘Observer’ → ‘+ Observer 생성’을 클릭합니다.



| 그림 5-7-2 | Observer 생성

③ **(가상자원관리시스템)** 클라우드 계정의 변경 이력을 감시 조건을 설정하여 상시 모니터링을 수행합니다.



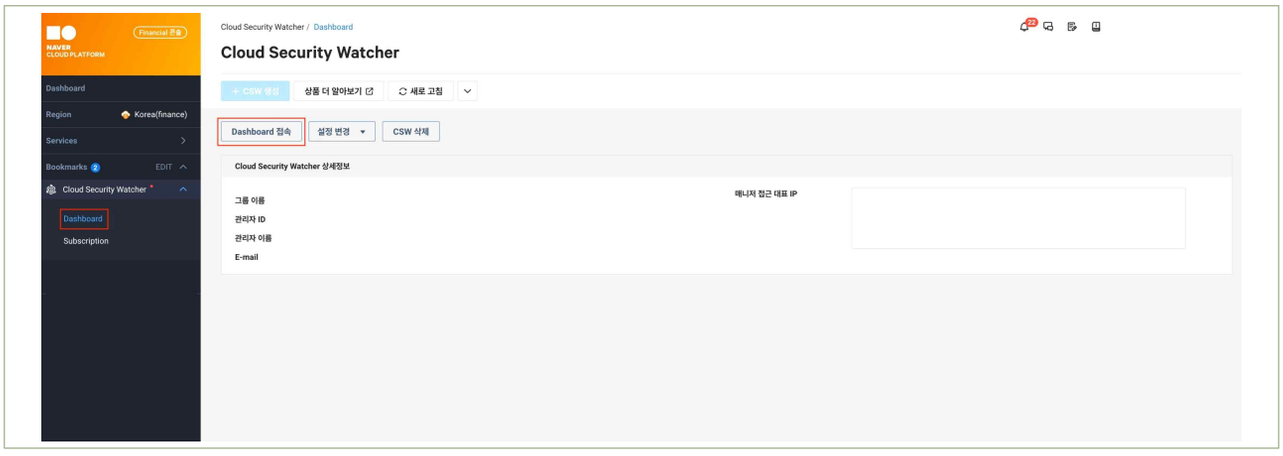
| 그림 5-7-3 | Resource Manager를 통한 클라우드 계정 모니터링 설정 예시

Cloud Security Watcher를 통한 클라우드 계정 변경사항 모니터링

① **(가상자원관리시스템)** ‘Services’ → ‘Cloud Security Watcher’ 상품을 선택합니다.

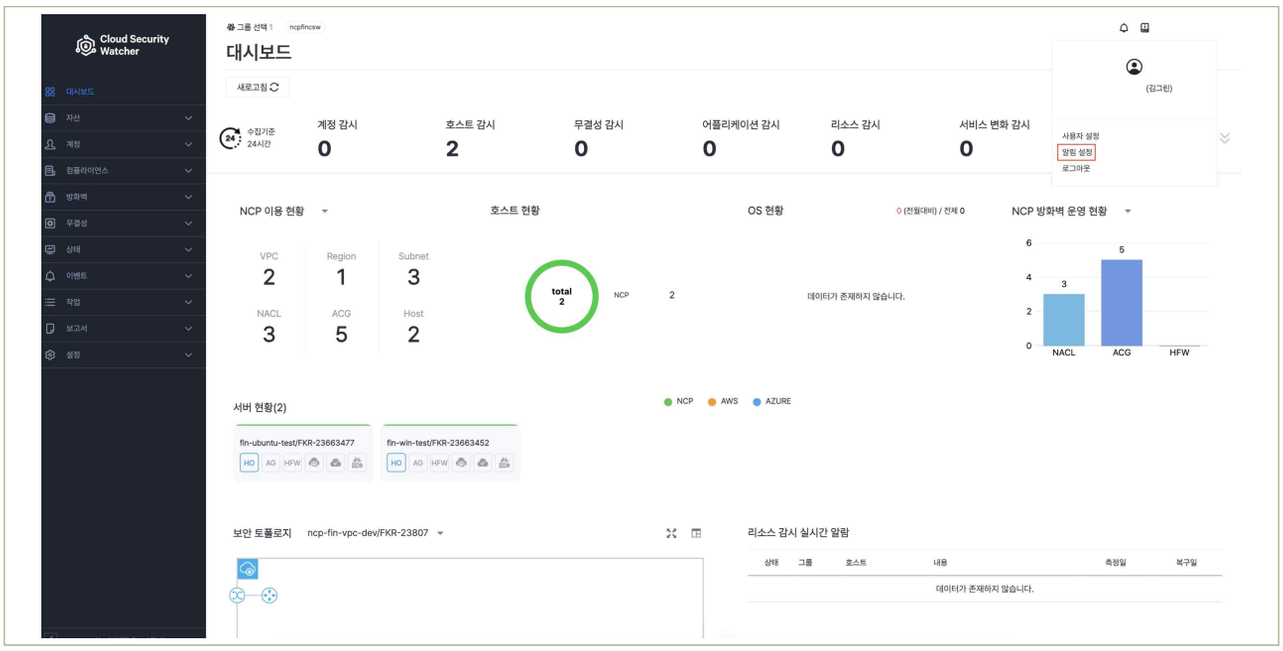
| 그림 5-7-4 | Cloud Security Watcher 상품 선택

② **(가상자원관리시스템)** ‘Dashboard’ → ‘Dashboard 접속’ 버튼을 클릭하여 Cloud Security Watcher 콘솔에 접속합니다.



| 그림 5-7-5 | Cloud Security Watcher 콘솔 접속

③ **(가상자원관리시스템)** '우측 상단 계정 아이콘 선택' → '알림 설정'을 클릭합니다.

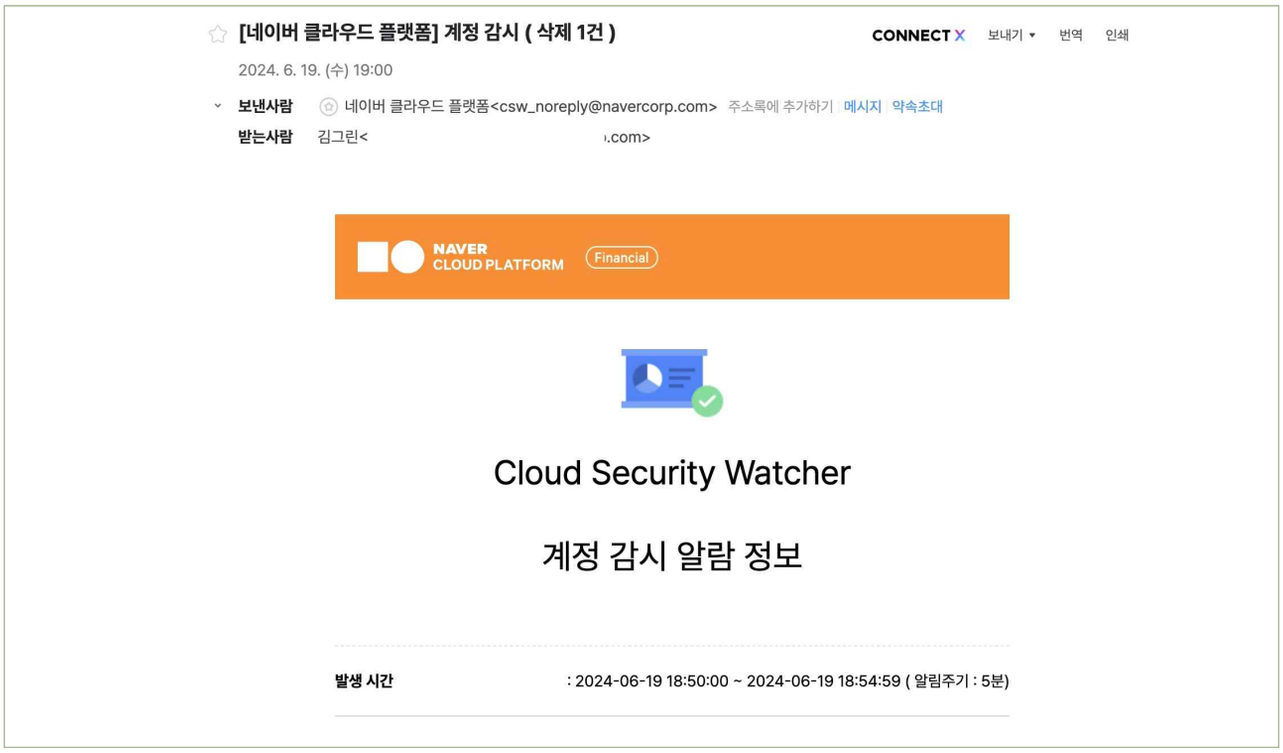


| 그림 5-7-6 | Cloud Security Watcher를 통한 클라우드 계정 모니터링 설정 예시

④ **(가상자원관리시스템)** 클라우드 계정 변경에 대한 상태감시 조건을 설정합니다.

| 그림 5-7-7 | Cloud Security Watcher를 통한 클라우드 계정 모니터링 설정 예시

⑤ **(가상자원관리시스템)** 클라우드 계정 상태감시 조건에 해당하는 이벤트가 발생될 경우 알림 메일이 발송됩니다.



| 그림 5-7-8 | 클라우드 계정 상태감시 알림 예시

4 참고 사항

- [참고1] Resource Manager 사용 가이드
- [참고2] Cloud Security Watcher 알림 설정 가이드

6. API 관리

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

6 API 관리

1 기준

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

2 설명

- API 호출 시 이용자를 인증할 수 있는 수단을 적용하여야 한다.

  - 예시

    1) API 호출이 가능한 IP 지정

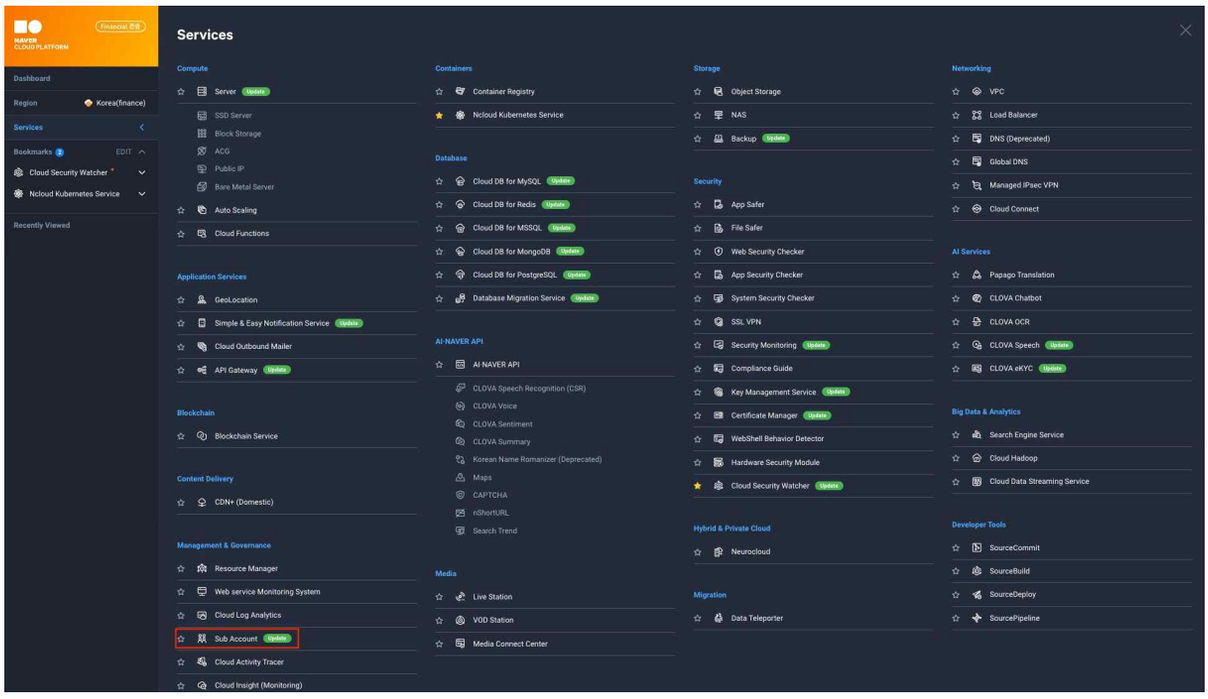
    2) IAM 기능과 연동하여 API를 호출할 수 있는 권한 제어 등

3 우수 사례

- 네이버 클라우드 플랫폼은 API 호출 시, 안전한 인증을 위해 단기적으로 사용 가능한 Signature를 이용하여 요청합니다. 또한, Sub Account를 통해 출발지 IP를 기준으로 가상자원 관리를 위한 API 접근과 Sub User별 접근 가능한 상품을 다음과 같이 제한할 수 있습니다.

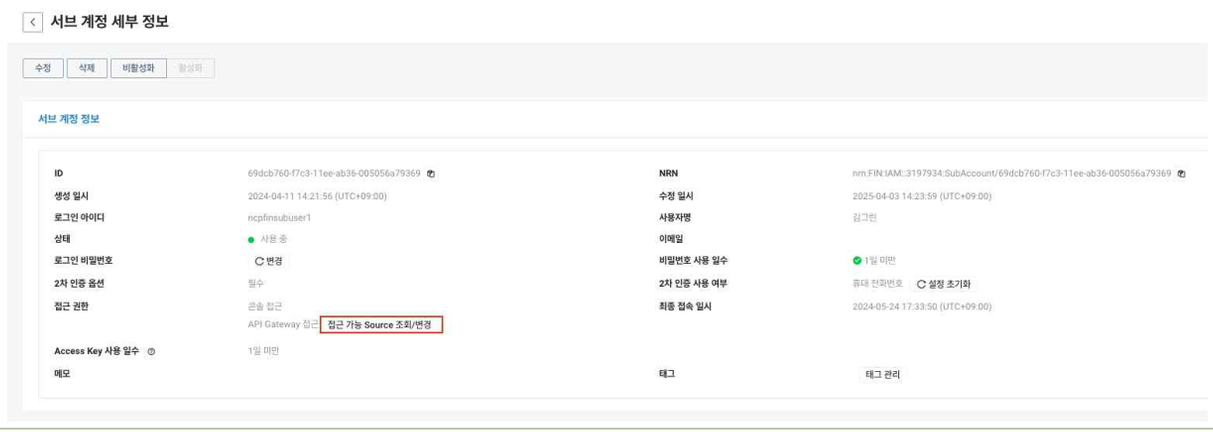
API 호출이 가능한 IP 제한

① **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ 상품을 선택합니다.



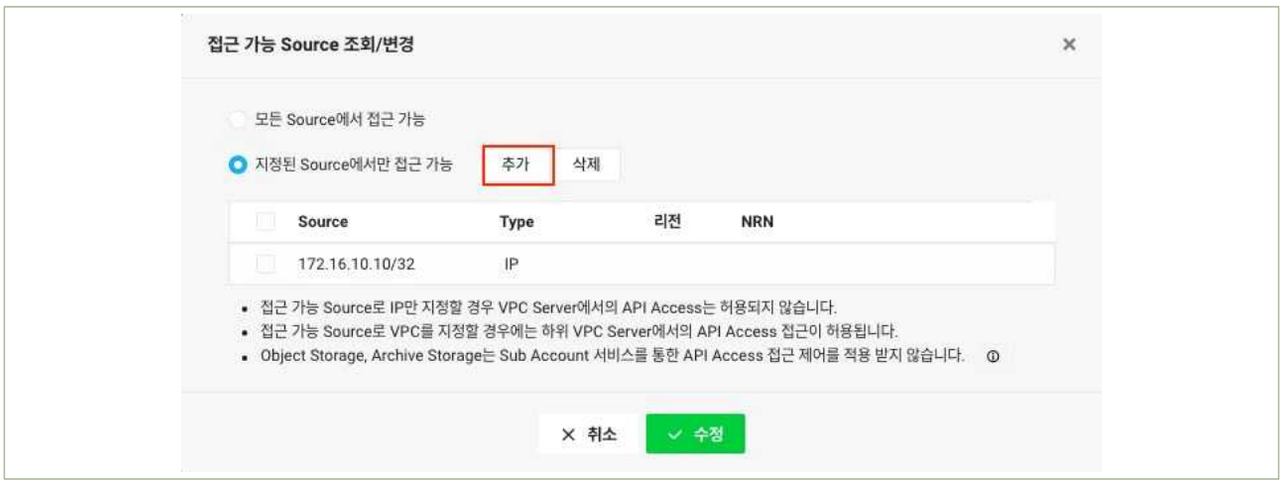
| 그림 6-1-1 | Sub Account 상품 선택

② **(가상자원관리시스템)** ‘Sub Accounts’ → ‘Sub User 선택’ → ‘접근 가능 Source 조회/변경’을 선택합니다.‘



| 그림 6-1-2 | 접근 가능 Source 조회/변경 선택

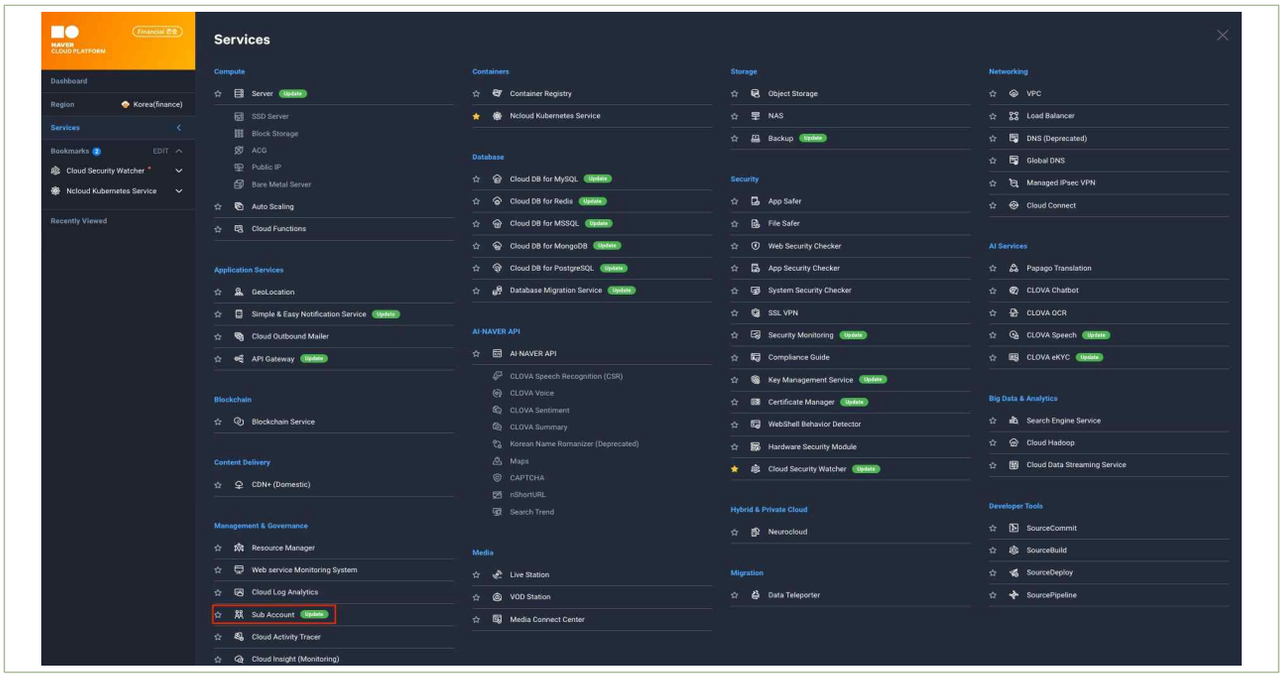
③ **(가상자원관리시스템)** '지정된 Source에서만 접근 가능' → '추가'를 선택하고 지정된 Source IP에서만 접근 가능하도록 IP 대역을 추가합니다.



| 그림 6-1-3 | API Gateway 접근에 대한 Source IP 대역 제한

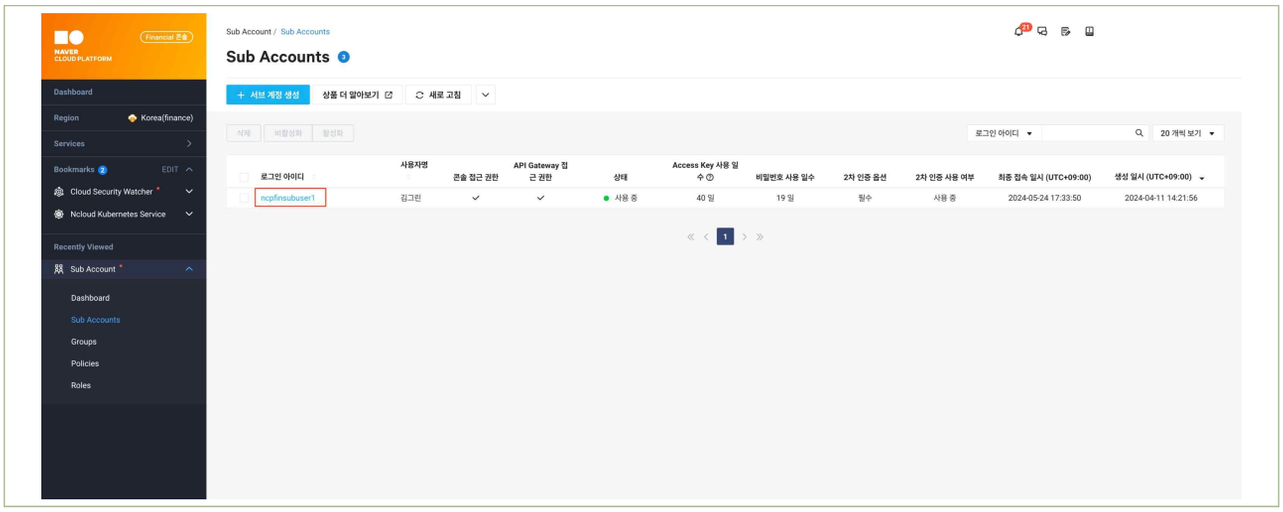
○ 서브계정 별 API 호출 가능 권한 제어

① **(가상자원관리시스템)** 'Services' → 'Sub Account' 상품을 선택합니다.



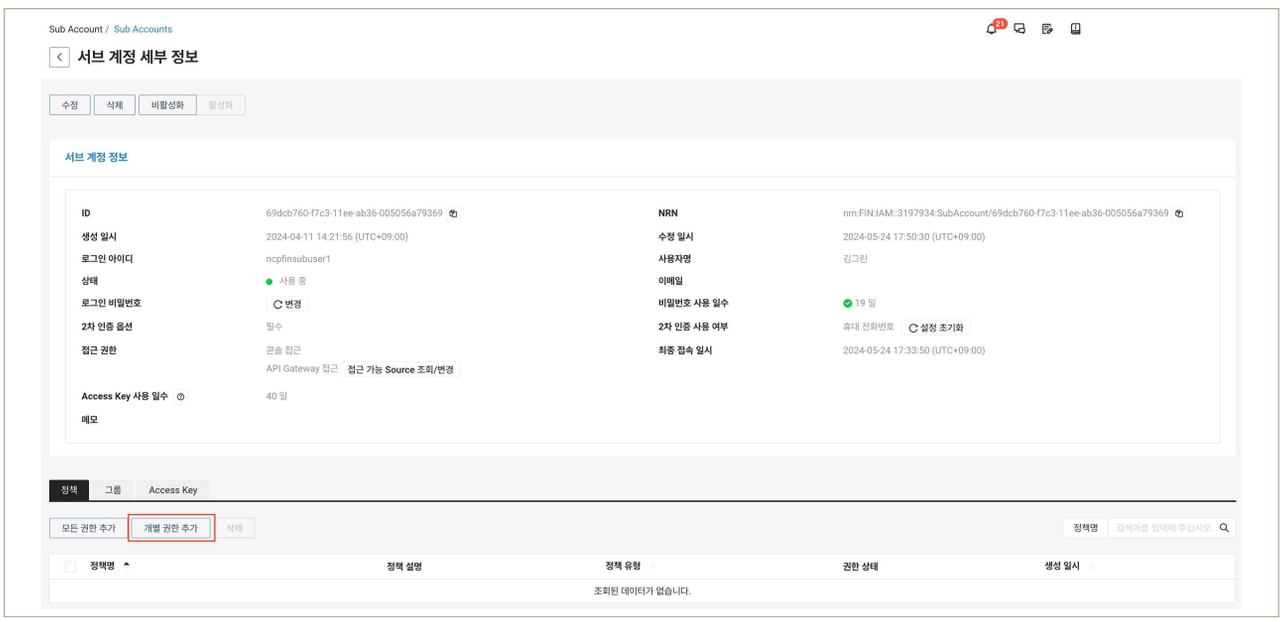
| 그림 6-1-4 | Sub Account 상품 선택

② **(가상자원관리시스템)** 서브계정에 대한 권한 설정을 위해 서브계정(로그인 아이디)를 클릭합니다.



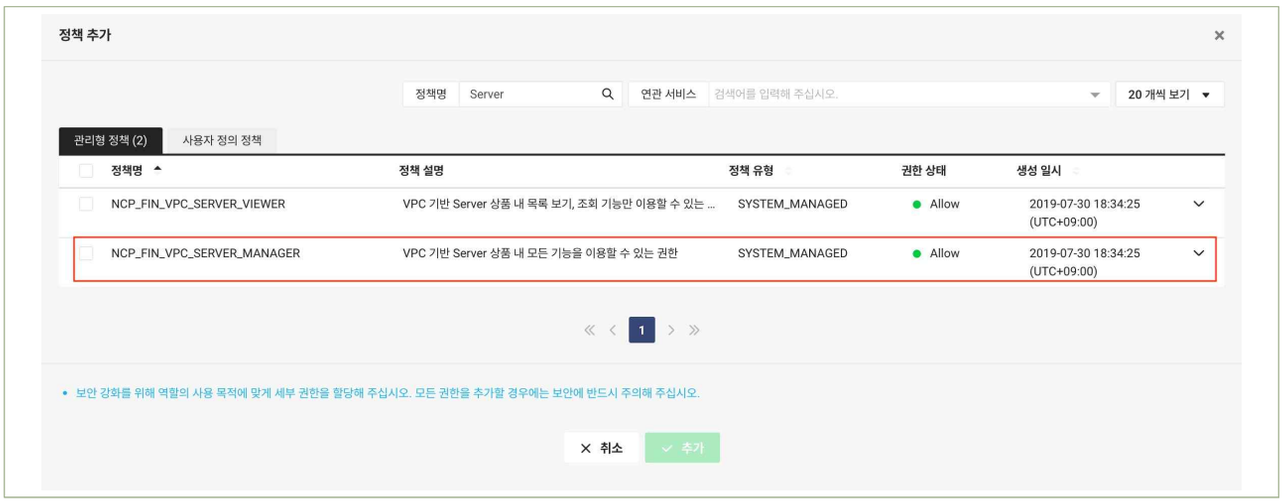
| 그림 6-1-5 | 권한설정을 위한 서브계정 선택

③ **(가상자원관리시스템)** '정책'탭의 '개별 권한 추가' 또는 '그룹' 탭의 '추가'를 통해 API Gateway 접근이 가능한 Sub User에 대하여 특정 상품에 대한 접근을 제한합니다.



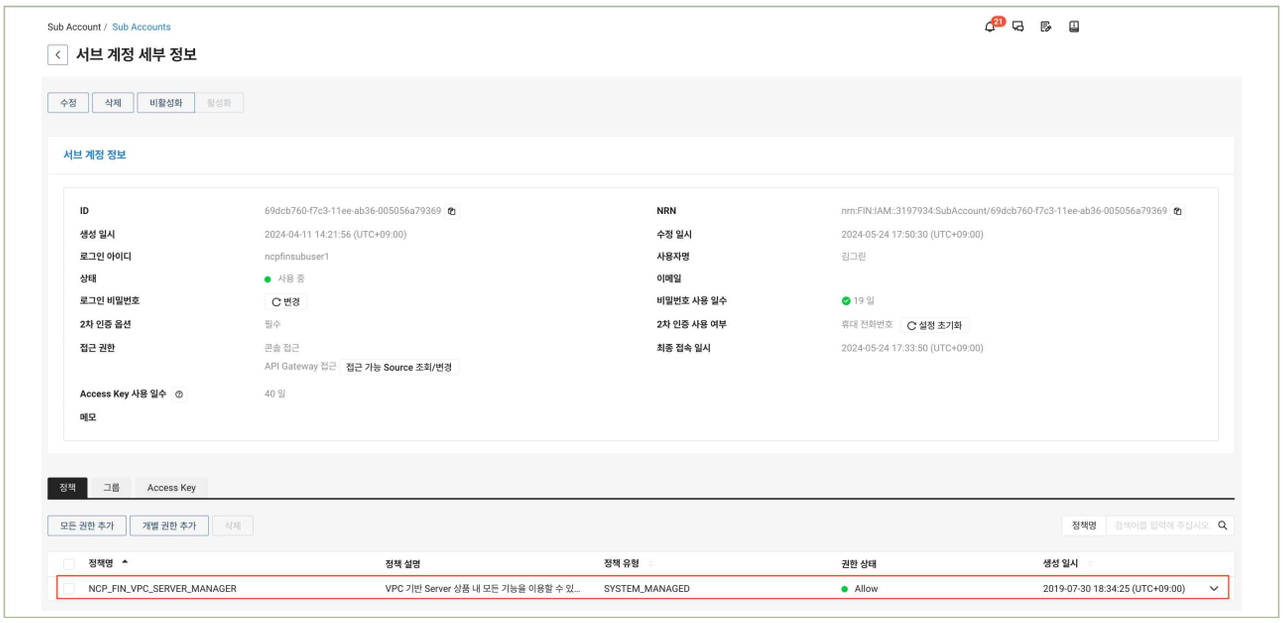
| 그림 6-1-6 | 서브계정의 권한 설정

④ **(가상자원관리시스템)** '관리형 정책'탭에서 서브 계정 별 필요한 NCP 상품 권한을 추가 합니다.



| 그림 6-1-7 | 서브계정에 대한 Server 상품 관리 권한 설정 예시

⑤ **(가상자원관리시스템)** 서브계정에 할당된 NCP 관리형 정책을 확인합니다.



| 그림 6-1-8 | 서브계정 별 권한 부여 완료 예시

※ NCP에 정의된 권한(SYSTEM_MANAGED) 외 사용자 정의 정책을 생성하여 권한을 부여할 수 있으며, 사용자 정의 정책을 사용하는 경우 상품 별 가상자원 대상 및 액션 권한 수준까지 세부적으로 권한 관리를 적용할 수 있습니다.

API 호출이 가능한 IP 제한

① **(API(CLI))** 'sub-accounts' API를 통해 서브계정의 API 접근 규칙을 수정합니다.

- 요청 예시

```
POST https://subaccount.apigw.fin-ntruss.com/api/v1/sub-accounts/{subAccountId}/access-rules/api
```

- 요청 예시 (Body)

```
curl --location --request PUT
'https://subaccount.apigw.fin-ntruss.com/api/v1/sub-accounts/2b141960-****-****-****-246e9659184c/acces
s-rules/api' \
--header 'x-ncp-apigw-timestamp: {Timestamp}' \
--header 'x-ncp-iam-access-key: {Access Key}' \
--header 'x-ncp-apigw-signature-v2: {API Gateway Signature}' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--data '{
    "useApiAllowSource": true,
    "apiAllowSources": [
        {
            "type": "IP",
            "source": "**.**.**.**"
        }
    ]
}'
```

- 응답 예시 (성공)

```
{
    "success": true,
    "id": "2b141960-****-****-****-246e9659184c"
}
```

| 그림 6-1-9 | API를 통한 서브 계정의 API 접근 규칙 예시

4 참고 사항

- [참고1]서브계정의 접근 제한 설정
- [참고2]서브계저의 정책 및 역할 관리
- [참고3]API를 통한 API 접근 규칙 수정

1 기준

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

2 설명

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

  - 예시

    1) API 보안 키와 서명을 통한 변조방지 대책 마련 등

3 우수 사례

- 네이버 클라우드 플랫폼은 API 호출 시, 무결성 보장을 위해 HMAC-SHA256 (Hash-based Authentication Code)를 사용하여 Signature를 생성합니다. 네이버 클라우드 플랫폼의 API는 반드시 Sub User의 개인 Secret Key를 이용해 요청정보에 대한 Signature를 생성하여 API 호출을 수행하여야 하며, 네이버 클라우드 플랫폼의 API서버는 해당 Signature를 통해 Sub User의 요청에 대한 변조 여부의 확인 및 검증 후 응답을 수행합니다.

- **Signature를 통한 API 인증**

- 요청 예시

```
curl -i -X GET \
    -H "x-ncp-apigw-timestamp:1505290625682" \
    -H "x-ncp-iam-access-key:D78BB444D6D3C84CA38D" \
    -H "x-ncp-apigw-signature-v2:WTPItrmMIfLUk/UyUIyoQbA/z5hq9o3G8eQMoIUzTEa=" \
 'https://example.apigw.fin-ntruss.com/photos/puppy.jpg?query1=&query2'
```

| 그림 6-2-1 | Signature를 통한 인증 파라미터

4 참고 사항

- [참고1] 네이버 클라우드 플랫폼의 API 인증키

1 기준

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

2 설명

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

  - 예시

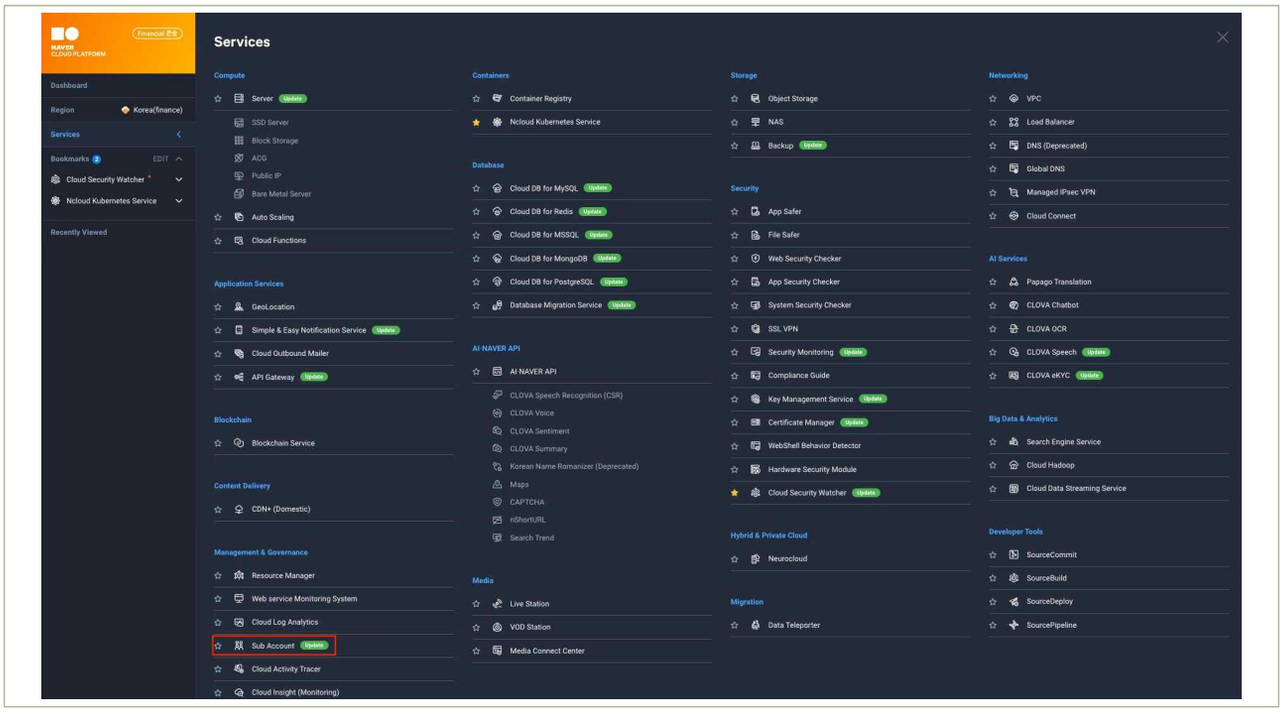
    1) API 호출을 서명하는데 사용되는 비밀키, 인증서 등은 노출되지 않도록 관리하여야 한다.

3 우수 사례

- 네이버 클라우드 플랫폼은 API 호출 시, 안전한 인증 및 무결성 검증을 위해 Sub User의 Access Key와 Secret Key가 필요하며, Sub User의 Secret Key는 고객의 편의를 위해 재확인이 가능하도록 되어있습니다. 클라우드 환경에서 중요한 Access Key와 Secret Key에 대한 접근을 제한하기 위하여 Sub Account의 모든 권한을 제한하거나, Sub Account의 사용자 정의 정책을 통해 Secret Key에 대한 조회권한을 최소한의 인원으로 제한하여 관리하여야 합니다.

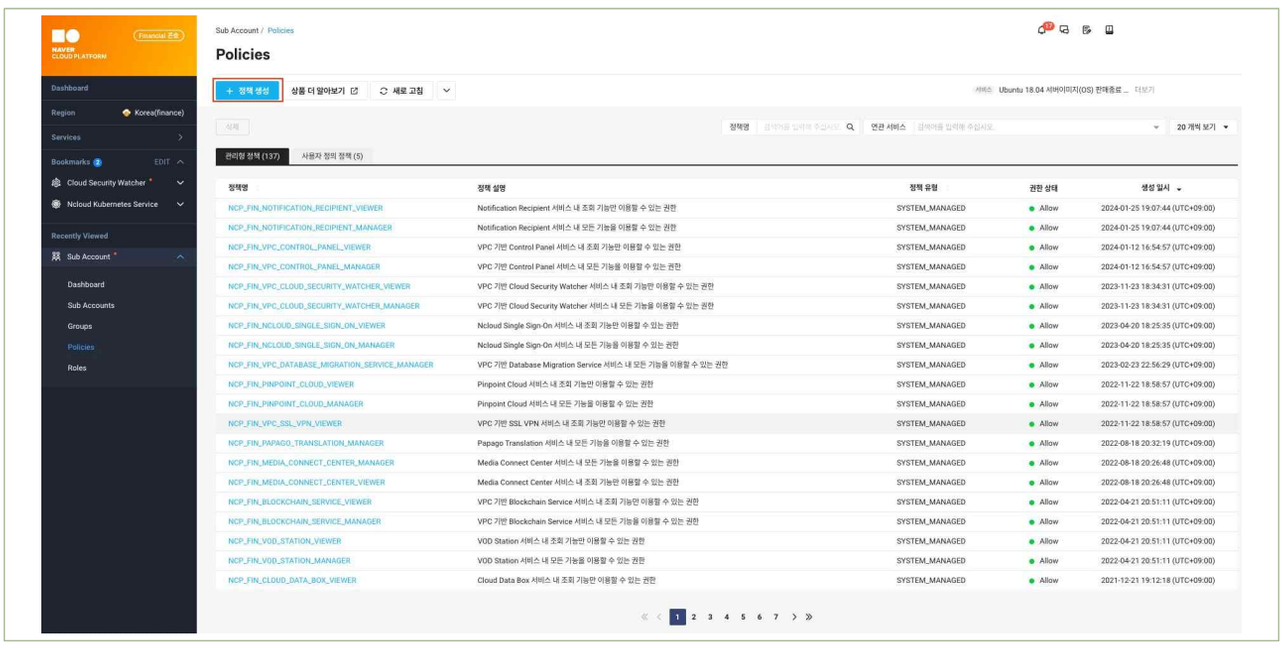
Access Key 조회권한 제한

① **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ 상품을 선택합니다.



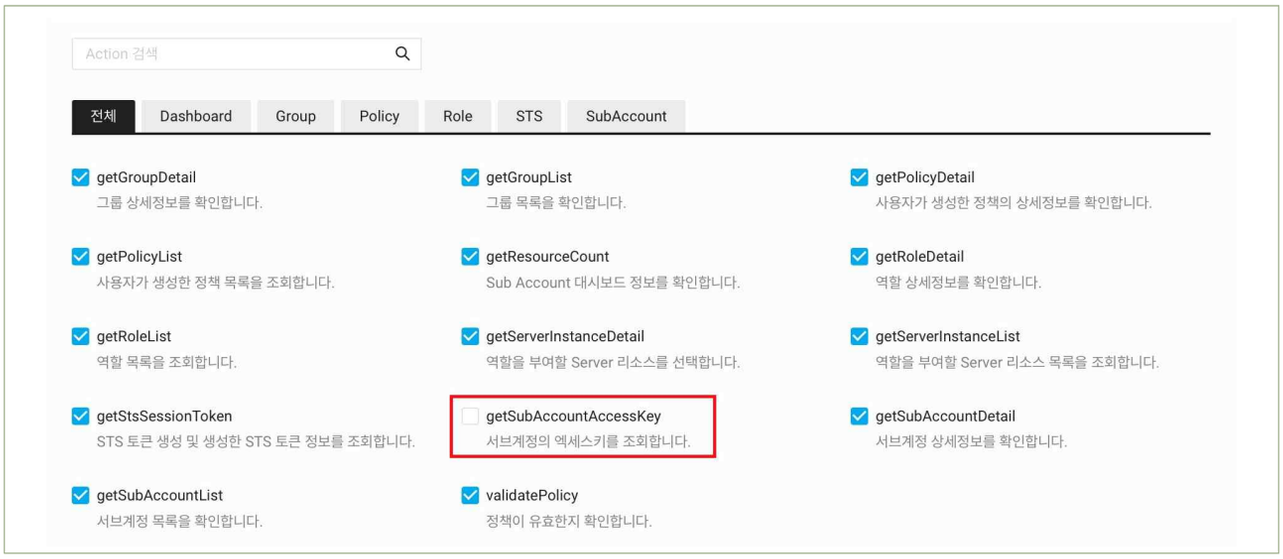
| 그림 6-3-1 | Sub Account 상품 선택

② **(가상자원관리시스템)** 사용자 정의 정책 생성을 위해 ‘Policies’ → ‘+ 정책 생성’버튼을 클릭합니다.



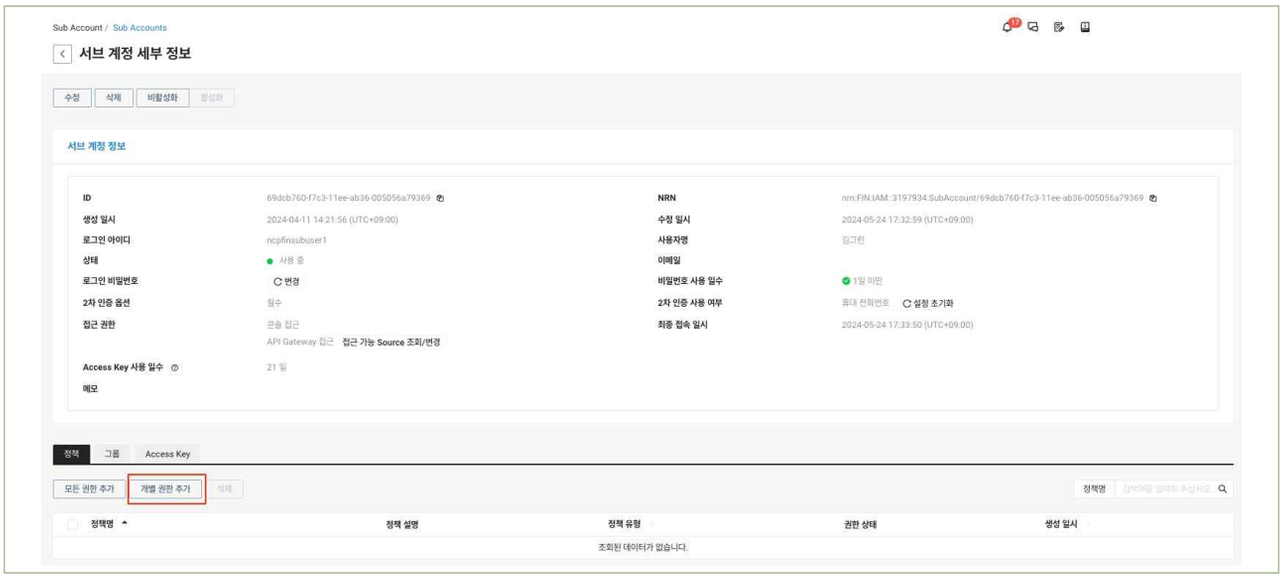
| 그림 6-3-2 | 사용자 정의 정책 생성

③ **(가상자원관리시스템)** Sub Account의 'getSubAccountAccessKey' Action을 제한하는 새로운 사용자 정의 정책을 생성합니다.



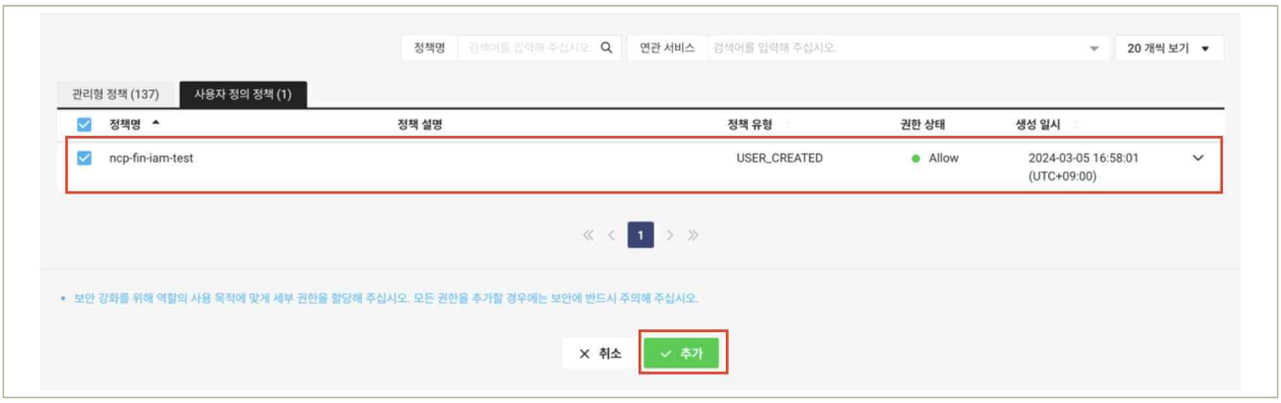
| 그림 6-3-3 | Sub Account의 사용자 정의 정책 정의

④ **(가상자원관리시스템)** 'Services' → 'Sub Account' → 'Sub Accounts'에서 사용자 정의 정책을 부여할 서브 계정을 선택하고, '개별 권한 추가'를 클릭합니다.



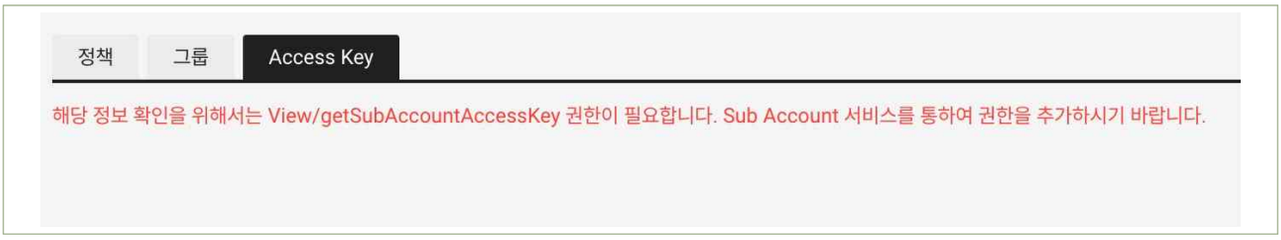
| 그림 6-3-4 | 서브 계정 별 개별 권한 추가

⑤ **(가상자원관리시스템)** 정책 추가 단계에서 사전에 정의한 '사용자 정의 정책'을 서브 계정에게 연결합니다.



| 그림 6-3-5 | 사용자 정의 정책 부여 예시

⑥ **(가상자원관리시스템)** '사용자 정의 정책'이 연결된 서브 계정으로 로그인하여 Access Key 조회가 차단되는지 확인합니다.



| 그림 6-3-6 | getSubAccountAccessKey 조회권한 제한에 대한 차단 예시

4 참고 사항

- [참고1] 사용자 정의 정책 생성 가이드

1 기준

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

2 설명

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

  - 예시

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

3 우수 사례

- 네이버 클라우드 플랫폼에서 API 요청 시, 서명(Signature)에 대한 유효시간은 5분 입니다. API 요청 내에는 timestamp 값을 포함하며, 서버는 요청에 대한 timestamp 값을 서버의 시간과 비교하여 5분 이상 차이가 나는 경우 유효하지 않은 요청으로 간주합니다.

- **유효하지 않은 timestamp에 대한 차단**

```
{"error":{"errorCode":"200","message":"Authentication Failed","details":"Expired timestamp."}}
```

| 그림 6-4-1 | 유효하지 않은 timestamp 값에 대한 차단 예시

4 참고 사항

- [참고1] 네이버 클라우드 플랫폼의 API 인증키

1 기준

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

2 설명

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

  - 예시

    1) SSL 적용 등

3 우수 사례

- 네이버 클라우드 플랫폼의 API는 TLS 1.3버전 프로토콜을 이용하여 HTTPS 프로토콜을 통해 통신구간을 암호화하여 사용자와 서버간 API 통신을 수행하며, TLS 1.3 버전을 이용하고 있습니다.

- **API의 TLS버전**

| 그림 6-5-1 | 네이버 클라우드 플랫폼 API의 TLS 버전 예시

4 참고 사항

- [참고1] 네이버 클라우드 플랫폼의 API 인증키

7. 스토리지 관리

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

7 스토리지 관리

1 기준

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

2 설명

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

  - 예시

    1) 외부에 공개가 필요없는 스토리지에 대해서는 퍼블릭 엑세스 차단 등 방안 적용

    2) 스토리지 종류별 접근 가능한 계정 관리 수행(IAM 기능 등을 활용)

    3) 단축 URL등 서명값이 포함된 URL로 접근 시 통제방안 수립(접근가능 시간, IP 제어 등) 등

3 우수 사례

- 네이버 클라우드 플랫폼의 Object Storage는 사용자가 언제 어디서나 원하는 데이터를 저장하고 탐색할 수 있도록 파일 저장 공간을 제공하는 상품입니다. Object Storage의 버킷에는 다양한 종류의 파일이 저장될 수 있으며, 경우에 따라 개인정보와 같은 민감한 정보가 저장될 수도 있습니다. 따라서, 고객은 네이버 클라우드 플랫폼의 Object Storage의 권한 관리와 Sub Account의 사용자 정의 정책을 통해 버킷의 용도에 따라 외부로부터의 접근 및 서브 계정 별 접근권한을 관리하여야 합니다.

버킷의 퍼블릭 엑세스 차단

① **(가상자원관리시스템)** ‘Services’ → ‘Object Storage’ 상품을 선택합니다.

| 그림 7-1-1 | Object Storage 상품 선택

② **(가상자원관리시스템)** ‘대상 버킷 … 클릭’ → ‘권한 관리’를 선택합니다.

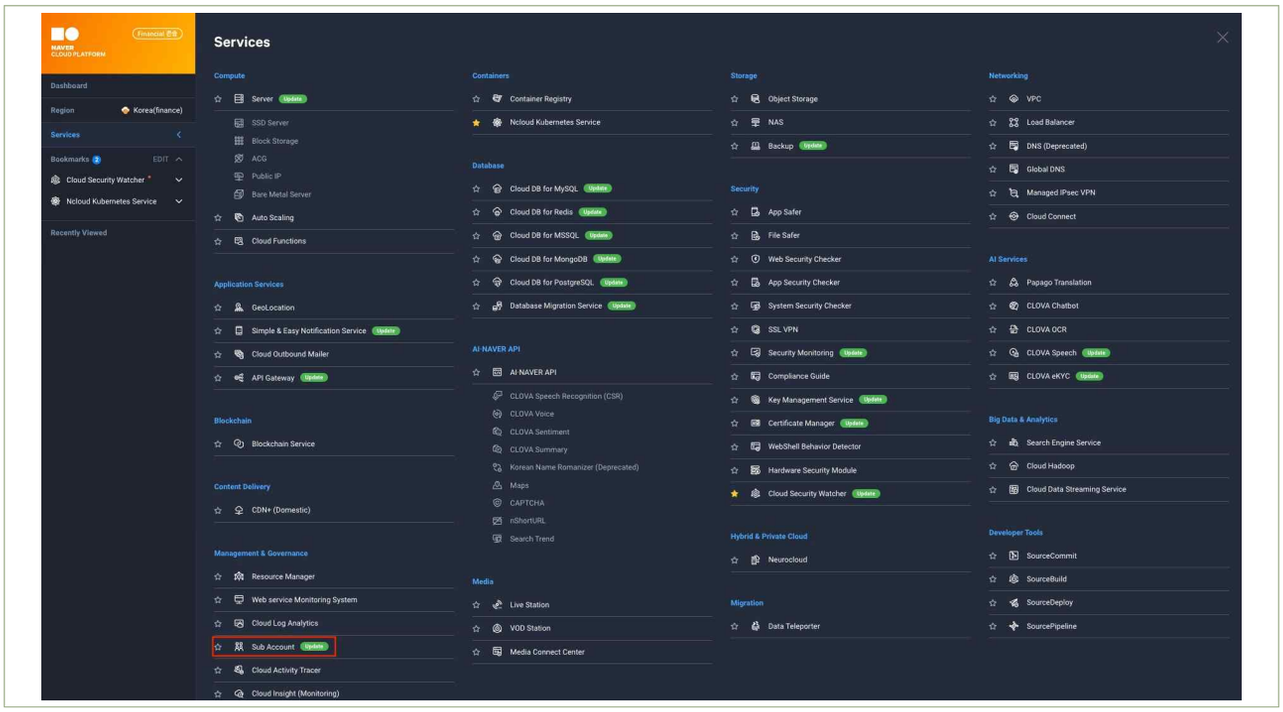
| 그림 7-1-2 | Object Storage 상품 선택

③ **(가상자원관리시스템)** 버킷의 전체 공개를 비활성화 하여, 버킷 내의 중요정보가 대외에 공개되지 않도록 설정합니다.

| 그림 7-1-3 | 버킷 비공개 적용 예시

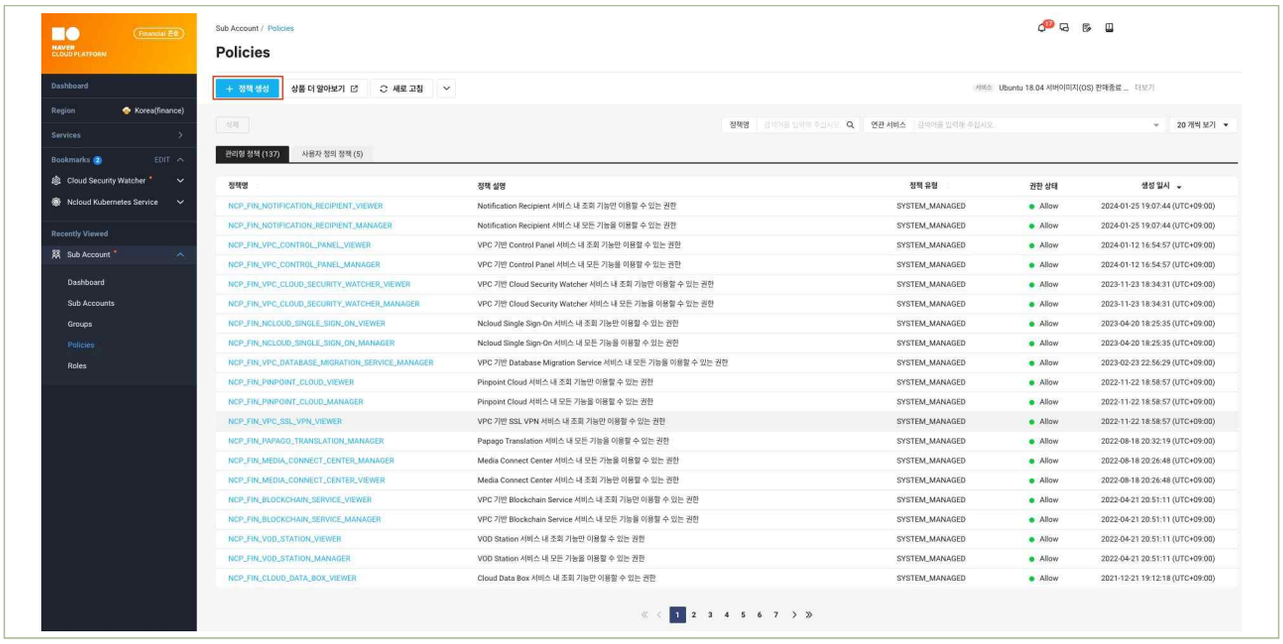
버킷 용도별 사용자 정의 정책 적용

① **(가상자원관리시스템)** 'Services' → 'Sub Account' 상품을 선택합니다.



| 그림 7-1-4 | Sub Account 상품 선택

② **(가상자원관리시스템)** 사용자 정의 정책 생성을 위해 'Policies' → '+ 정책 생성'버튼을 클릭합니다.



| 그림 7-1-5 | 사용자 정의 정책 생성

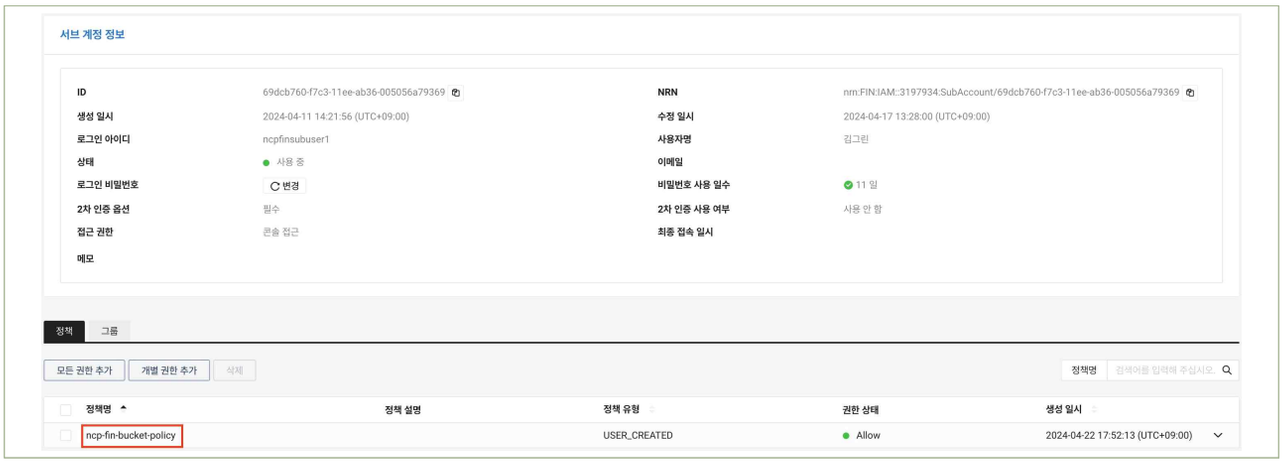
③ **(가상자원관리시스템)** 'Services' → 'Sub Account' → 'Policies' → '+ 정책 생성'을 통해 Object Storage의 버킷 용도에 따라 사용자 정의 정책을 생성합니다.

타입	액션명
View	getObjectList getMultipartUploadList getBucketCORSList getAccessLogList getBucketWebsite getBucketEventList
Change	writeObject deleteBucket changeBucketCORS deleteBucketCORS changeAccessLog changeBucketWebsite deleteBucketWebsite createBucketEvent deleteBucketEvent changeBucketEvent sendBucketExtendedMetricData changeBucketMetricFilter deleteBucketMetricFilter

NRN	리전	리소스 타입	리소스명
nrn:FIN:ObjectStorage:FKR:3197934:Bucket/ncpfinbucket/1713337998883	Korea(finance)	Bucket	ncpfinbucket

| 그림 7-1-6 | 버킷 용도별 사용자 정의 정책 생성 예시

④ **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ → ‘Sub Accounts’ → ‘Sub User 선택’ → ‘그룹 권한 추가 또는 개별 권한 추가’를 통해 버킷 접근이 필요한 서브 계정에게만 사용자 정의 정책을 적용합니다.



| 그림 7-1-7 | 버킷 용도별 사용자 정의 정책 적용 예시

API를 통한 사용자 정의 정책 생성 및 연결

① **(API(CLI))** ‘polices’ API를 통해 목적별 접근허용 버킷에 대한 사용자 정의 정책을 생성합니다.

- 요청 예시

```
POST https://subaccount.apigw.fin-ntruss.com/api/v1/policies
```

- 요청 예시 (Body)

```
{
  "policyName": "string",
  "description": "string",
  "permissions": [
    {
      "effect": "string",
      "targets": [
        {
          "product": "string",
          "actions": [
            "string"
          ],
          "resourceNrns": [
            "string"
          ]
        }
      ]
    }
  ]
}
```

- 응답 예시 (성공)


```
{
  "policyId": "string",
  "policyName": "string",
  "description": "string",
  "validationResult": {
    "details": [
      {
        "code": "string",
        "location": "string",
        "message": "string",
        "type": "ERROR"
      }
    ],
    "success": true
  }
}
```


| 그림 7-1-8 | API를 통한 사용자 정의 정책 생성 예시

② **(API(CLI))** 'polices' API를 통해 서브 계정별 접근허용 버킷에 대한 사용자 정의 정책을 할당합니다.

- 요청 예시

```
POST https://subaccount.apigw.fin-ntruss.com/api/v1/sub-accounts/{subAccountId}/policies
```

- 요청 예시 (Body)


```
{
  "policyIdList": [
    "string"
  ]
}
```


- 응답 예시


```
[
  {
      "id": "policyId1",
      "success": true
  }
]
```


| 그림 7-1-9 | API를 통한 서브 계정별 사용자 정의 정책 할당 예시

4 참고 사항

- [참고1] Object Storage 사용 가이드
- [참고2] Object Storage 권한 관리 가이드
- [참고3] 사용자 정의 정책 생성 가이드
- [참고4] 사용자 정의 정책 생성 API 사용 가이드
- [참고5] 서브계정에 정책 할당 API 사용 가이드

1 기준

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

2 설명

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

  - 예시

    1) 스토리지 객체에 관한 권한(읽기, 쓰기 등)을 세분화하여 목적에 따라 적용하여야 한다.

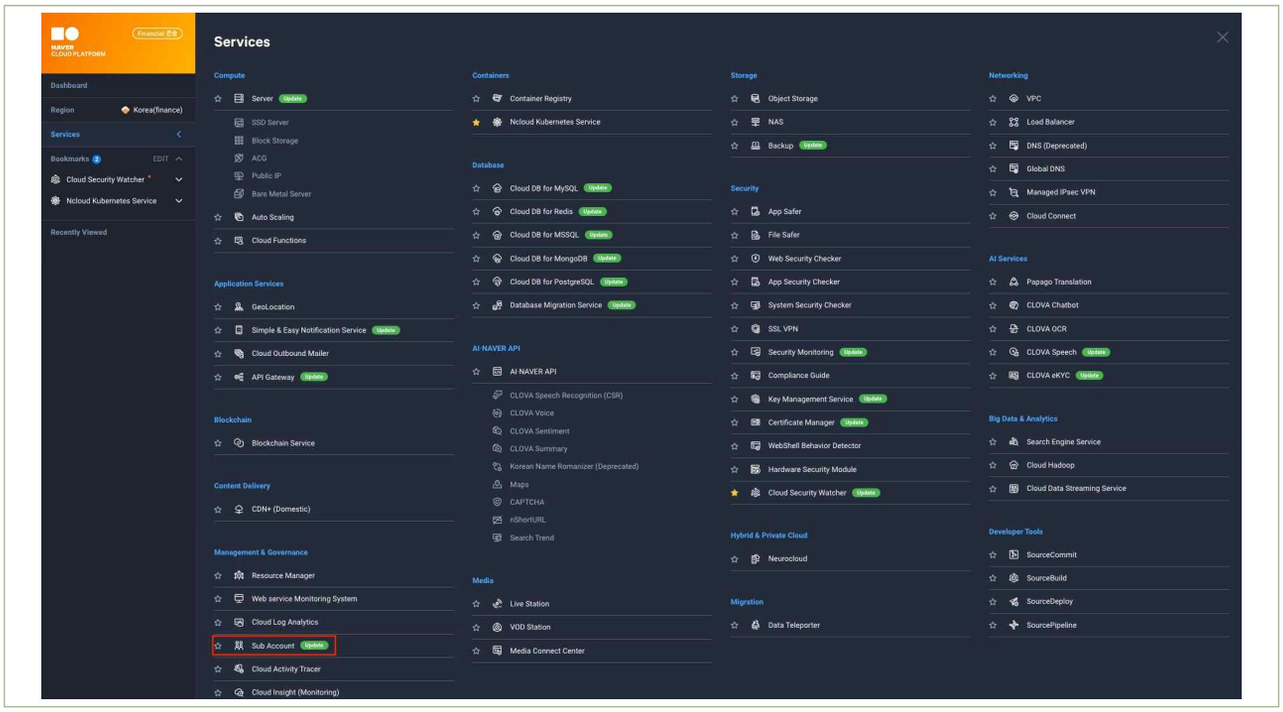
    2) 스토리지 권한 부여 현황에 대한 모니터링 및 주기적 검토 수행

3 우수 사례

- 네이버 클라우드 플랫폼의 Sub Account는 사용자의 업무별로 접근권한을 통제할 수 있도록 권한 관리할 수 있는 상품입니다. 고객은 Sub Account의 사용자 정의 정책을 통해 서브 계정별 접근 가능한 버킷을 정의하고 관리할 수 있습니다.

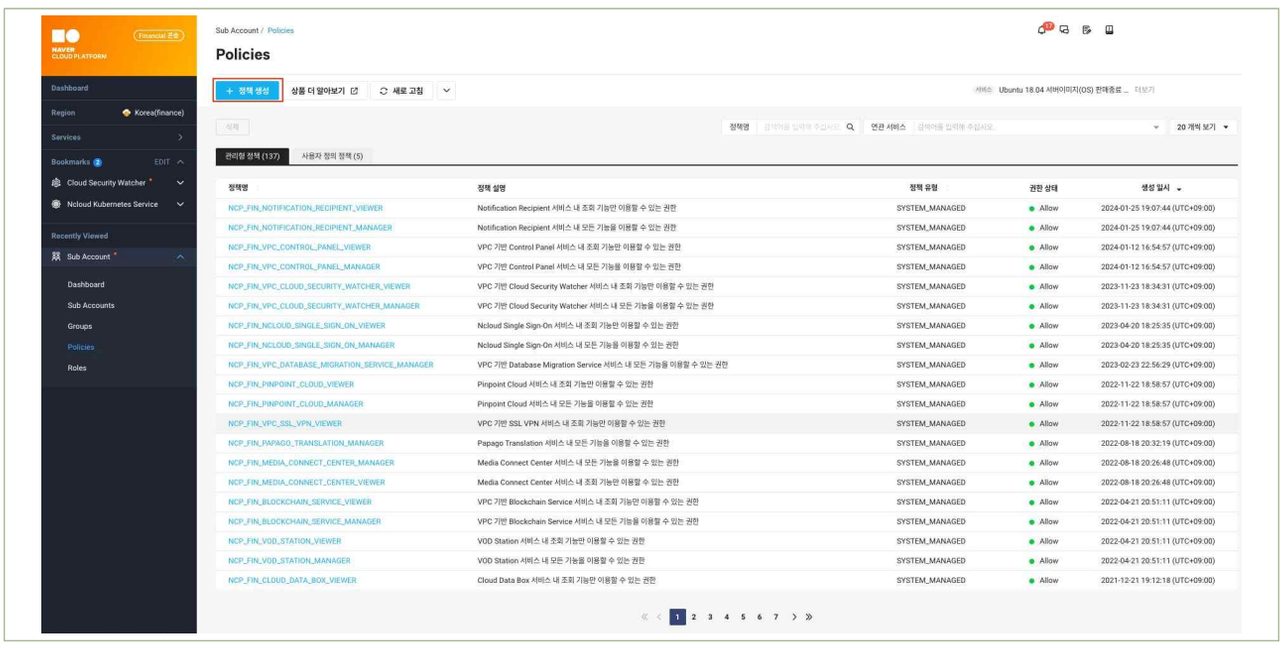
버킷 용도별 사용자 정의 정책 적용

① **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ 상품을 선택합니다.



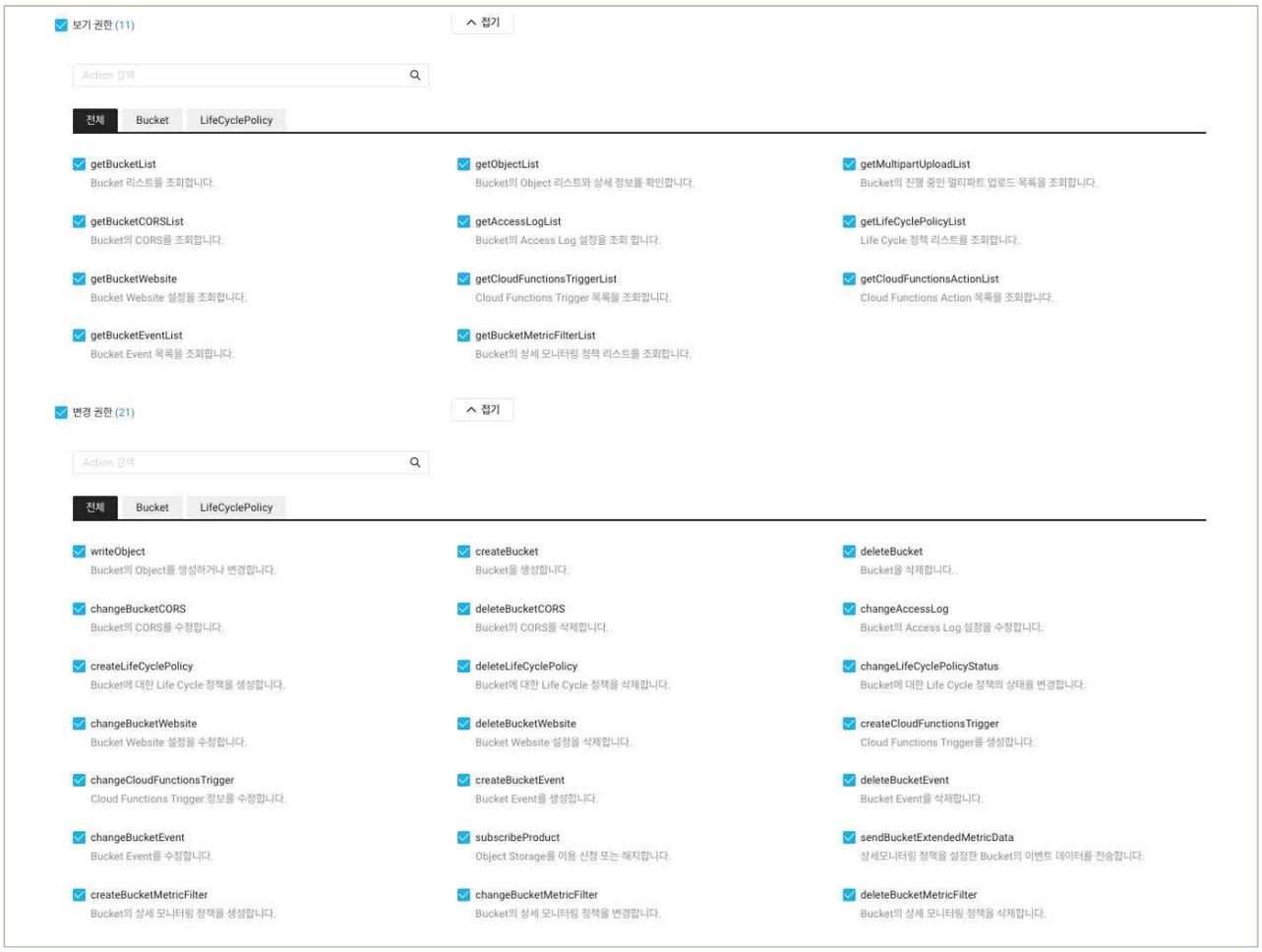
| 그림 7-2-1 | Sub Account 상품 선택

② **(가상자원관리시스템)** 사용자 정의 정책 생성을 위해 ‘Policies’ → ‘+ 정책 생성’버튼을 클릭합니다.



| 그림 7-2-2 | 사용자 정의 정책 생성

③ **(가상자원관리시스템)** 버킷에 대한 읽기, 쓰기 권한을 적용하기 위해 사용자에게 필요한 보기 및 변경 액션을 선택합니다.



| 그림 7-2-3 | 사용자 정의 액션 설정

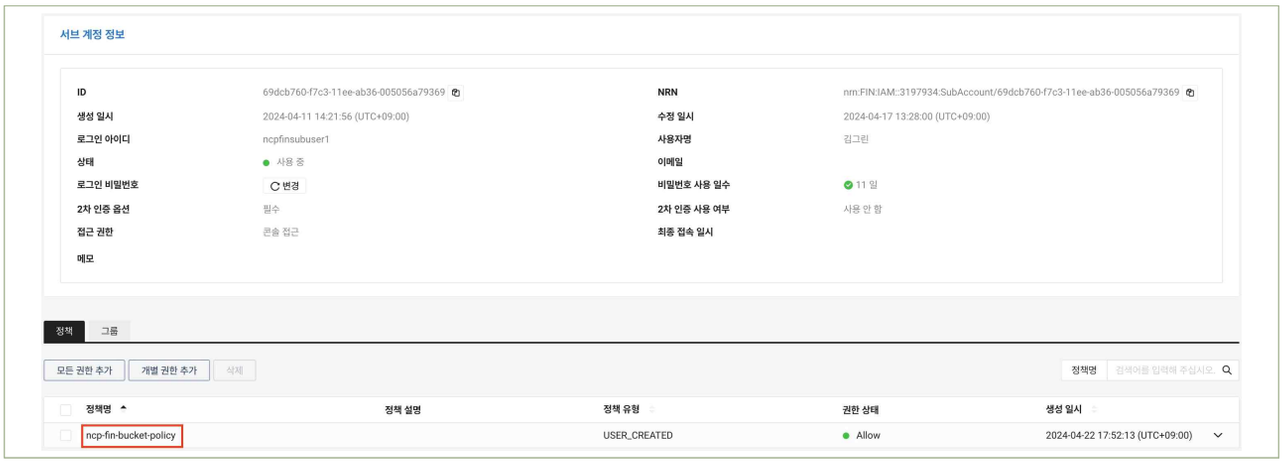
④ **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ → ‘Policies’ → ‘+ 정책 생성’을 통해 Object Storage의 버킷 용도에 따라 사용자 정의 정책을 생성합니다.

타입	액션명
View	getObjectList getMultipartUploadList getBucketCORSList getAccessLogList getBucketWebsite getBucketEventList
Change	writeObject deleteBucket changeBucketCORS deleteBucketCORS changeAccessLog changeBucketWebsite deleteBucketWebsite createBucketEvent deleteBucketEvent changeBucketEvent sendBucketExtendedMetricData changeBucketMetricFilter deleteBucketMetricFilter

NRN	리전	리소스 타입	리소스명
nrn:FIN:ObjectStorage:FKR:3197934:Bucket/ncpfinbucket/1713337998883	Korea(finance)	Bucket	ncpfinbucket

| 그림 7-2-4 | 버킷 용도별 사용자 정의 정책 생성 예시

⑤ **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ → ‘Sub Accounts’ → ‘Sub User 선택’ → ‘그룹 권한 추가 또는 개별 권한 추가’를 통해 버킷 접근이 필요한 서브 계정에게만 사용자 정의 정책을 적용합니다.



| 그림 7-2-5 | 버킷 용도별 사용자 정의 정책 적용 예시

API를 통한 사용자 정의 정책 생성 및 연결

① **(API(CLI))** ‘polices’ API를 통해 목적별 접근허용 버킷에 대한 사용자 정의 정책을 생성합니다.

- 요청 예시

```
POST https://subaccount.apigw.fin-ntruss.com/api/v1/policies
```

- 요청 예시 (Body)

```
{
  "policyName": "string",
  "description": "string",
  "permissions": [
    {
      "effect": "string",
      "targets": [
        {
          "product": "string",
          "actions": [
            "string"
          ],
          "resourceNrns": [
            "string"
          ]
        }
      ]
    }
  ]
}
```

- 응답 예시 (성공)


```
{
  "policyId": "string",
  "policyName": "string",
  "description": "string",
  "validationResult": {
    "details": [
      {
        "code": "string",
        "location": "string",
        "message": "string",
        "type": "ERROR"
      }
    ],
    "success": true
  }
}
```


| 그림 7-2-6 | API를 통한 사용자 정의 정책 생성 예시

② **(API(CLI))** 'polices' API를 통해 서브 계정별 접근허용 버킷에 대한 사용자 정의 정책을 할당합니다.

- 요청 예시

```
POST https://subaccount.apigw.fin-ntruss.com/api/v1/sub-accounts/{subAccountId}/policies
```

- 요청 예시 (Body)


```
{
  "policyIdList": [
    "string"
  ]
}
```


- 응답 예시


```
[
  {
      "id": "policyId1",
      "success": true
  }
]
```


| 그림 7-2-7 | API를 통한 서브 계정별 사용자 정의 정책 할당 예시

4 참고 사항

- [참고1] Object Storage 사용 가이드
- [참고2] Object Storage 권한 관리 가이드
- [참고3] 사용자 정의 정책 생성 가이드
- [참고4] 사용자 정의 정책 생성 API 사용 가이드
- [참고5] 서브계정에 정책 할당 API 사용 가이드

1 기준

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

2 설명

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

  - 예시

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

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

3 우수 사례

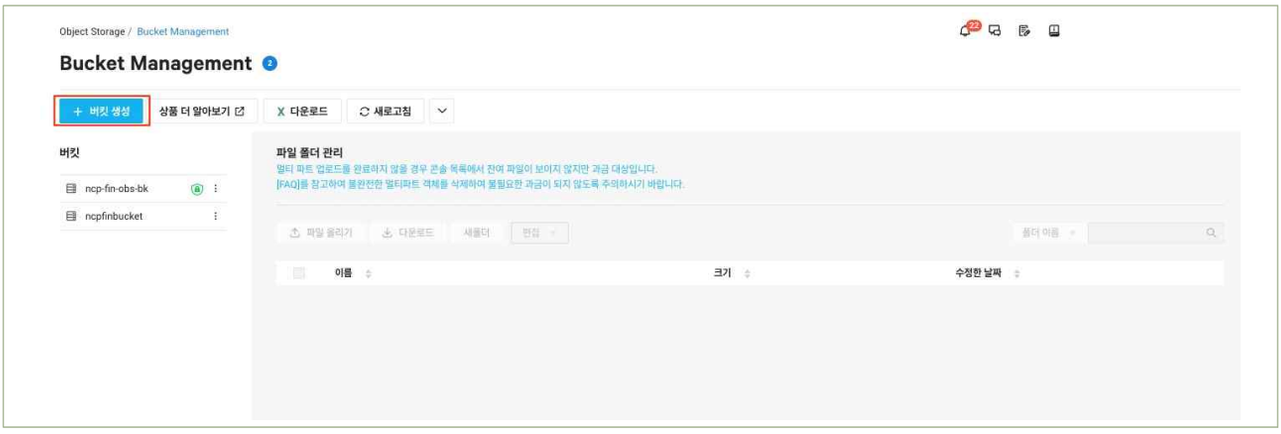
- 네이버 클라우드 플랫폼의 Object Storage는 업로드, 다운로드 등에 대한 상세 모니터링을 지원합니다. 고객은 상세 모니터링의 접두사, 접미사를 정의를 활용하여 특정 파일명과 파일 확장자에 대한 업로드, 다운로드 등을 탐지하고 알림을 전송 받을 수 있도록 구성하여야 합니다.

확장자 모니터링을 위한 정책 적용

① **(가상자원관리시스템)** ‘Services’ → ‘Object Storage’ 상품을 선택합니다.

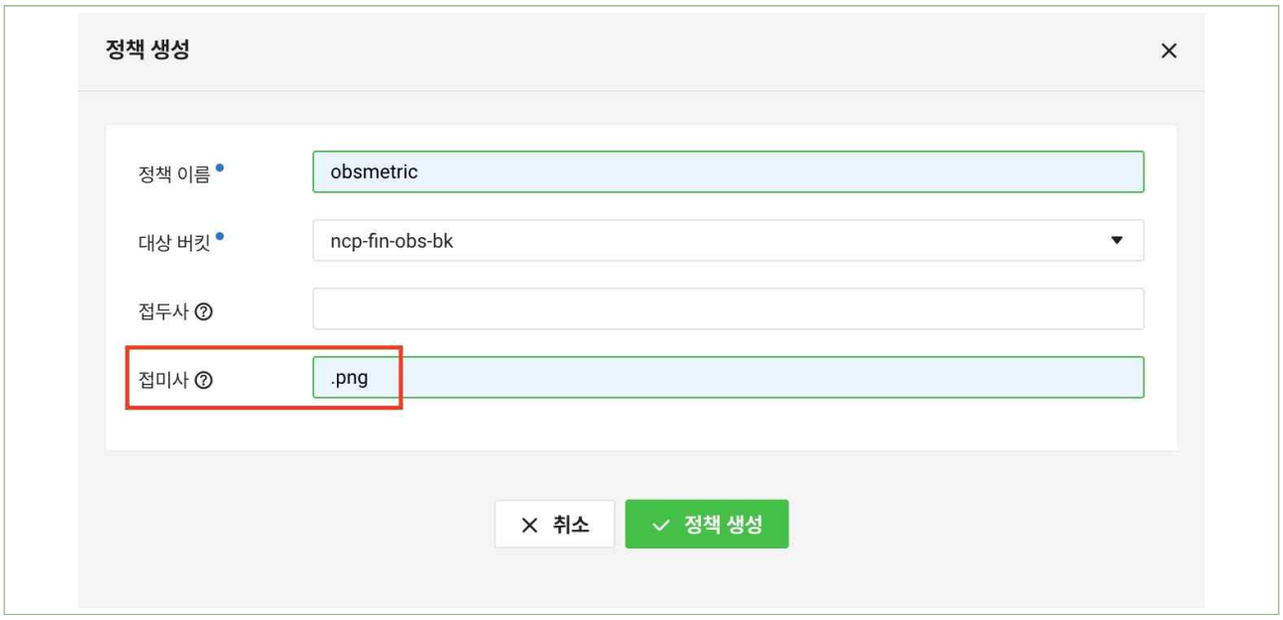
| 그림 7-3-1 | Object Storage 상품 선택

② **(가상자원관리시스템)** ‘Bucket Management’ → ‘+ 버킷 생성’을 클릭하여 버킷을 생성합니다.



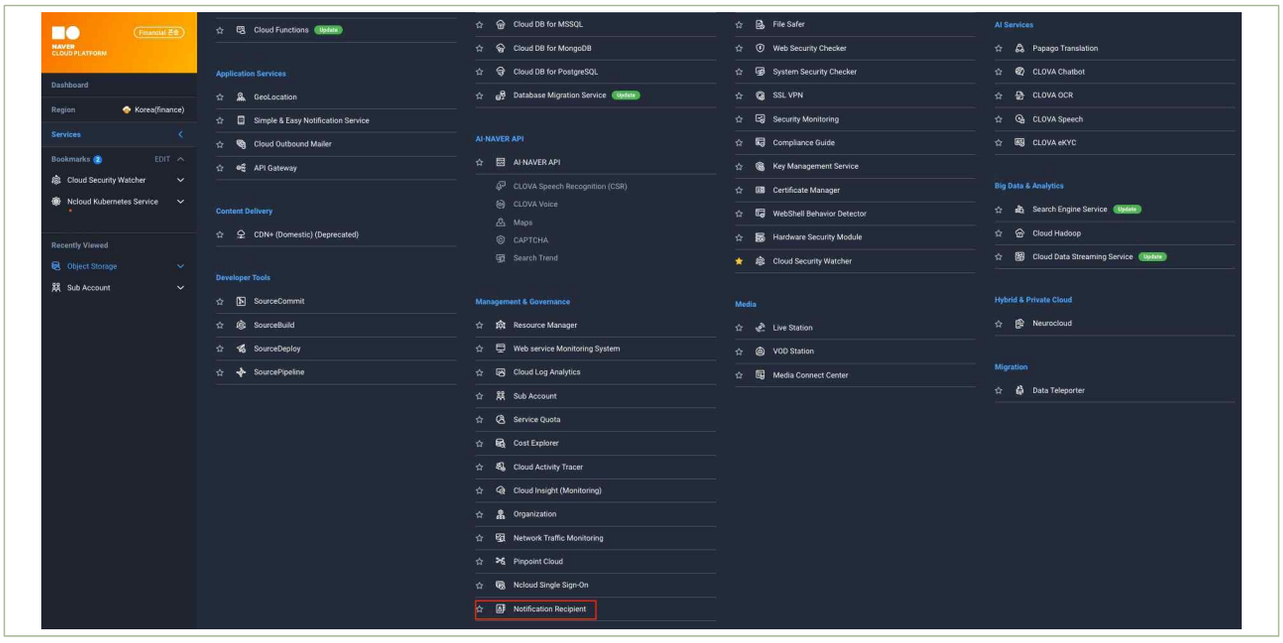
| 그림 7-3-2 | Object Storage 버킷 생성

③ **(가상자원관리시스템)** ‘Metric Management’ → ‘+ 상세 모니터링 정책 생성’을 통해 상세 모니터링이 필요한 파일 확장자를 접미사(suffix)로 등록합니다.



| 그림 7-3-3 | 모니터링을 위한 파일 확장자 등록 예시

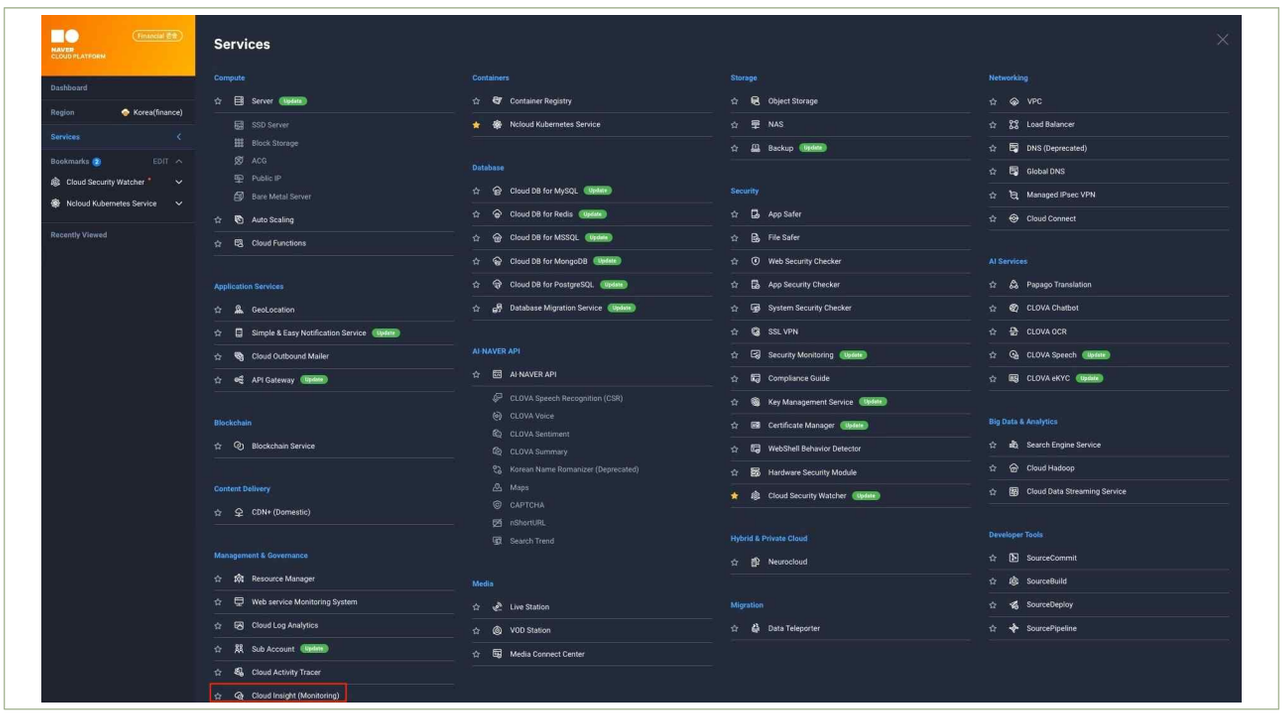
④ **(가상자원관리시스템)** ‘Services’ → ‘Notification Recipient’ 상품을 선택합니다.



⑤ **(가상자원관리시스템)** ‘Notification Recipient’ → ‘+ 대상자 추가’를 통해 알림을 수신할 관리자의 휴대전화 번호, 이메일 주소를 등록합니다.

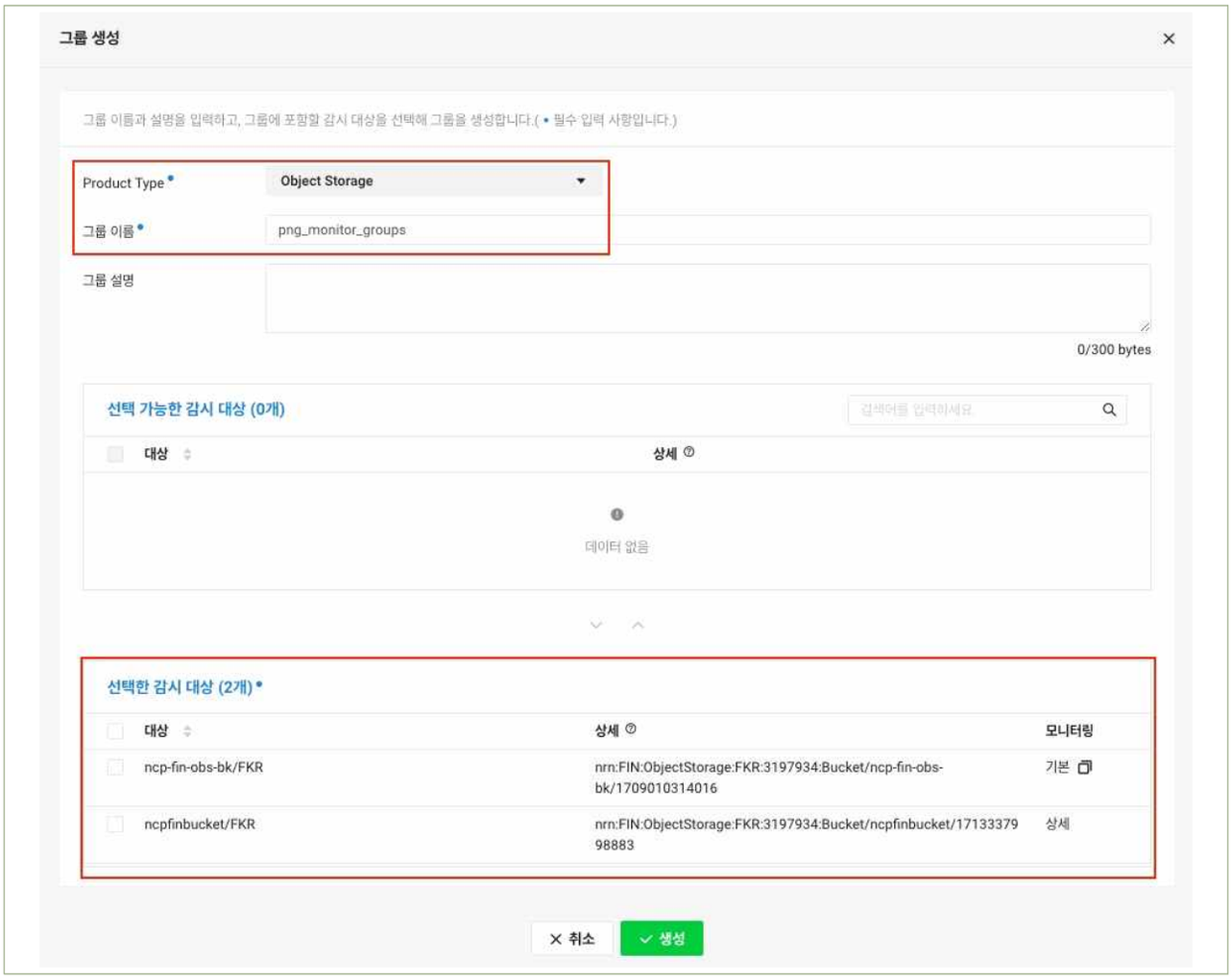
| 그림 7-3-4 | 모니터링 관리자 알림 등록 예시

⑥ **(가상자원관리시스템)** ‘Services’ → ‘Cloud Insight’ 상품을 선택합니다.



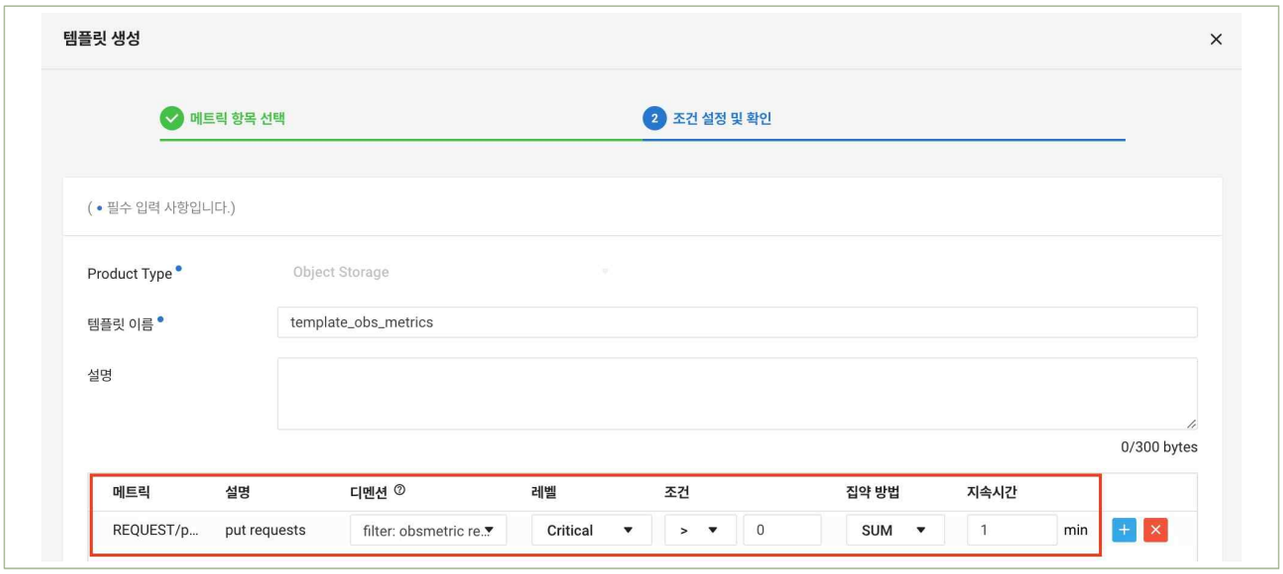
| 그림 7-3-5 | Cloud Insight 상품 선택

⑦ **(가상자원관리시스템)** 'Configuration' → 'Template' → '대상 그룹 생성'을 통해 상세 모니터링이 필요한 Object Storage의 버킷을 지정합니다.



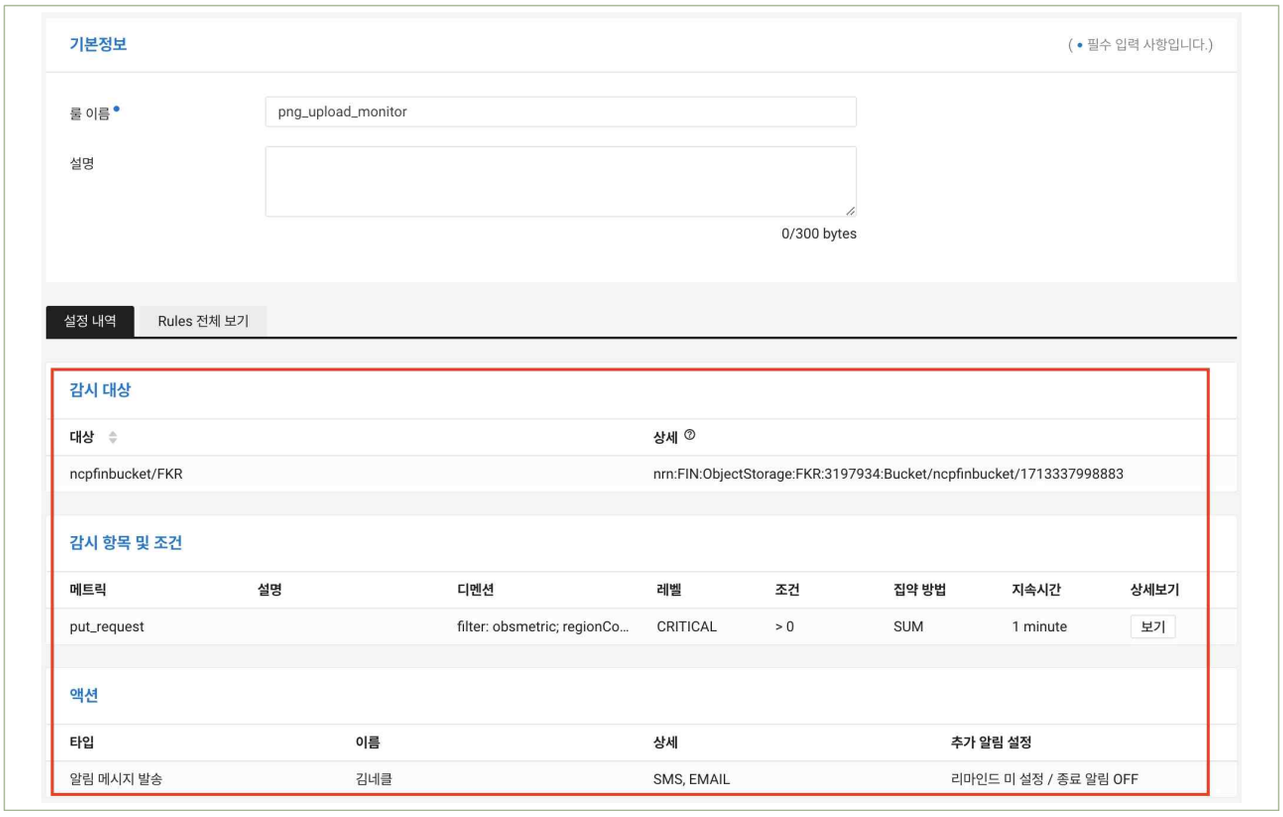
| 그림 7-3-6 | 모니터링 대상 Object Storage선택

⑧ **(가상자원관리시스템)** ‘Configuration’ → ‘Template’ → ‘룰 템플릿 생성’을 통해 앞서 정의한 Object Storage의 Metric 정책에 대한 임계값을 설정합니다.



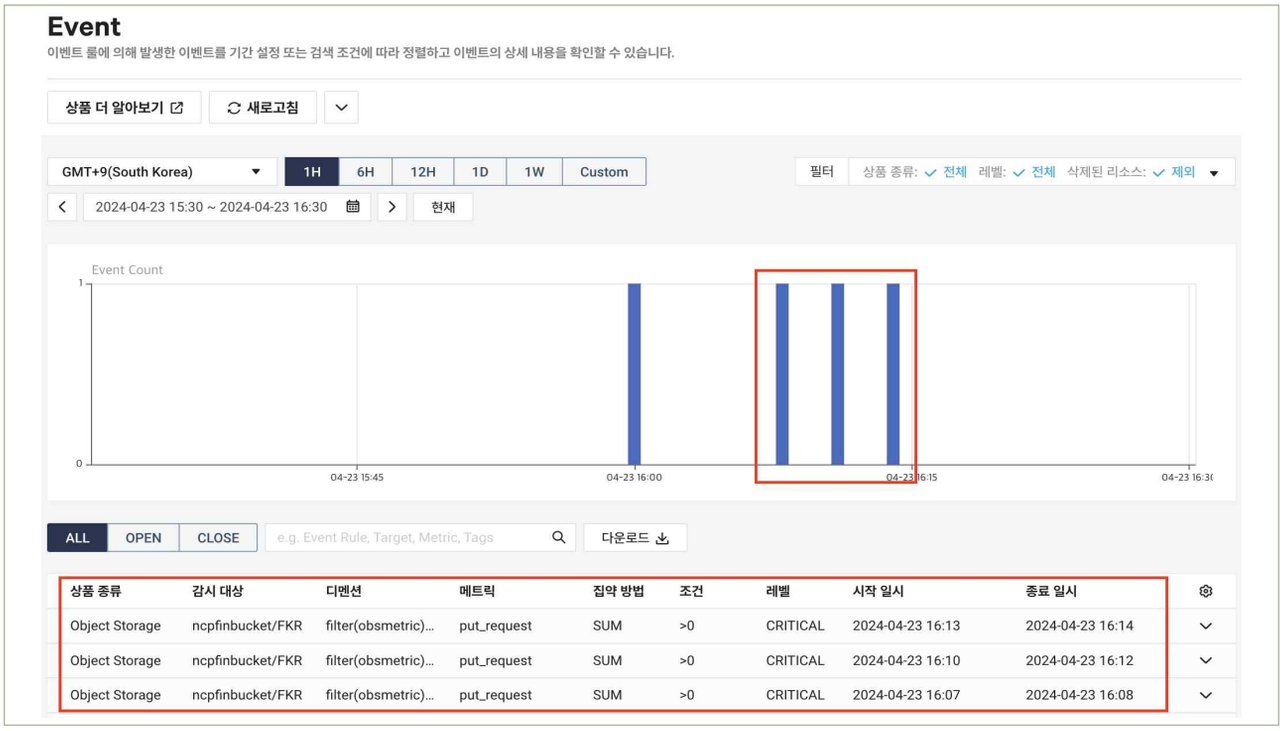
| 그림 7-3-7 | 모니터링 대상 버킷 및 임계값 정의 예시

⑨ **(가상자원관리시스템)** ‘Configuration’ → ‘Event Rule’ → ‘Event Rules 생성’을 통해 그룹(대상 버킷), 템플릿(임계값 정책), 알림 대상자를 연결합니다.

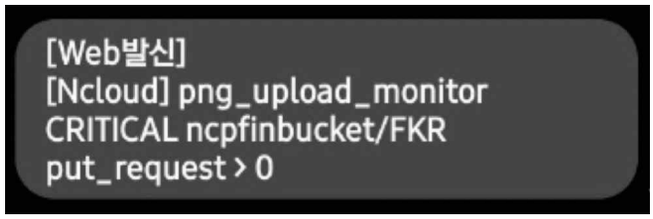


| 그림 7-3-8 | 특정 파일 확장자 업로드 모니터링 정책 생성 예시

⑩ **(가상자원관리시스템)** 생성된 이벤트 룰은 Cloud Insight의 Event에서 모니터링 할 수 있으며, 정의한 이벤트 룰에 따라 이벤트가 감지되면 지정한 관리자에게 SMS 또는 E-mail 등을 통해 알림이 전송됩니다.



| 그림 7-3-9 | 특정 파일 확장자 업로드 모니터링 예시



| 그림 7-3-10 | 특정 파일 확장자 업로드 알림 SMS 예시

이 외에도 Cloud Function을 이용하면 이벤트 로그를 파라미터로 사용하여 다양한 형태로 응용할 수 있습니다. 자세한 사항은 참고 사항 링크를 통해 확인할 수 있습니다.

4 참고 사항

- [참고1] Object Storage 사용 가이드
- [참고2] Object Storage 이벤트 알람 이용 가이드
- [참고3] Cloud Insight Event Rule 생성 가이드

8. 백업 및 이중화 관리

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

8 백업 및 이중화 관리

1 기준

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

2 설명

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

  - 예시

    1) 스토리지 행위 감사로그 백업

    2) 클라우드 웹 콘솔 감사로그 별도의 파일로 보관 등

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

3 우수 사례

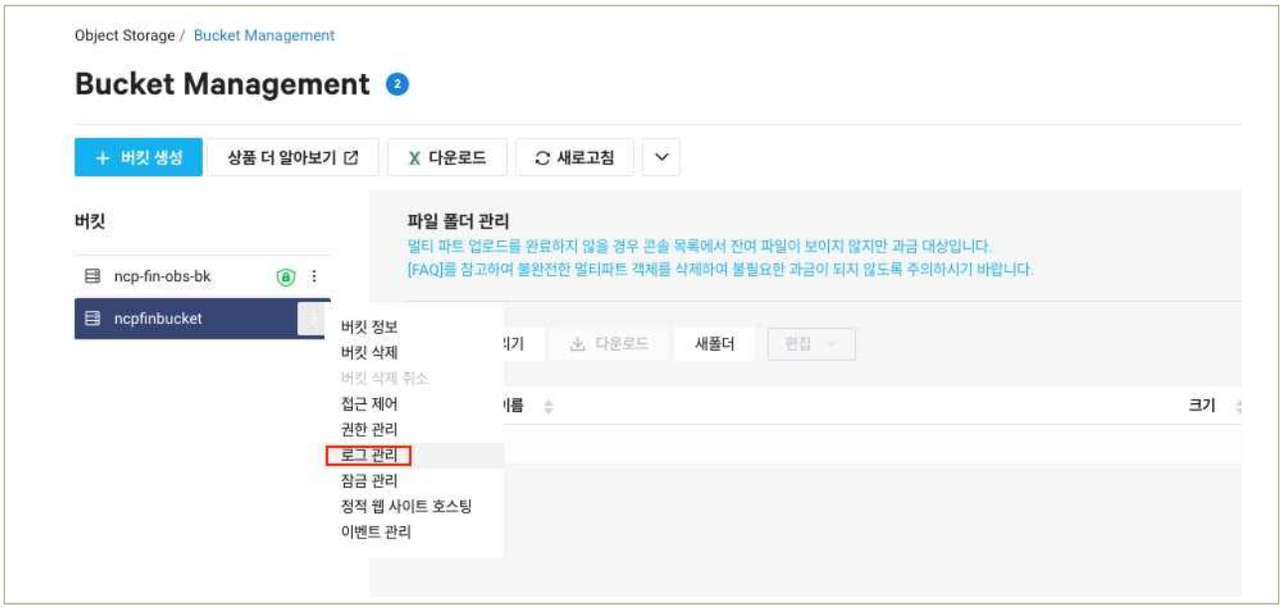
- 네이버 클라우드 플랫폼은 클라우드 이용 내역을 추적할 수 있도록 다양한 상품을 통해 지원합니다. 가상자원관리시스템(클라우드 관리 콘솔)의 경우에는 Cloud Security Activity 상품을 통해 사용자가 가상자원관리시스템(클라우드 관리 콘솔)에서 수행하는 내용과 API를 통한 요청에 대해서도 모두 기록하고 내용을 추적할 수 있으며, Object Storage에서는 별도의 로그 관리 기능을 통해 Storage 내 객체의 저장과 삭제 등에 대해서 자세하게 기록할 수 있습니다.

Object Storage의 로그 관리 설정

① **(가상자원관리시스템)** ‘Services’ → ‘Object Storage’ 상품을 선택합니다.

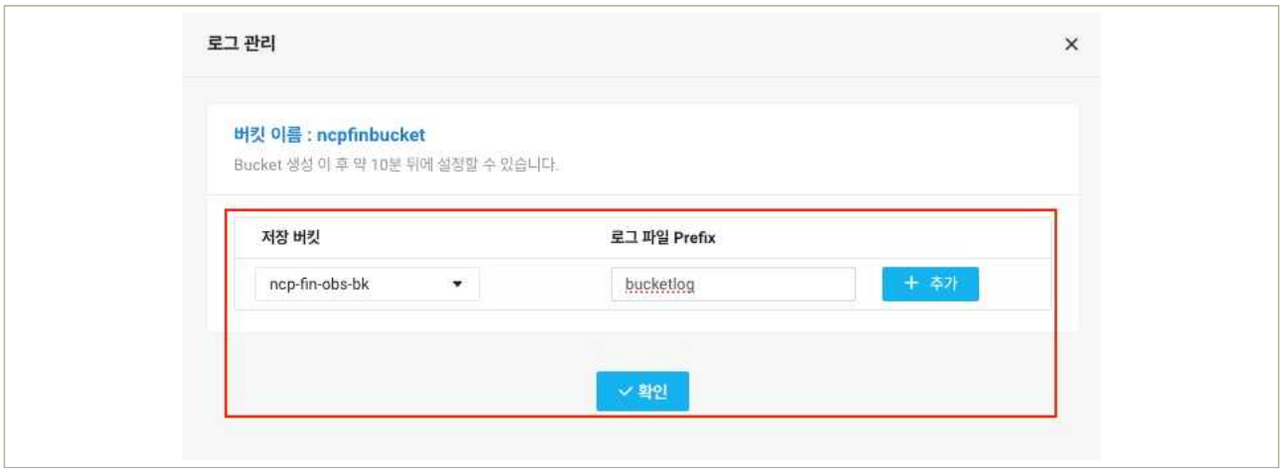
| 그림 8-1-1 | Object Storage 상품 선택

② **(가상자원관리시스템)** 로그 관리 설정이 필요한 ‘버킷 선택’ → ‘로그 관리’를 선택합니다.



| 그림 8-1-2 | 로그 관리 선택

③ **(가상자원관리시스템)** 로그를 저장할 버킷과 로그 파일의 접두사를 작성하고 '+ 추가' 버튼을 선택하여 로그 관리 설정을 완료합니다.



| 그림 8-1-3 | 로그 관리 설정

④ **(가상자원관리시스템)** 로그 저장 버킷에서 기록된 로그를 확인합니다.

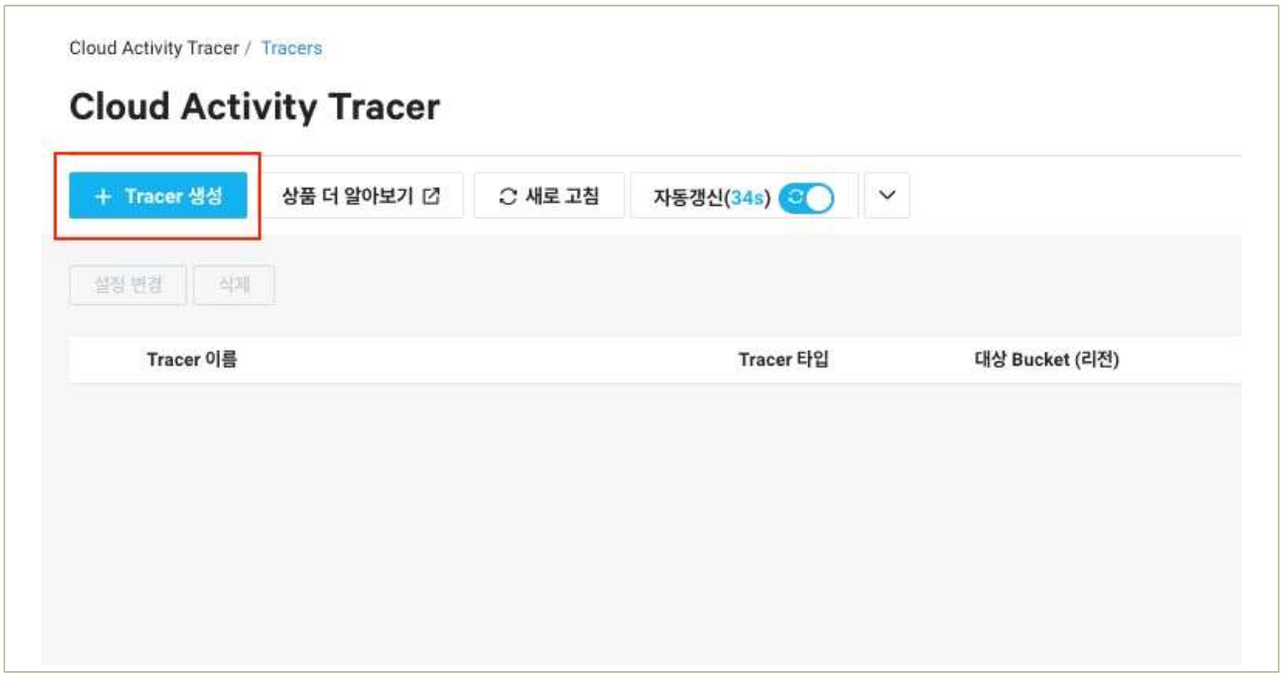
| 그림 8-1-4 | 기록된 로그 확인

Cloud Activity Tarcer의 로그 백업 설정

① **(가상자원관리시스템)** ‘Services’ → ‘Cloud Activity Tracer’ 상품을 선택합니다.

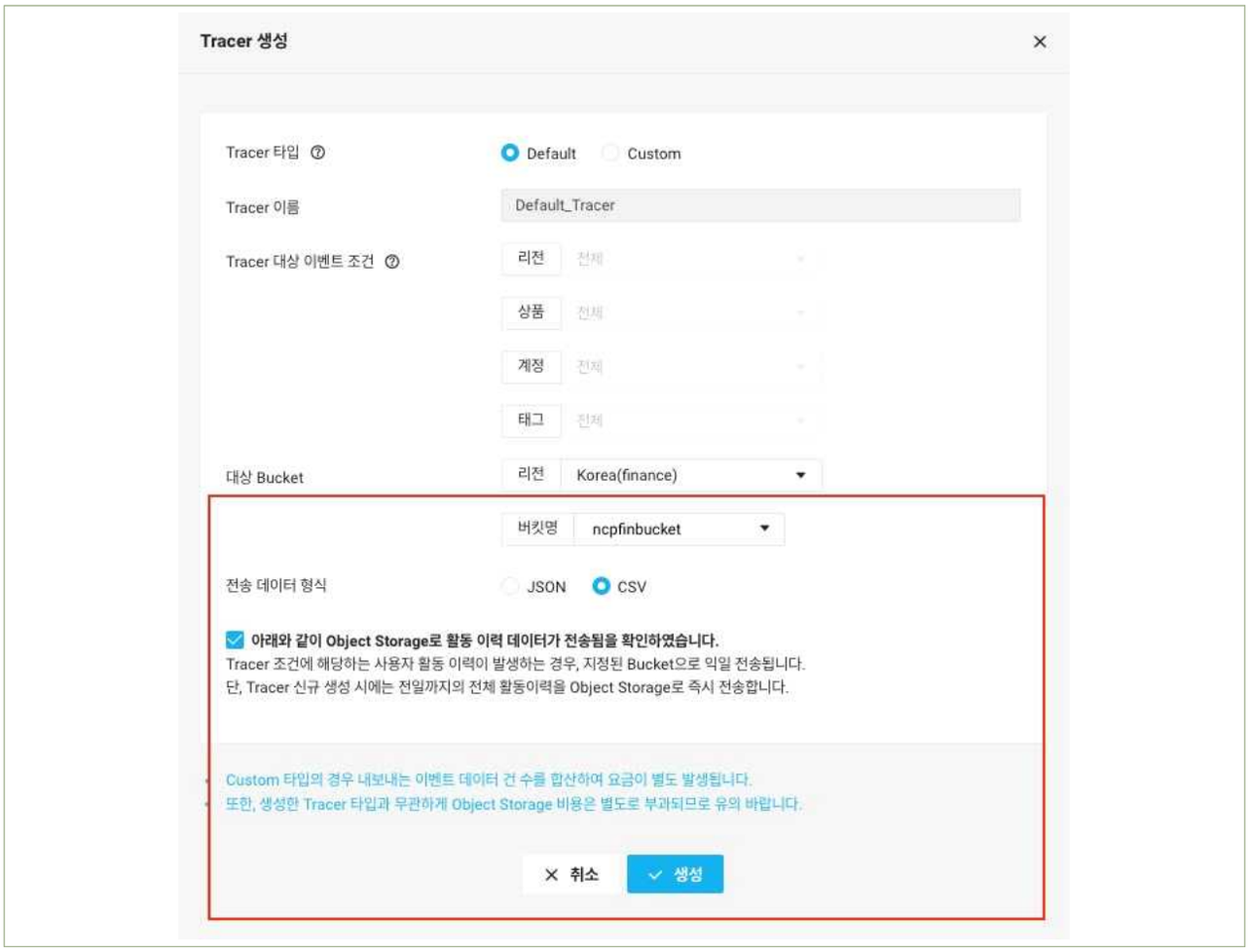
| 그림 8-1-5 | Cloud Activity Tracer상품 선택

② **(가상자원관리시스템)** ‘Tracers’ → ‘+ Tracer 생성’을 선택합니다.



| 그림 8-1-6 | Tracer 생성 선택

③ **(가상자원관리시스템)** Cloud Activity Tracer의 로그를 저장할 버킷과 전송 데이터 형식을 를 지정하고 로그 백업 설정을 완료합니다.

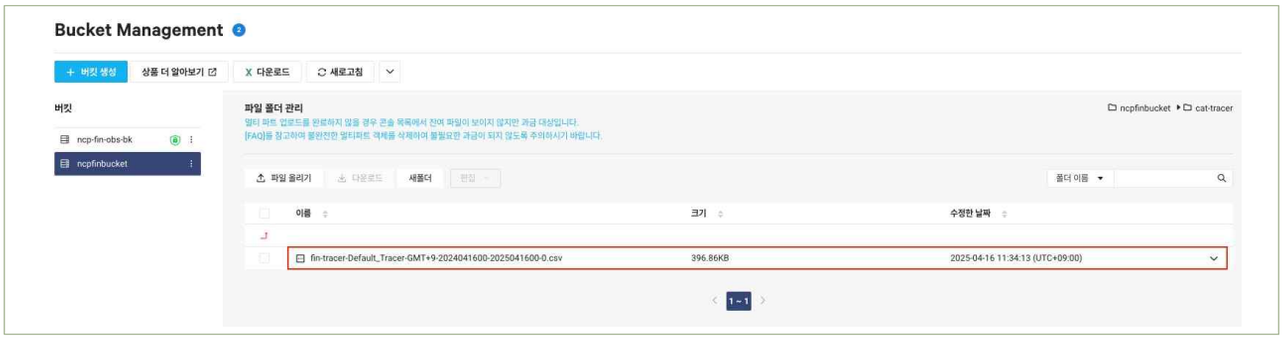


| 그림 8-1-7 | Tracer 설정

④ **(가상자원관리시스템)** 생성된 Tracer의 설정 사항을 확인합니다.

| 그림 8-1-8 | Tracer 생성 확인

⑤ **(가상자원관리시스템)** 로그 저장 버킷에서 생성된 Cloud Activity Tracer 로그를 확인합니다.



| 그림 8-1-9 | 로그 생성 결과 확인

4 참고 사항

- [참고1] Object Storage 로그 관리 설정 가이드
- [참고2] Cloud Activity Tracer 사용자 가이드

1 기준

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

2 설명

- 이용자의 행위추적성 백업 증적(로그 등)은 무결하게 보관하여야 한다.

  - 예시

    1) 감사로그 훼손 탐지에 대한 알람 설정

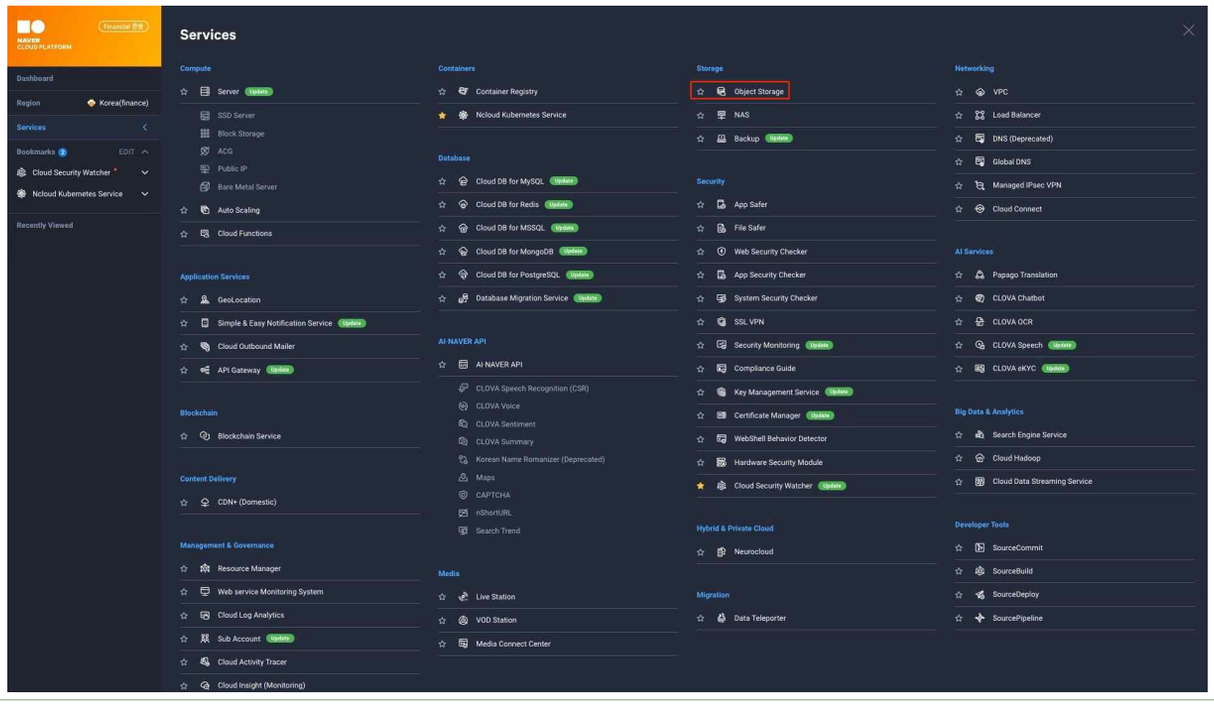
    2) 별도 스토리지 백업 기능(객체 잠금 등)을 통해 로그 무결성 보장 등

3 우수 사례

- 네이버 클라우드 플랫폼은 사용자의 클라우드 이용 내역을 추적할 수 있도록 Cloud Activity Tracer의 로그는 Object Storage에 안전하게 보존할 수 있도록 구성할 수 있으며, 이러한 감사로그의 훼손을 탐지하기 위해 사용자는 Cloud Activity Tracer 로그가 기록되는Object Storage Bucket의 접근권한을 최소한으로 부여하고, Bucket의 이벤트 설정을 통해 객체 삭제에 대한 알람을 설정할 수 있습니다.

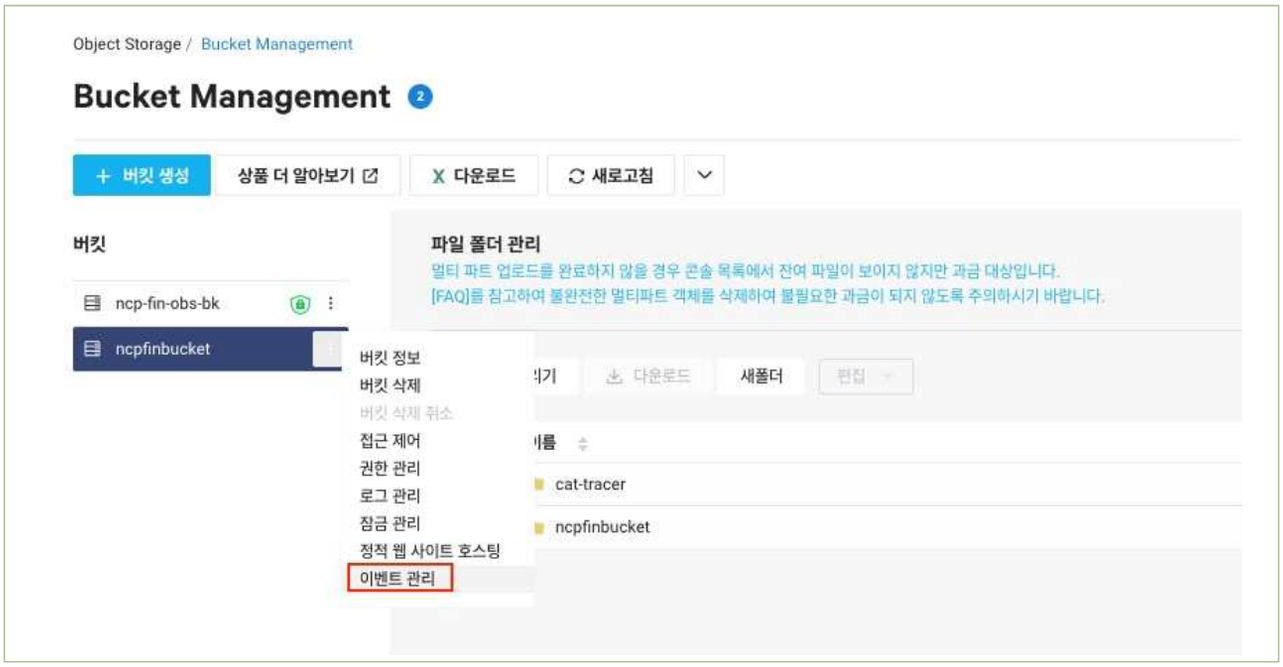
Object Storage 이벤트 설정

① **(가상자원관리시스템)** 'Services' → 'Object Storage' 상품을 선택합니다.



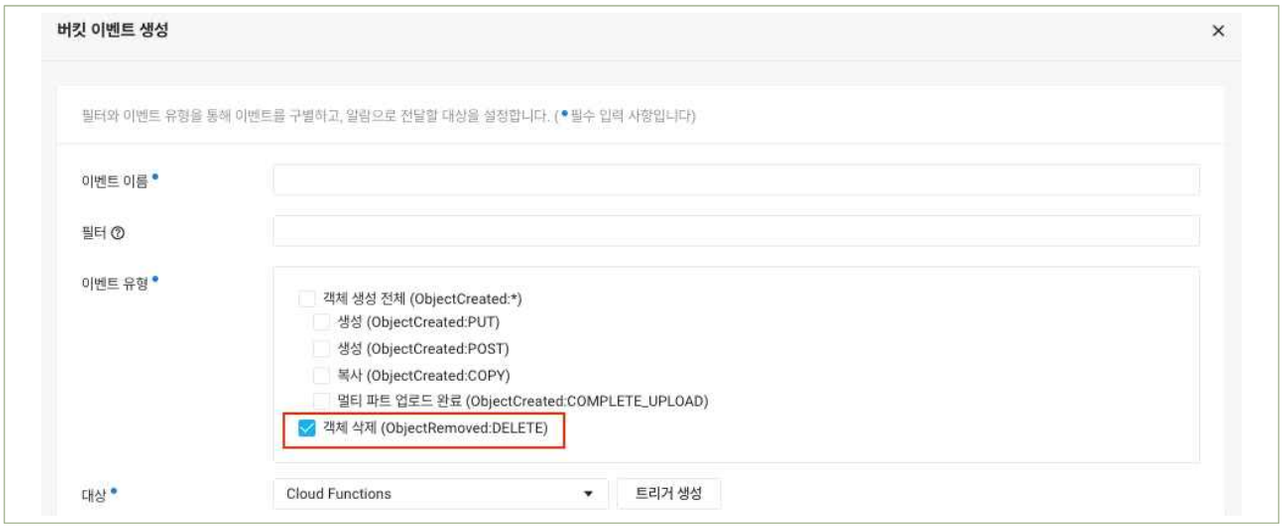
| 그림 8-2-1 | Object Storage 상품 선택

② **(가상자원관리시스템)** 'Bucket Management' → '적용 대상 Bucket' → '이벤트 관리'를 선택합니다.



| 그림 8-2-2 | 이벤트 관리 선택

③ **(가상자원관리시스템)** 이벤트 유형에서 '객체 삭제'를 선택하고, Cloud Functions의 Trigger와 Action을 생성하여 Simple & Easy Notification Service를 통해 알림을 받도록 연동합니다.



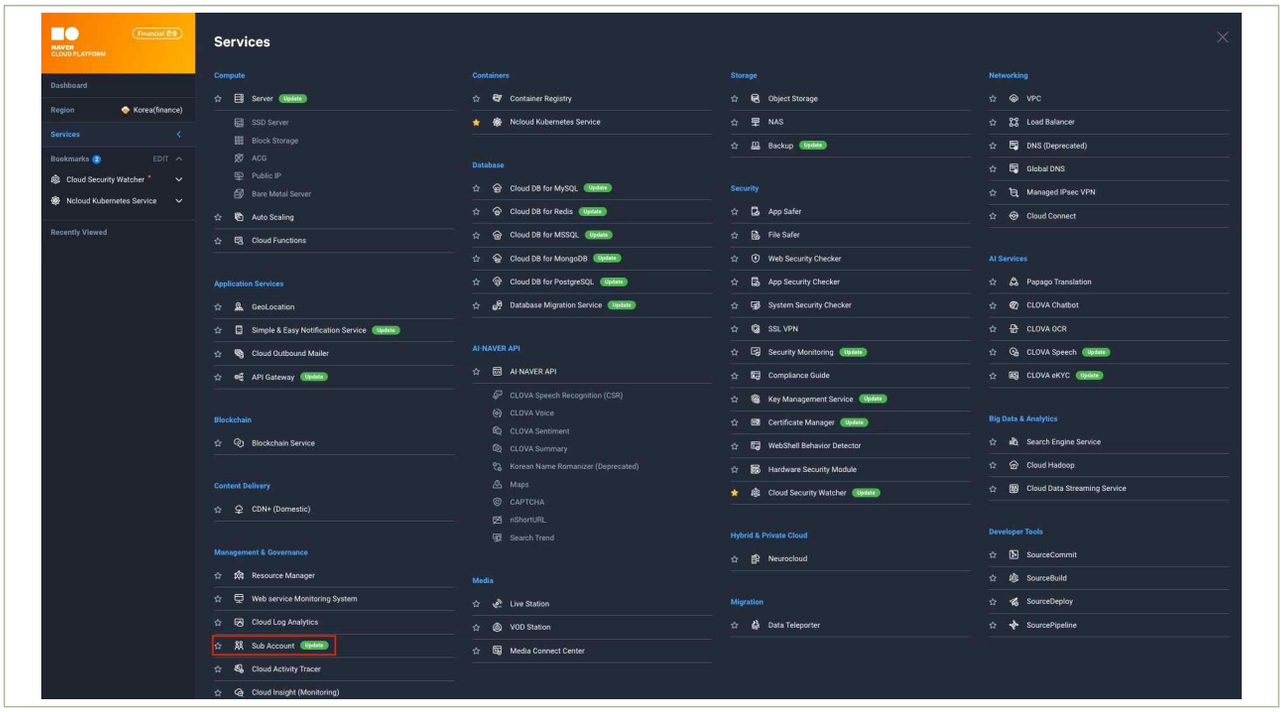
| 그림 8-2-3 | 이벤트 생성 및 Cloud Functions 연동

※ Object Storage에서 생성한 이벤트가 발생하면 Object Storage 타입 트리거에 이벤트 정보가 전달됩니다. 전달된 이벤트를 Object Storage 타입 트리거에 연결된 액션 코드에서 파라미터로 사용하여 다양하게 응용할 수 있습니다. Object Storage 타입 트리거에 전달되는 이벤트 예제는 다음과 같습니다.

```
{
  "container_name": "my-bucket",          // 버킷 이름
  "event_name": "my-event-rule",          // 이벤트 이름
  "event_type": "ObjectCreated:PUT"       // 이벤트 종류
  "event_version": "1.0"                  // 이벤트 포맷 버전
  "object_length": "1000",                // 객체 크기
  "object_name": "my-object",             // 객체 키
  "region": "KR",                         // 리전 이름
  "remote_address": "127.0.0.1",          // 요청 IP
  "remote_user_sha256": "ef5dd4b34d...", // 사용자 Access Key의 SHA256 hash hex값
  "remote_user_type": "user",             // 사용자 종류
  "request_method": "PUT",                // 요청 메서드
  "request_type": "REST.PUT.OBJECT",      // 요청 종류
  "timestamp_finish": "1627881611929",    // 요청 처리가 끝난 시간, 유닉스 시간, 밀리초
  "timestamp_start": "1627881611914"      // 요청 처리를 시작한 시간, 유닉스 시간, 밀리초
}
```

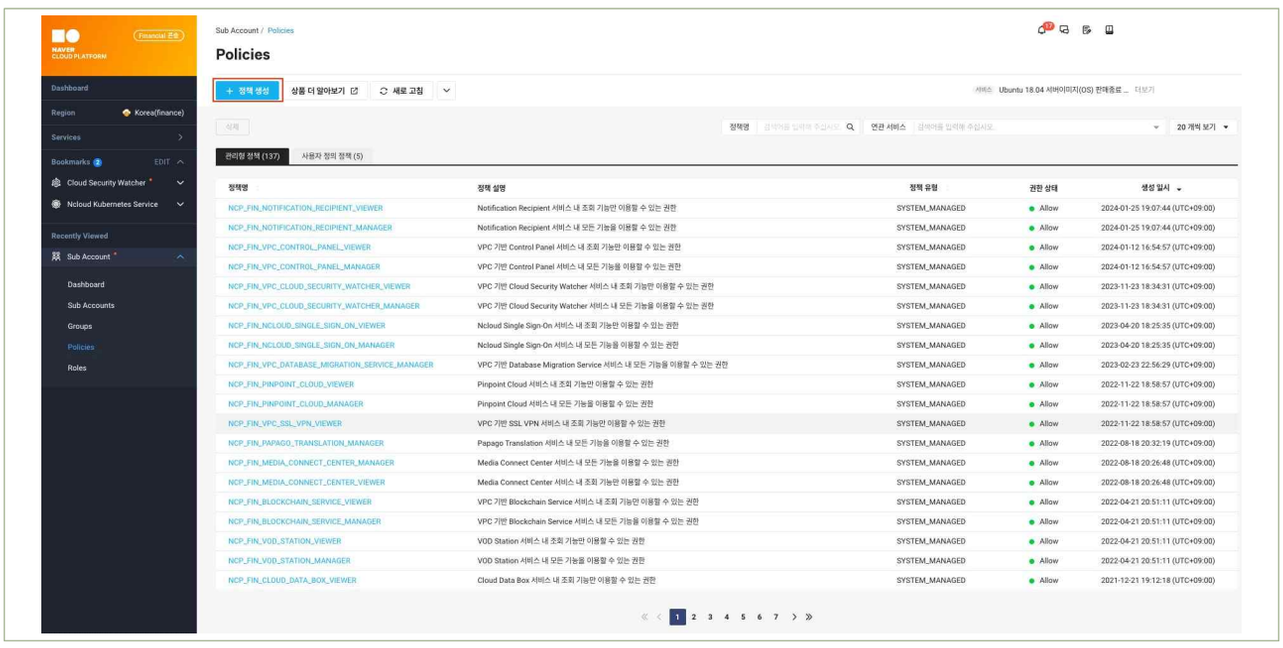
Cloud Activity Tracer 로그의 접근권한 최소화 설정

① **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ 상품을 선택합니다.



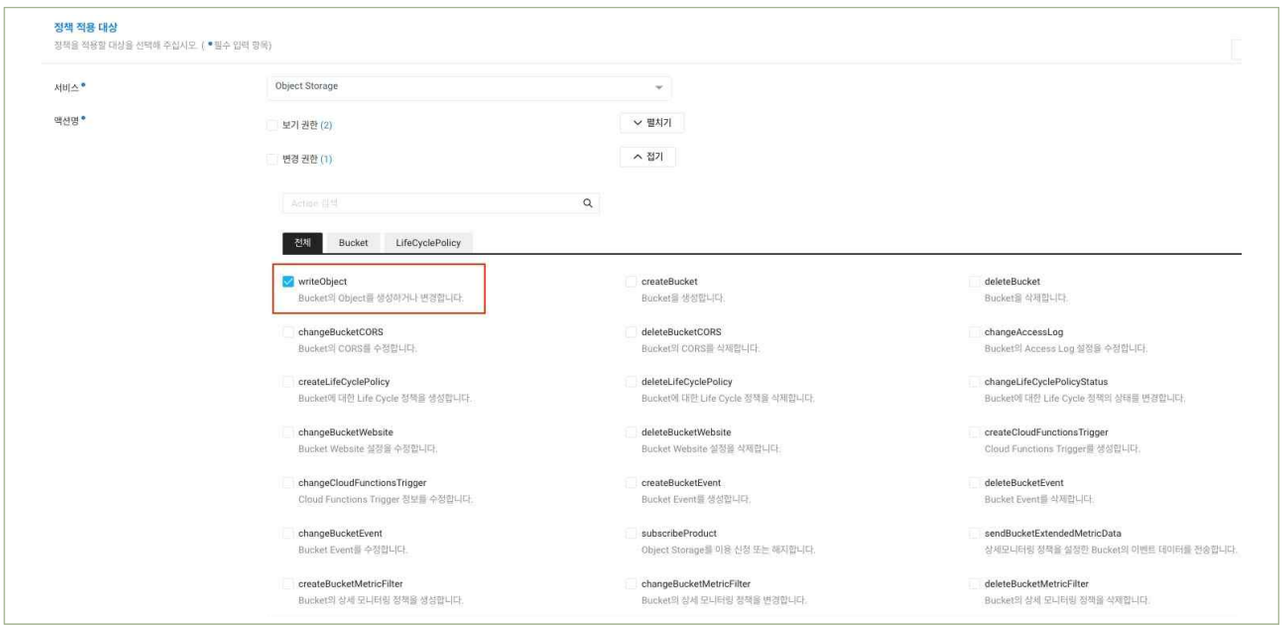
| 그림 8-2-4 | Sub Account 상품 선택

② **(가상자원관리시스템)** 사용자 정의 정책 생성을 위해 ‘Policies’ → ‘+ 정책 생성’버튼을 클릭합니다.



| 그림 8-2-5 | 사용자 정의 정책 생성

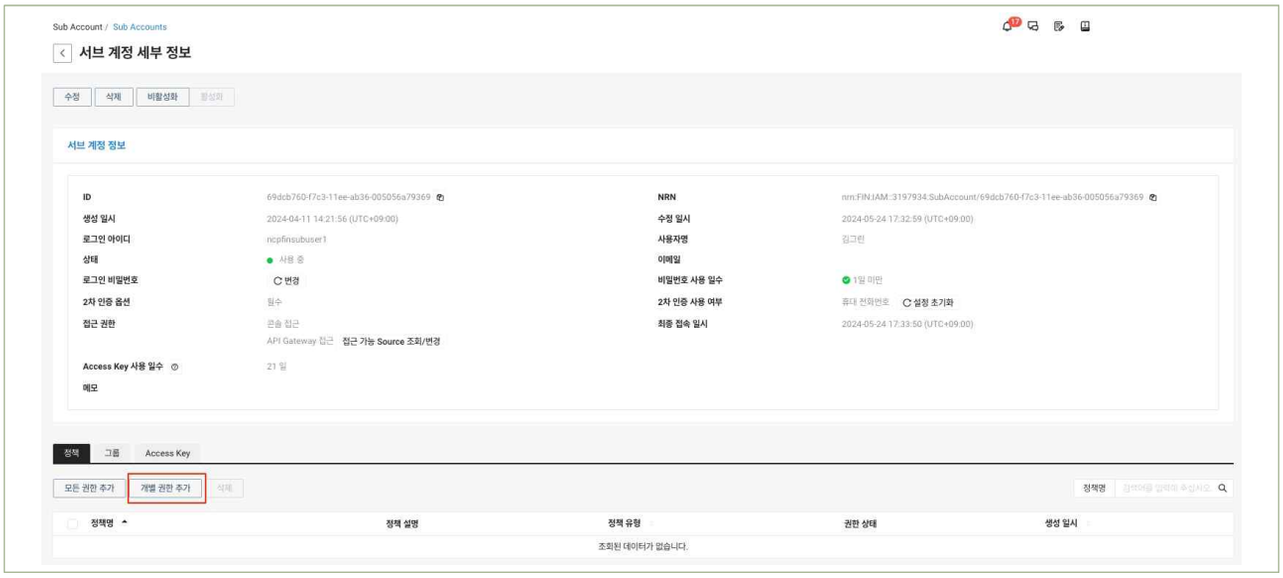
③ **(가상자원관리시스템)** ‘Policies’ → ‘+ 정책 생성’를 통해 버킷의 객체 변경 권한과 Cloud Activity Tracer 로그가 기록되는 버킷을 선택하여 정책을 생성합니다.



| 그림 8-2-6 | 버킷의 객체 변경 권한 선택

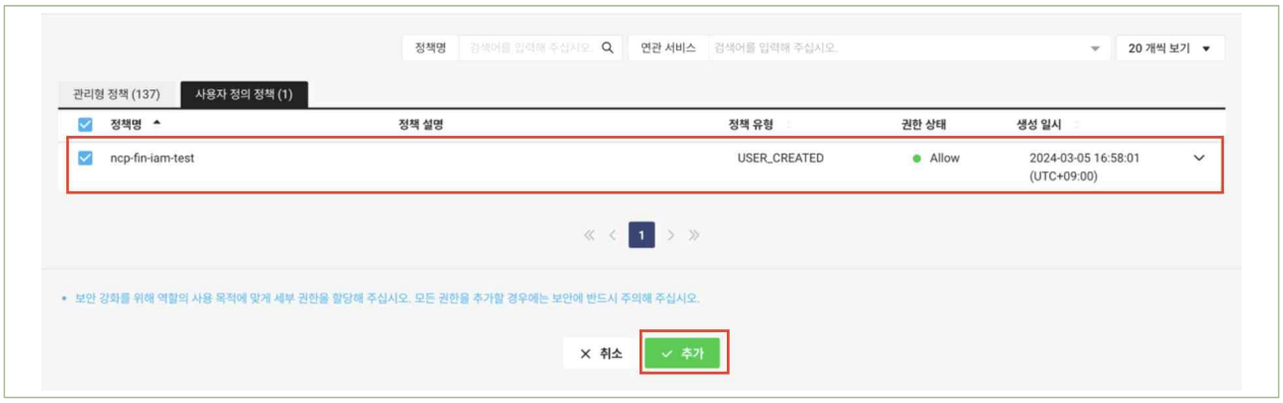
| 그림 8-2-7 | 로그 저장 버킷 선택

④ **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ → ‘Sub Accounts’에서 사용자 정의 정책을 부여할 서브 계정을 선택하고, ‘개별 권한 추가’를 클릭합니다.



| 그림 8-2-8 | 서브 계정 별 개별 권한 추가

⑤ **(가상자원관리시스템)** 정책 추가 단계에서 사전에 정의한 '사용자 정의 정책'을 서브 계정에게 연결합니다.



| 그림 8-2-9 | 사용자 정의 정책 부여 예시

4 참고 사항

- [참고1] Object Storage 이벤트 관리 설정 가이드
- [참고2] Cloud Functions 트리거 설정 가이드

1 기준

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

2 설명

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

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

– 예시

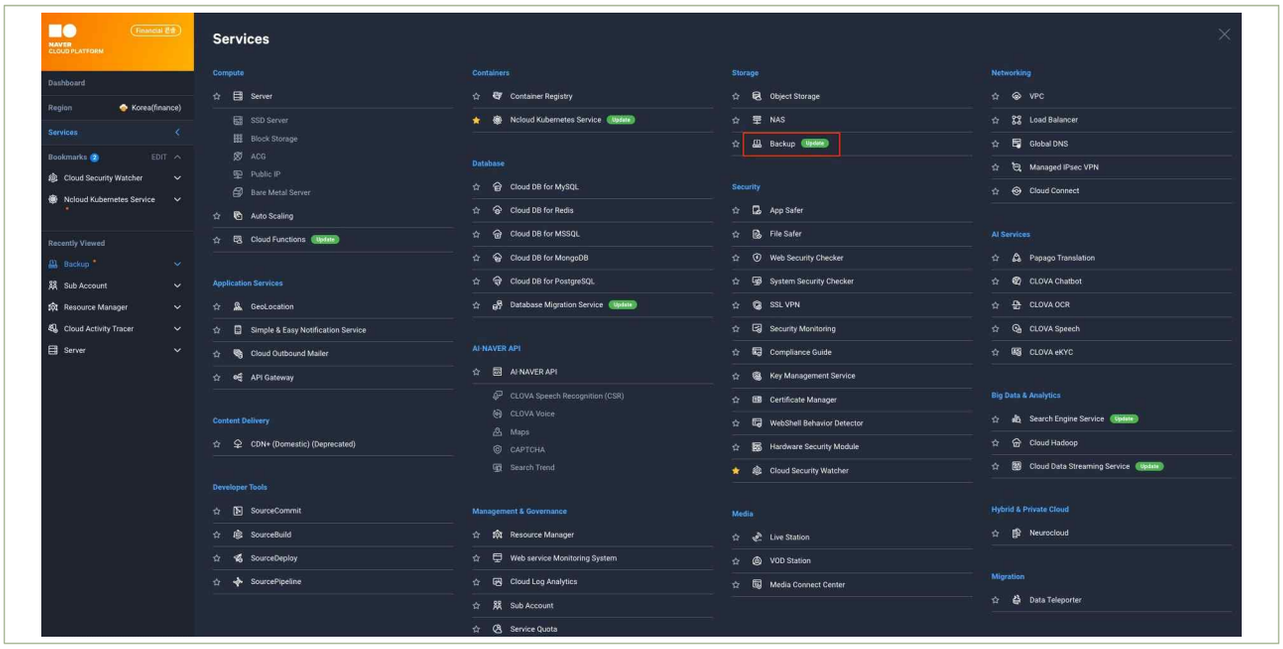
1) 클라우드 서비스 제공자(CSP)의 백업 서비스 이용
2) 전산자료를 별도로 다운받아 금융회사가 관리하는 백업 서버내 보관 등

3 우수 사례

- 네이버 클라우드 플랫폼은 사용자의 가상자원에 대하여 안전하게 데이터를 보존하기 위한 Backup 상품을 제공하고 있습니다. 사용자는 Backup 상품을 이용하여 사용자 정의 정책기반으로 데이터를 쉽고 안전하게 Backup하고 Restore할 수 있습니다.

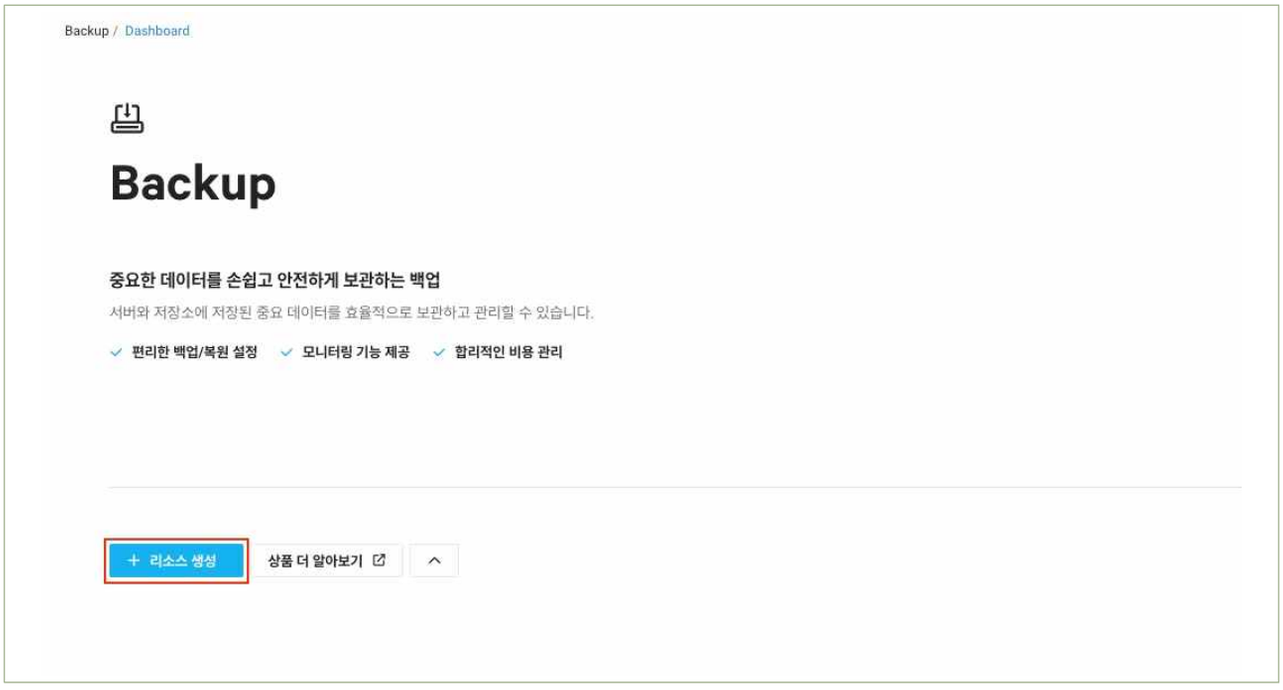
Backup상품을 통한 Server, DBMS의 백업

① **(가상자원관리시스템)** ‘Services’ → ‘Backup’ 상품을 선택합니다.



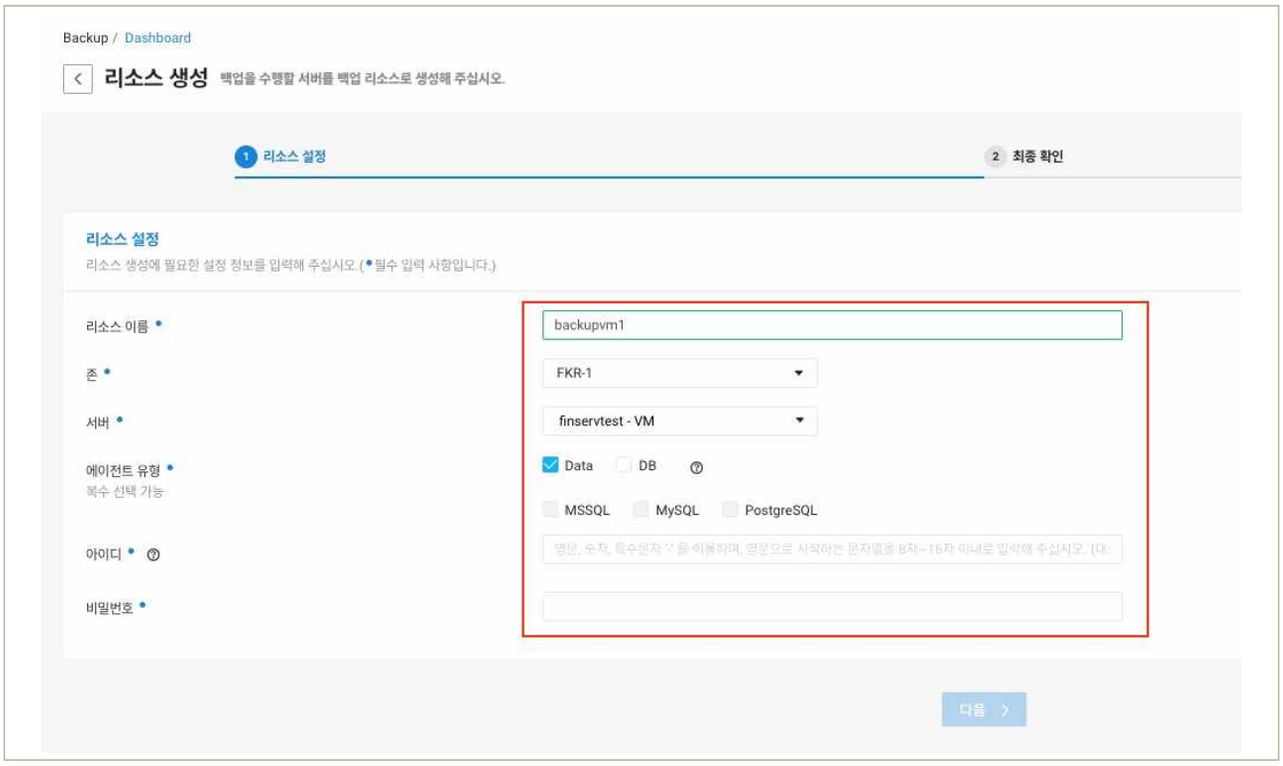
| 그림 8-3-1 | Backup 상품 선택

② **(가상자원관리시스템)** ‘+ 리소스 생성’을 선택합니다.



| 그림 8-3-2 | Backup 리소스 생성 선택

③ **(가상자원관리시스템)** 리소스 이름, 백업 대상의 존과 Server, 에이전트 유형 등을 선택하여 Backup 리소스를 생성합니다.



| 그림 8-3-3 | Backup 리소스 생성

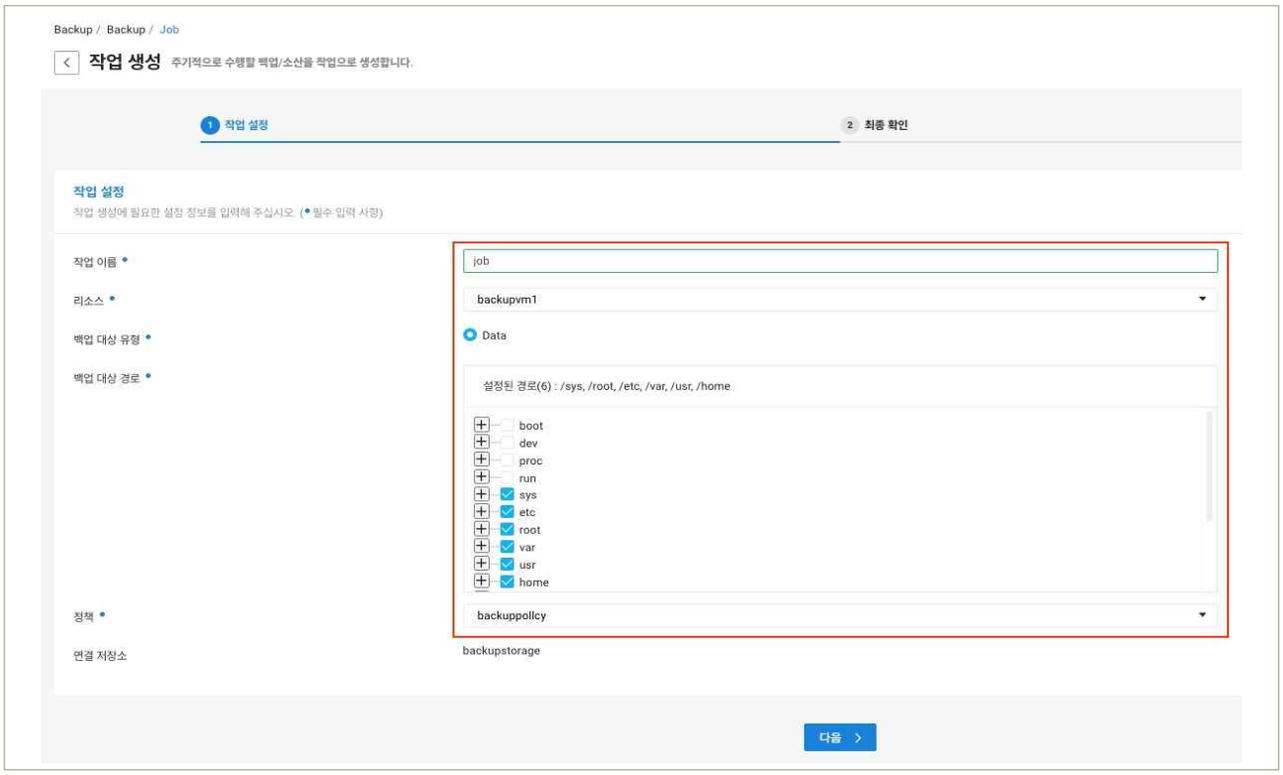
④ **(가상자원관리시스템)** 'Storage' → '+ 저장소 생성'을 선택하여 저장소 이름, 백업 위치 존 정의를 통해 저장소를 생성합니다.

| 그림 8-3-4 | Backup 저장소 생성

⑤ **(가상자원관리시스템)** 'Policy' → '+ 정책 생성'을 선택하여 정책 이름, 보존 기간, 존을 정의하여 Backup 정책을 생성합니다.

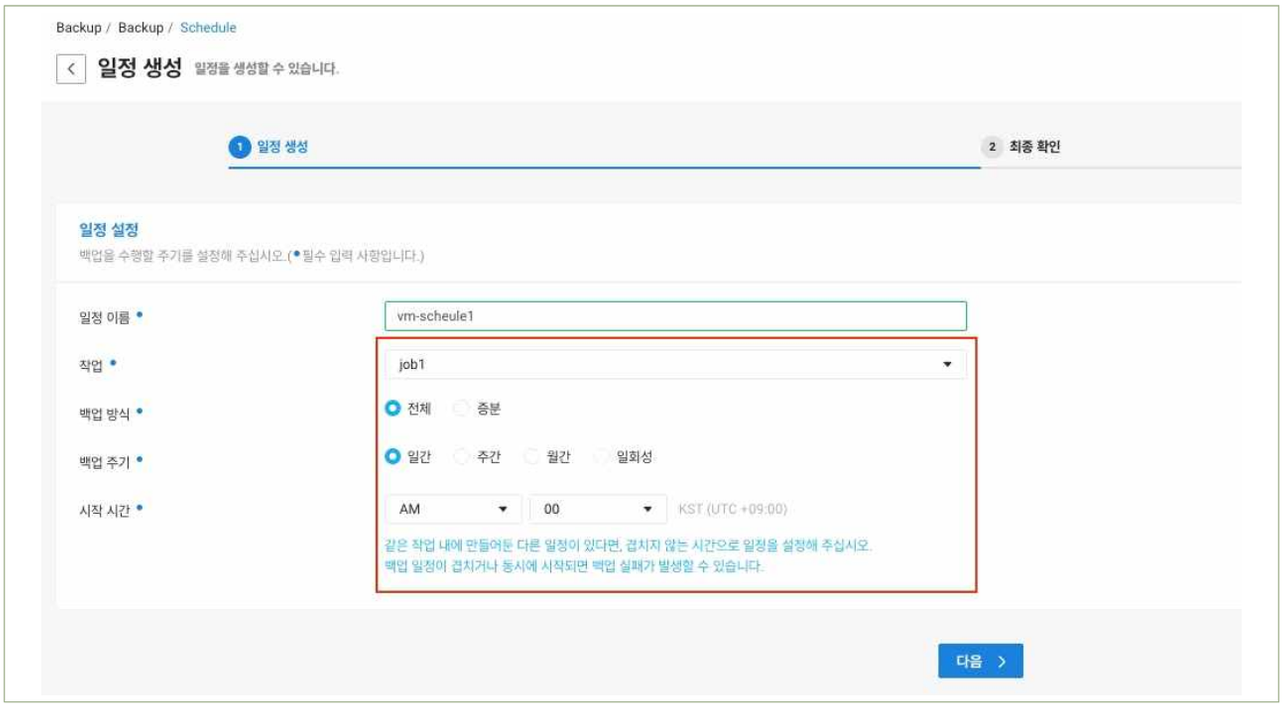
| 그림 8-3-5 | Backup 정책 생성

⑥ **(가상자원관리시스템)** 'Job' → '+ 작업 생성'을 선택하여 작업 이름, 리소스, 백업 대상 유형, 백업 대상 경로를 정의하고 정책을 연결하여 Backup 작업을 생성합니다.



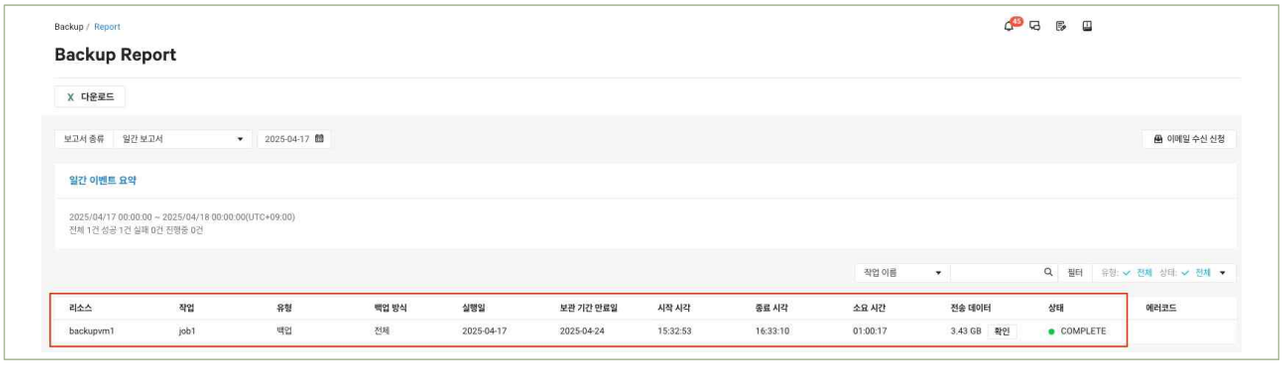
| 그림 8-3-6 | Backup 작업 생성

⑦ **(가상자원관리시스템)** ‘Schedule’ → ‘+ 일정 생성’을 선택하여 일정 이름, 작업, 백업 방식, 백업 주기, 시작 시간을 정의하여 Backup 일정을 생성합니다.



| 그림 8-3-7 | Backup 일정 생성

⑧ **(가상자원관리시스템)** ‘Report’를 선택하여 정의된 Backup 대상, 일정 등에 따라 Backup이 정상적으로 완료되었는지 확인합니다.



| 그림 8-3-8 | Backup 결과 확인

4 참고 사항

- [참고1] Backup 사용자 가이드

1 기준

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

2 설명

- 백업을 통해 보관되고 있는 전산자료에 대해 무결성이 보장되어야 한다.

  - 예시

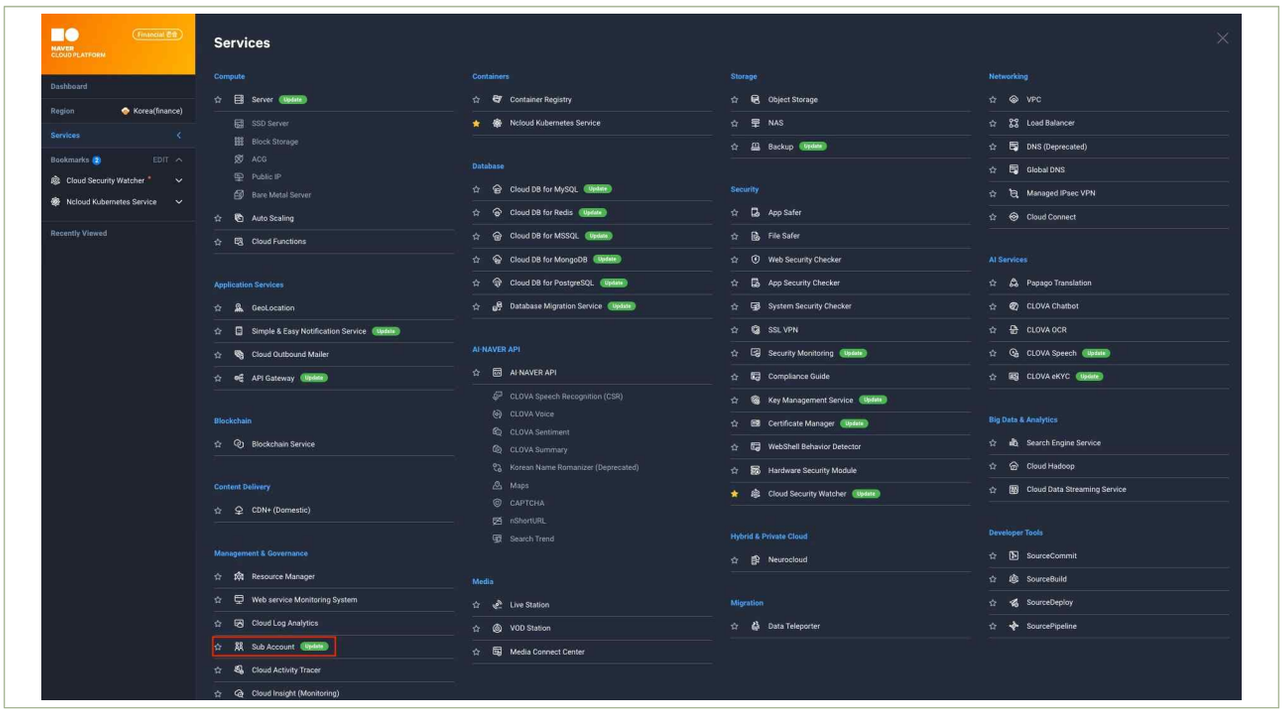
    1) 백업 파일에 대한 접근권한 관리

3 우수 사례

- 네이버 클라우드 플랫폼은 백업 파일에 대한 최소한 접근권한을 적용하여 특정 사용자만 백업파일에 접근할 수 있도록 하여 백업파일의 무결성이 보장될 수 있도록 Sub Account 상품을 통해 상품 접근권한을 관리할 수 있습니다.

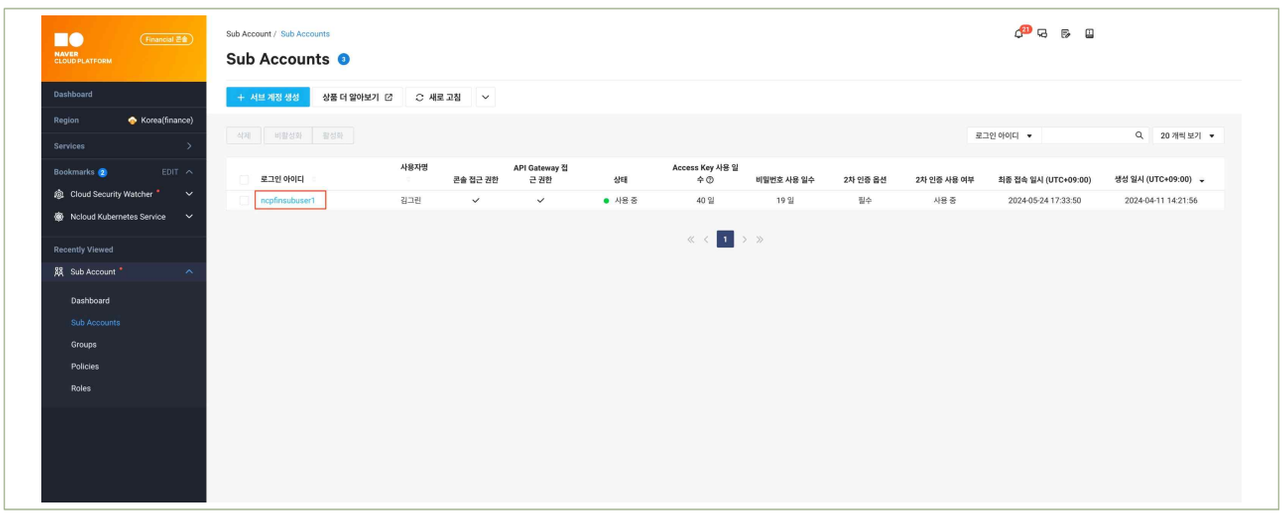
Backup 관리 권한 최소화 설정

① **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ 상품을 선택합니다.



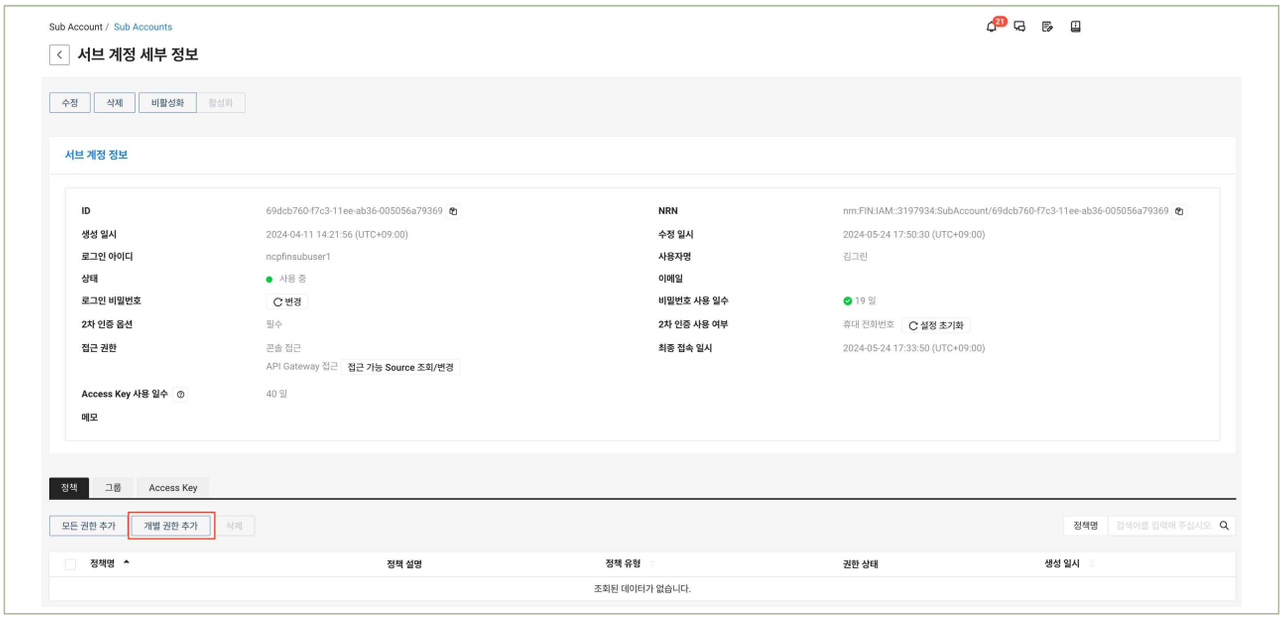
| 그림 8-4-1 | Sub Account 상품 선택

② **(가상자원관리시스템)** 서브계정에 대한 권한 설정을 위해 서브계정(로그인 아이디)를 클릭합니다.



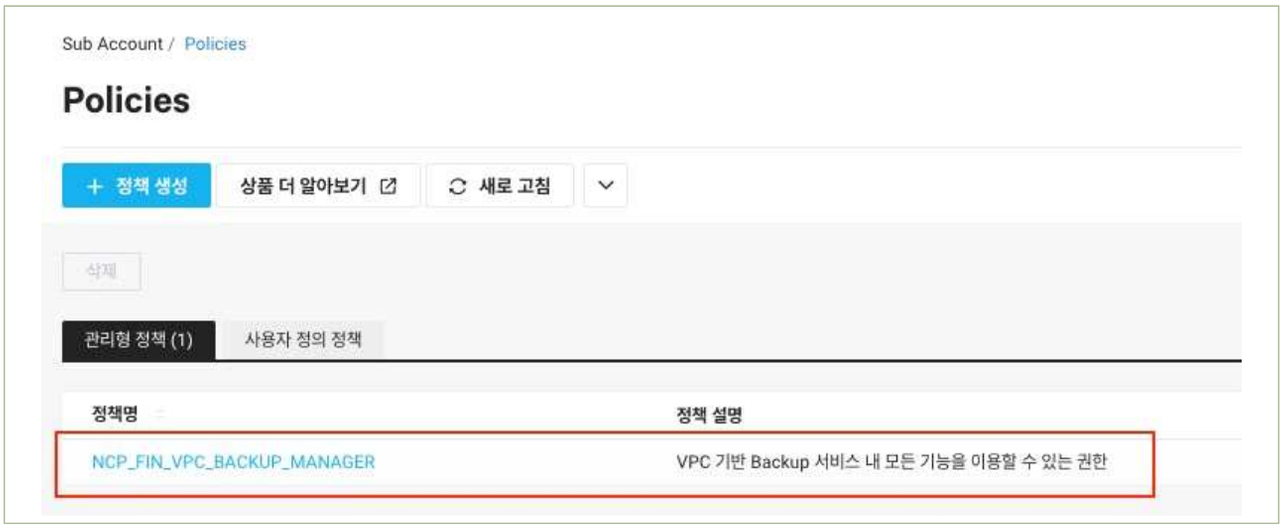
| 그림 8-4-2 | 권한설정을 위한 서브계정 선택

③ **(가상자원관리시스템)** '정책'탭의 '개별 권한 추가' 또는 '그룹' 탭의 '추가'를 통해 사용자 별 개별 권한 또는 권한 그룹을 할당합니다.



| 그림 8-4-3 | 서브계정의 권한 설정

④ **(가상자원관리시스템)** '관리형 정책'탭에서 최소한의 서브 계정에 Backup 상품 관리 권한을 추가합니다.



| 그림 8-4-4 | 서브계정에 Backup 상품 관리 권한 할당

API를 통한 서브계정 정책 할당

① **(API(CLI))** 'sub-accounts' API를 통해 서브계정에 정책을 할당합니다.

- 요청 예시 (API)

```
POST https://subaccount.apigw.fin-ntruss.com/api/v1/sub-accounts/{subAccountId}/policies
```

- 요청 예시 (Body)

```
curl --location --request POST
'https://subaccount.apigw.fin-ntruss.com/api/v1/sub-accounts/2b141960-****-****-****-246e9659184c/polic
ies' \
--header 'x-ncp-apigw-timestamp: {Timestamp}' \
--header 'x-ncp-iam-access-key: {Access Key}' \
--header 'x-ncp-apigw-signature-v2: {API Gateway Signature}' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--data '{
    "policyIdList": [
        "3b773a30-****-****-****-246e96592200",
        "28ab8550-****-****-****-005056a79baa"
    ]
}'
```

- 응답 예시

```
[
    {
        "success": true,
        "id": "28ab8550-****-****-****-005056a79baa",
        "name": "addPolicy"
    }
]
```

| 그림 8-4-5 | 서브계정 정책 할당 예시

4 참고 사항

- [참고1] Sub Account 정책 관리 사용자 가이드
- [참고2] 서브 계정 정책 할당 API 가이드

1 기준

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

2 설명

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

  - 예시

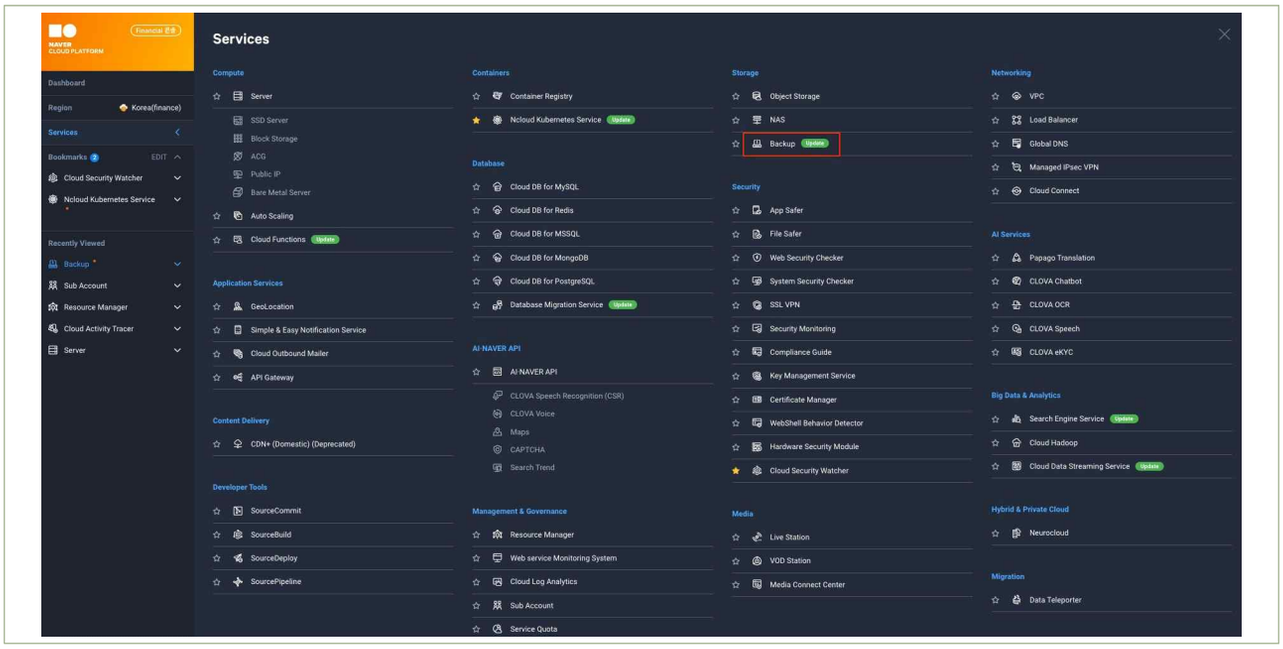
    1) 백업 작업 로그 저장
    2) 백업대상, 백업주기, 백업담당자 등 정책 수립
    3) 정상적인 백업 수행 여부에 대한 모니터링 등

3 우수 사례

- 네이버 클라우드 플랫폼은 사용자가 안전하게 데이터를 보존할 수 있도록 Backup 상품을 통해 백업 대상, 주기 등을 정의하고 백업 결과 로그를 통해 백업 정상 완료 여부에 대해서 모니터링을 수행할 수 있습니다. 또한, Sub Account 상품을 통해 Backup 상품에 접근 가능한 백업담당자를 지정하여 백업파일을 안전하게 관리할 수 있습니다.

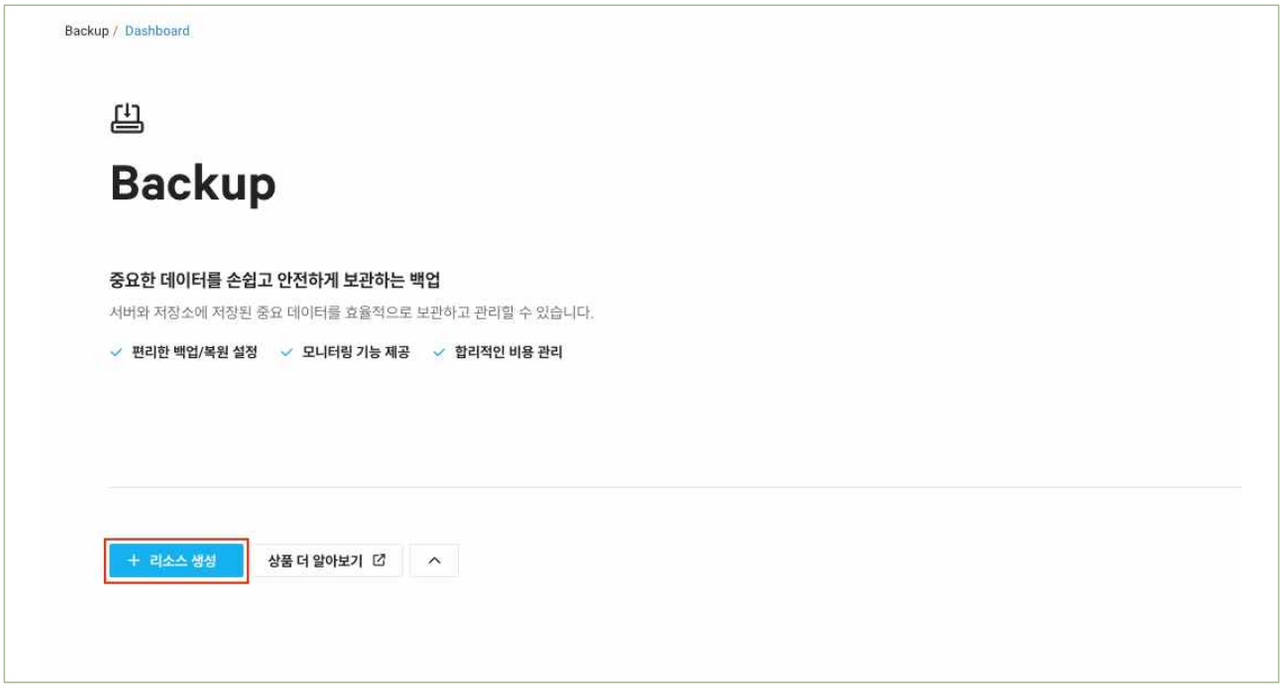
Backup상품을 통한 Server, DBMS의 백업

① **(가상자원관리시스템)** ‘Services’ → ‘Backup’ 상품을 선택합니다.



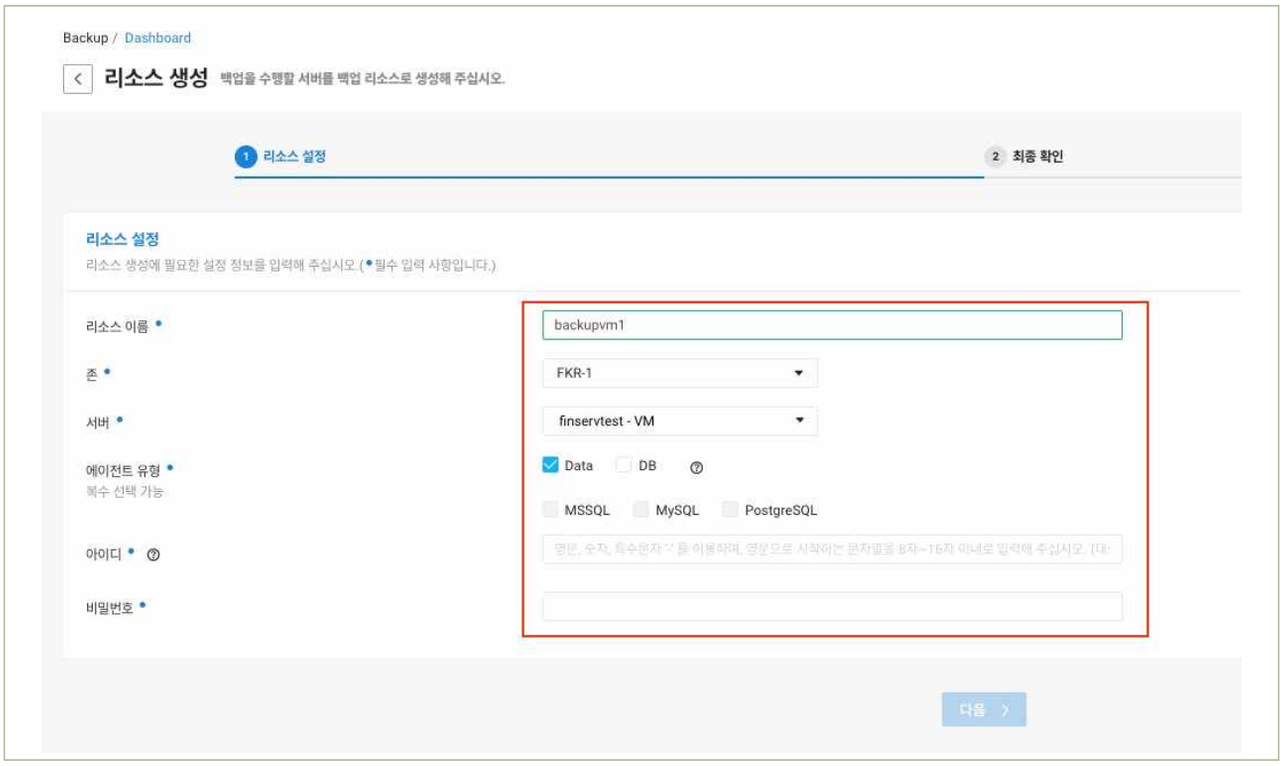
| 그림 8-5-1 | Backup 상품 선택

② **(가상자원관리시스템)** ‘+ 리소스 생성’을 선택합니다.



| 그림 8-5-2 | Backup 리소스 생성 선택

③ **(가상자원관리시스템)** 리소스 이름, 백업 대상의 존과 Server, 에이전트 유형 등을 선택하여 Backup 리소스를 생성합니다.



| 그림 8-5-3 | Backup 리소스 생성

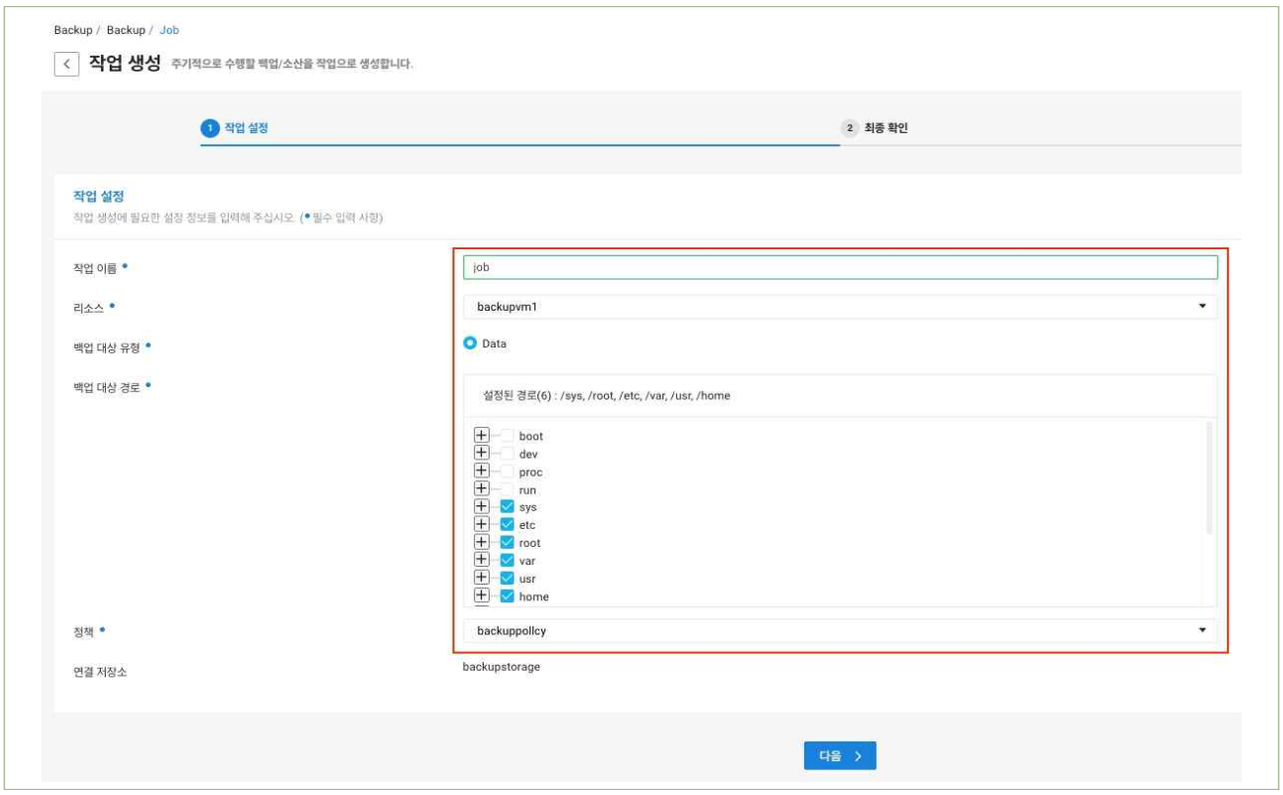
④ **(가상자원관리시스템)** 'Storage' → '+ 저장소 생성'을 선택하여 저장소 이름, 백업 위치 존 정의를 통해 저장소를 생성합니다.

| 그림 8-5-4 | Backup 저장소 생성

⑤ **(가상자원관리시스템)** 'Policy' → '+ 정책 생성'을 선택하여 정책 이름, 보존 기간, 존을 정의하여 Backup 정책을 생성합니다.

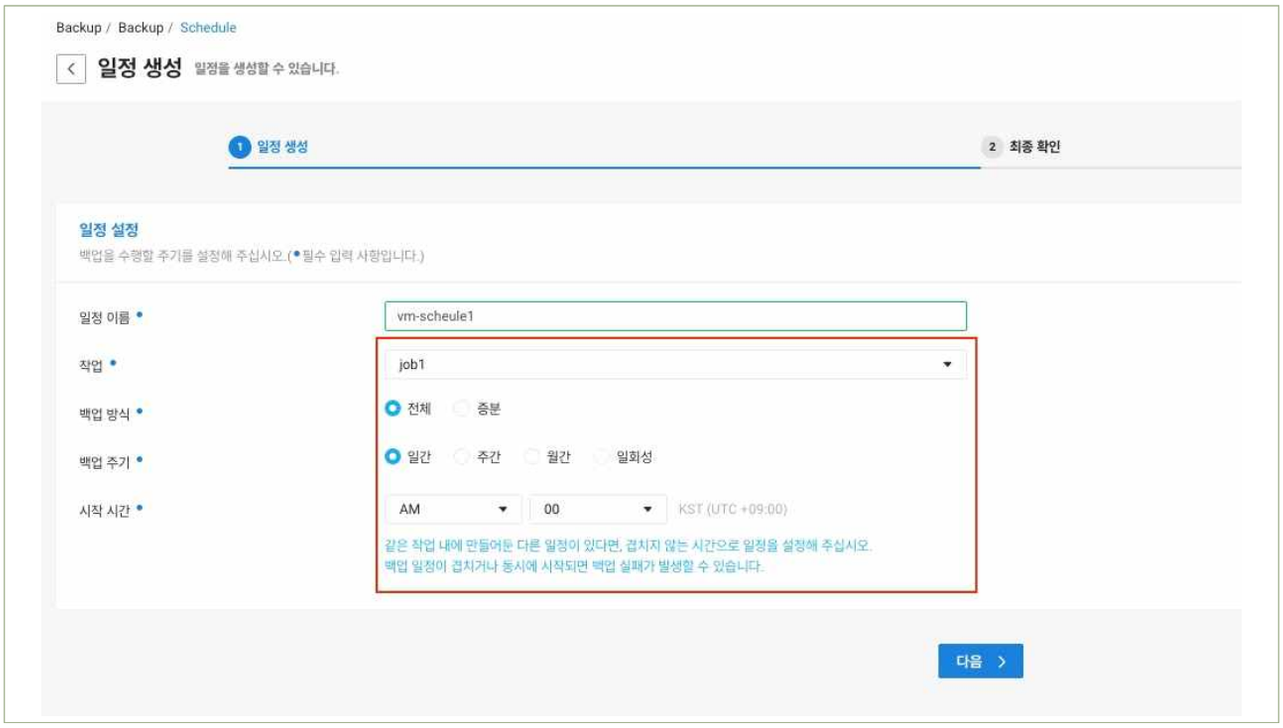
| 그림 8-5-5 | Backup 정책 생성

⑥ **(가상자원관리시스템)** 'Job' → '+ 작업 생성'을 선택하여 작업 이름, 리소스, 백업 대상 유형, 백업 대상 경로를 정의하고 정책을 연결하여 Backup 작업을 생성합니다.



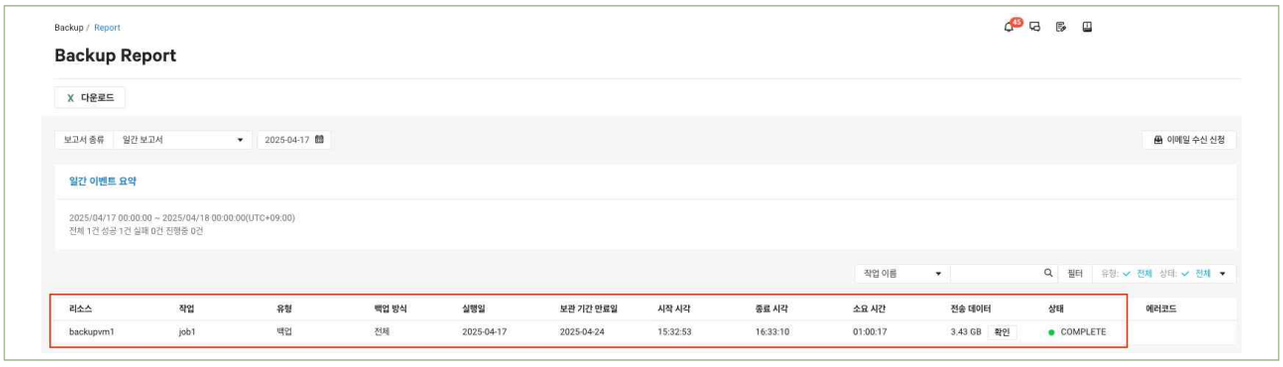
| 그림 8-5-6 | Backup 작업 생성

⑦ **(가상자원관리시스템)** ‘Schedule’ → ‘+ 일정 생성’을 선택하여 일정 이름, 작업, 백업 방식, 백업 주기, 시작 시간을 정의하여 Backup 일정을 생성합니다.



| 그림 8-5-7 | Backup 일정 생성

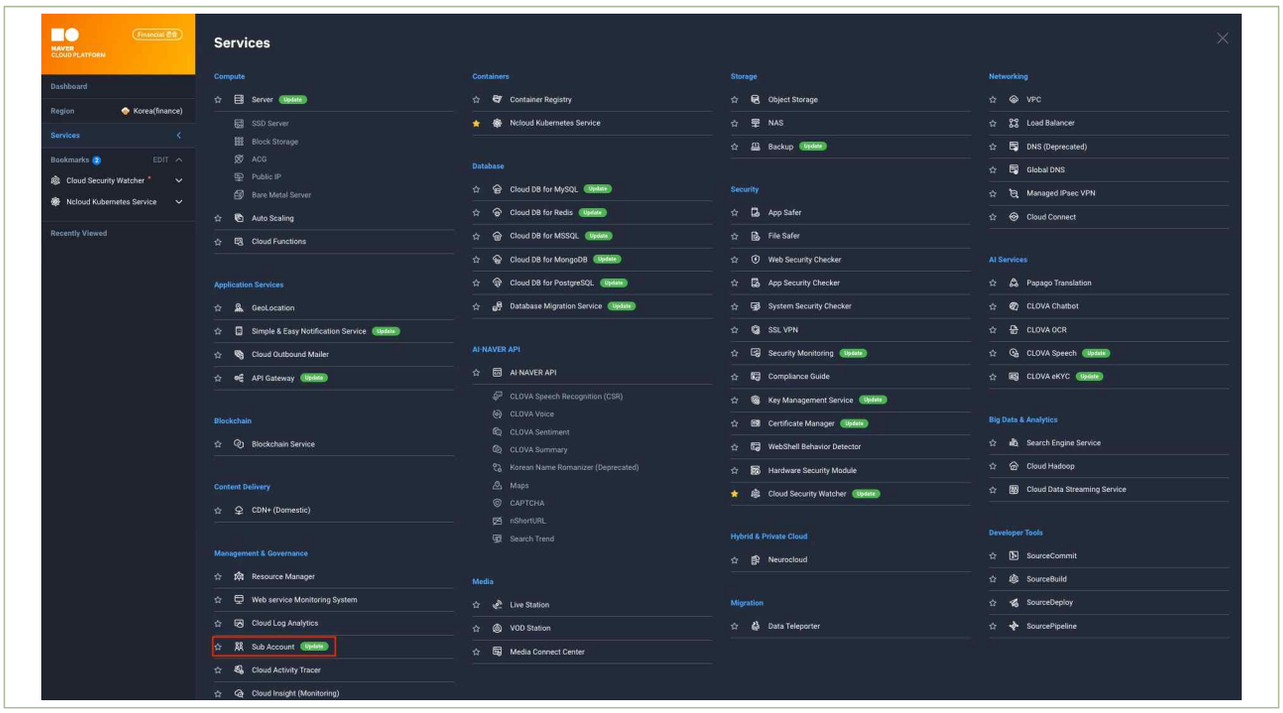
⑧ **(가상자원관리시스템)** ‘Report’를 선택하여 정의된 Backup 대상, 일정 등에 따라 Backup이 정상적으로 완료되었는지 확인합니다.



| 그림 8-5-8 | Backup 결과 확인

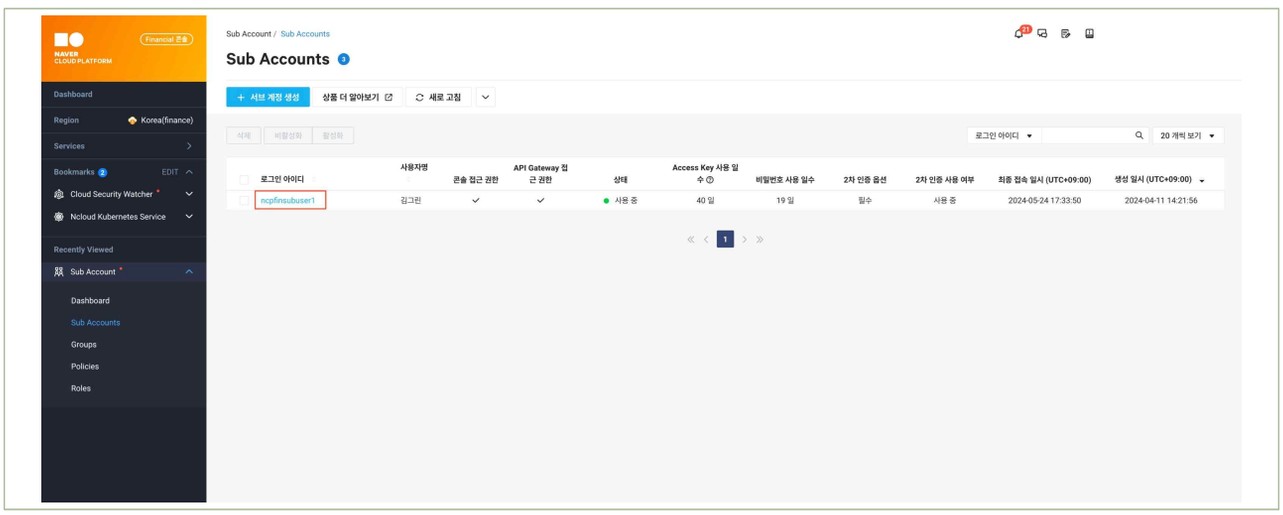
Backup 관리 권한 최소화 설정

① **(가상자원관리시스템)** ‘Services’ → ‘Sub Account’ 상품을 선택합니다.



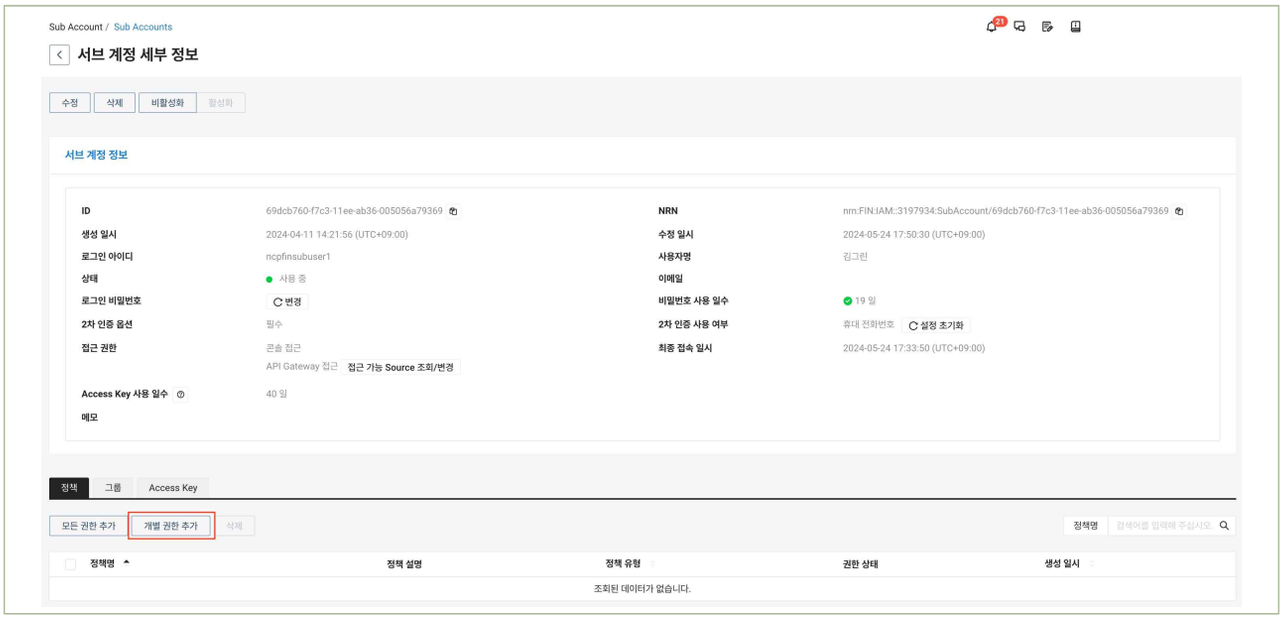
| 그림 8-5-9 | Sub Account 상품 선택

② **(가상자원관리시스템)** 서브계정에 대한 권한 설정을 위해 서브계정(로그인 아이디)를 클릭합니다.



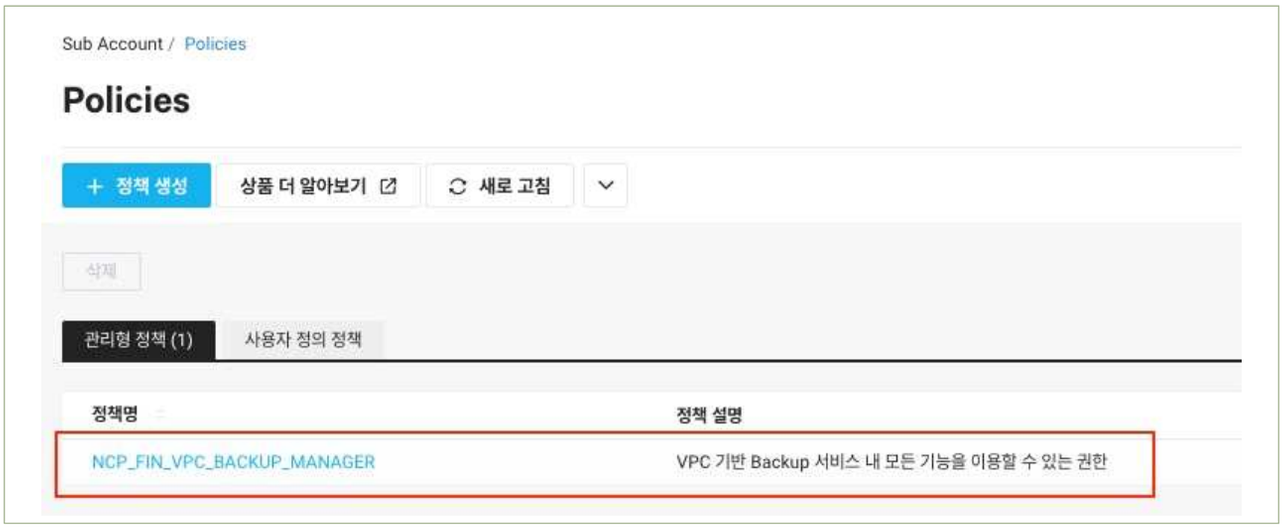
| 그림 8-5-10 | 권한설정을 위한 서브계정 선택

③ **(가상자원관리시스템)** '정책'탭의 '개별 권한 추가' 또는 '그룹' 탭의 '추가'를 통해 사용자 별 개별 권한 또는 권한 그룹을 할당합니다.



| 그림 8-5-11 | 서브계정의 권한 설정

④ **(가상자원관리시스템)** '관리형 정책'탭에서 최소한의 서브 계정에 Backup 상품 관리 권한을 추가합니다.



| 그림 8-5-12 | 서브계정에 Backup 상품 관리 권한 할당

API를 통한 서브계정 정책 할당

① **(API(CLI))** 'sub-accounts' API를 통해 서브계정에 정책을 할당합니다.

- 요청 예시 (API)

```
POST https://subaccount.apigw.fin-ntruss.com/api/v1/sub-accounts/{subAccountId}/policies
```

- 요청 예시 (Body)

```
curl --location --request POST
'https://subaccount.apigw.fin-ntruss.com/api/v1/sub-accounts/2b141960-****-****-****-246e9659184c/polic
ies' \
--header 'x-ncp-apigw-timestamp: {Timestamp}' \
--header 'x-ncp-iam-access-key: {Access Key}' \
--header 'x-ncp-apigw-signature-v2: {API Gateway Signature}' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--data '{
    "policyIdList": [
        "3b773a30-****-****-****-246e96592200",
        "28ab8550-****-****-****-005056a79baa"
    ]
}'
```

- 응답 예시

```
[
    {
        "success": true,
        "id": "28ab8550-****-****-****-005056a79baa",
        "name": "addPolicy"
    }
]
```

| 그림 8-5-13 | 서브계정 정책 할당 예시

4 참고 사항

- [참고1] Backup 사용자 가이드
- [참고2] Sub Account 정책 관리 사용자 가이드
- [참고3] 서브 계정 정책 할당 API 가이드

1 기준

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

2 설명

- 중요한 금융회사 전산자료는 보안이 강화된 원격 저장소에 보관하여야 한다.

  - 예시

    1) 클라우드 서비스 제공자(CSP)의 DR 서비스 이용

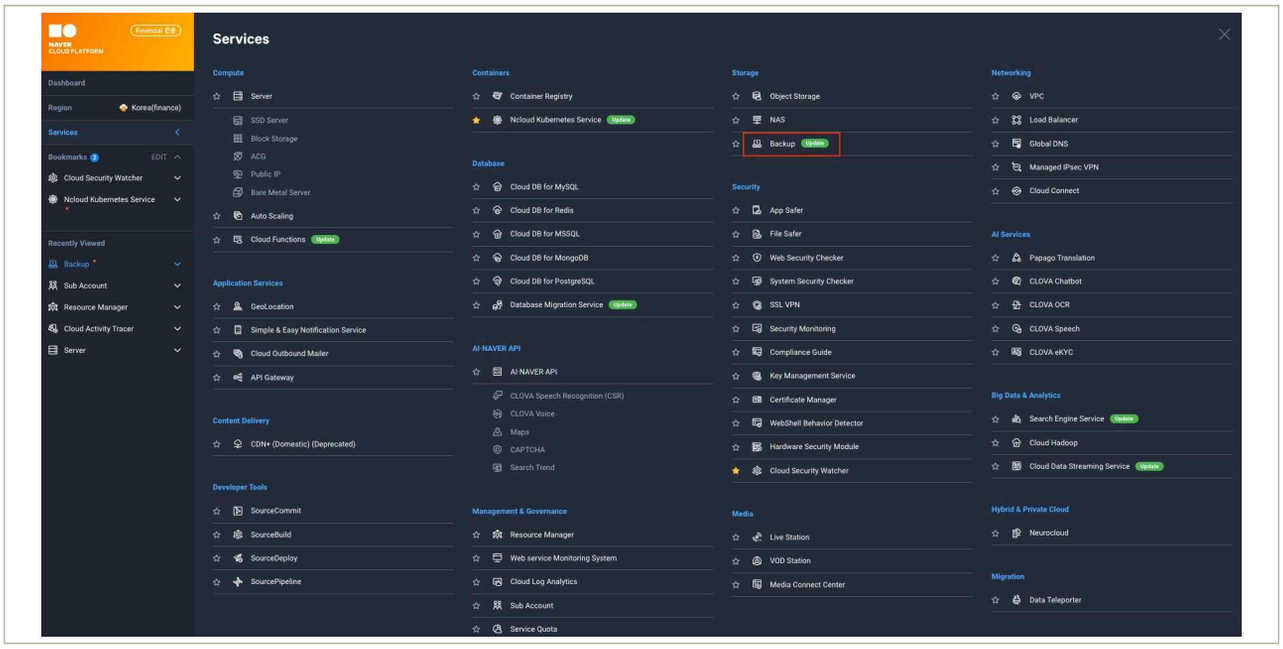
    2) 금융회사 자체 데이터센터로 소산하여 보관 등

3 우수 사례

- 네이버 클라우드 플랫폼은 사용자가 Backup 데이터를 안전한 지역에 소산하여 보존할 수 있도록 Remote Backup을 제공합니다. 사용자는 Remote Backup상품을 이용하여 Server, DBMS 등 가상자원이 위치한 존과 별도의 존에 저장소를 구성하고, 사용자 정의에 따라 소산 백업 대상, 일정, 보존 기간 등을 정의하여 Remote Backup을 구성할 수 있습니다.

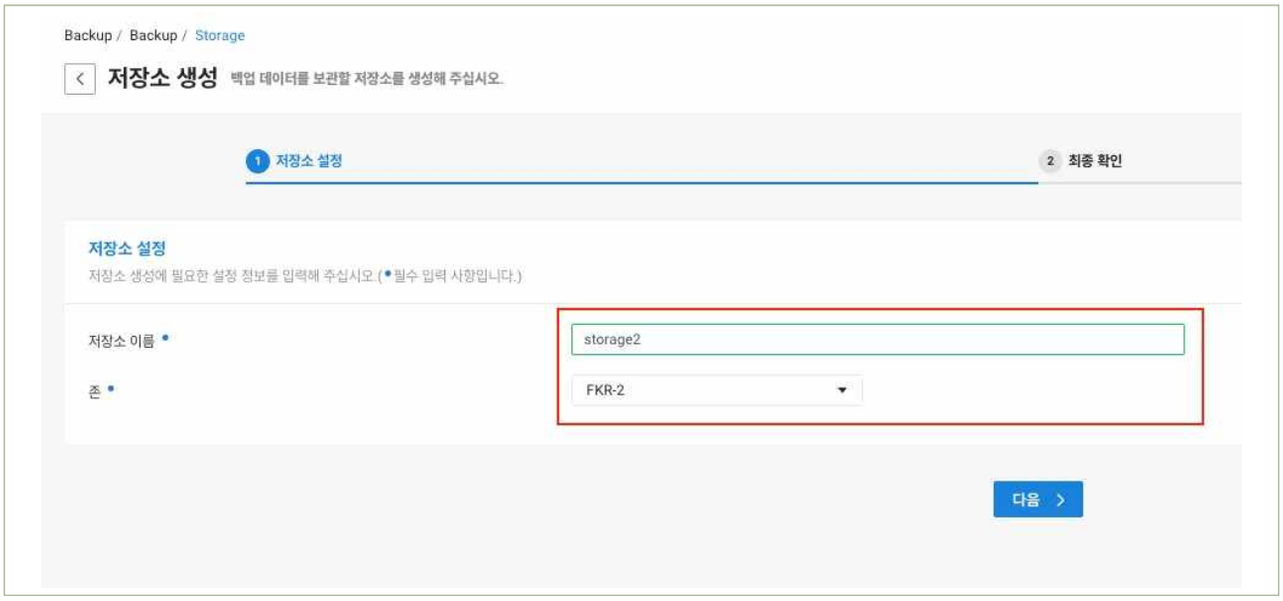
Backup상품을 통한 소산 백업

① **(가상자원관리시스템)** ‘Services’ → ‘Backup’ 상품을 선택합니다.



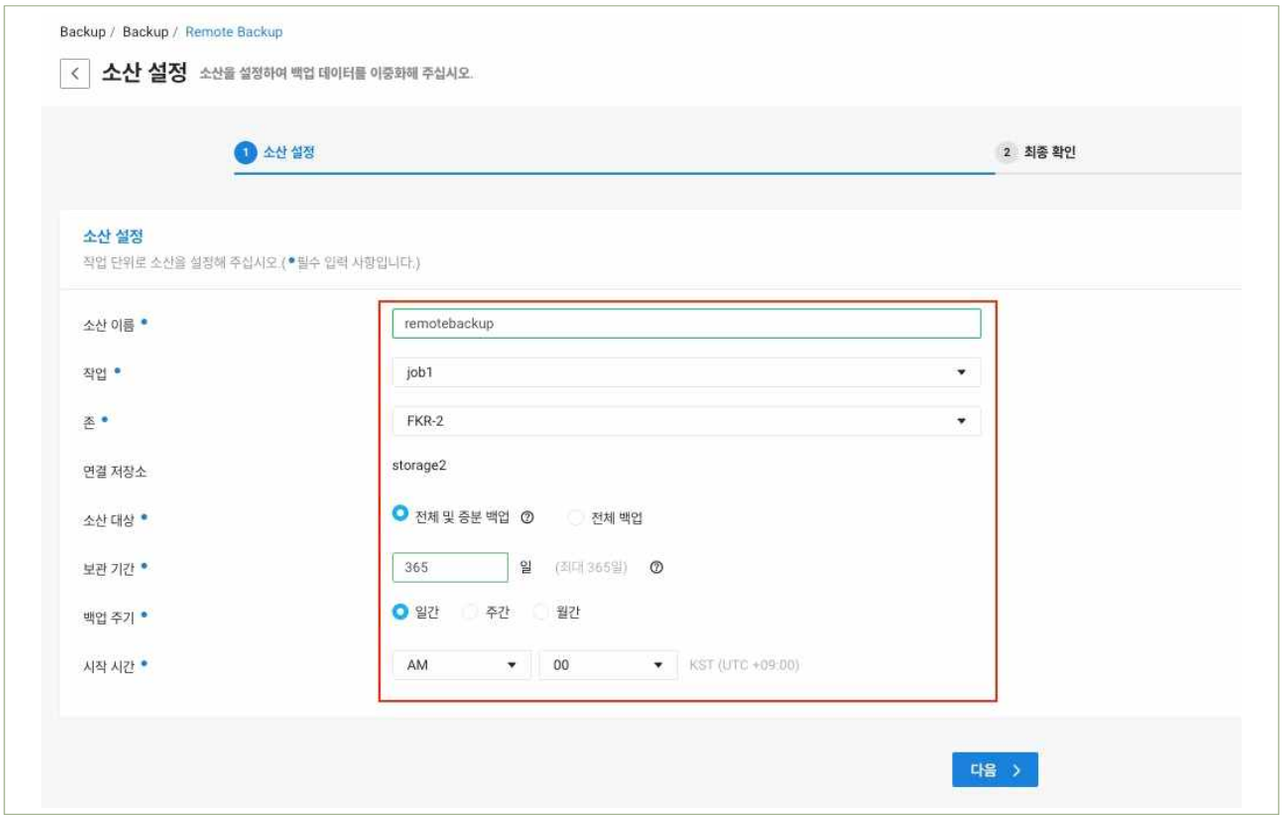
| 그림 8-6-1 | Backup 상품 선택

② **(가상자원관리시스템)** ‘Storage’ → ‘+ 저장소 생성’을 선택하고 Server, DBMS 등이 존재하는 존과 다른 존(소산 백업 장소)에 저장소를 생성합니다.



| 그림 8-6-2 | 소산 백업 저장소 생성

③ **(가상자원관리시스템)** 'Remote Backup' → '+ 소산 설정'을 선택하고 소산을 수행할 작업, 존을 선택하면 연결 저장소(소산 백업 장소)가 지정되며, 소산 대상, 보존 기간, 백업 주기, 백업 시간 등을 정의하여 소산 설정을 완료합니다.



| 그림 8-6-3 | 소산 백업 설정

4 참고 사항

- [참고1] Remote Backup 설정 사용자 가이드

1 기준

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

2 설명

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

  - 예시

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

    2) 이중화 구성 시 원격 안전지역 등을 고려

3 우수 사례

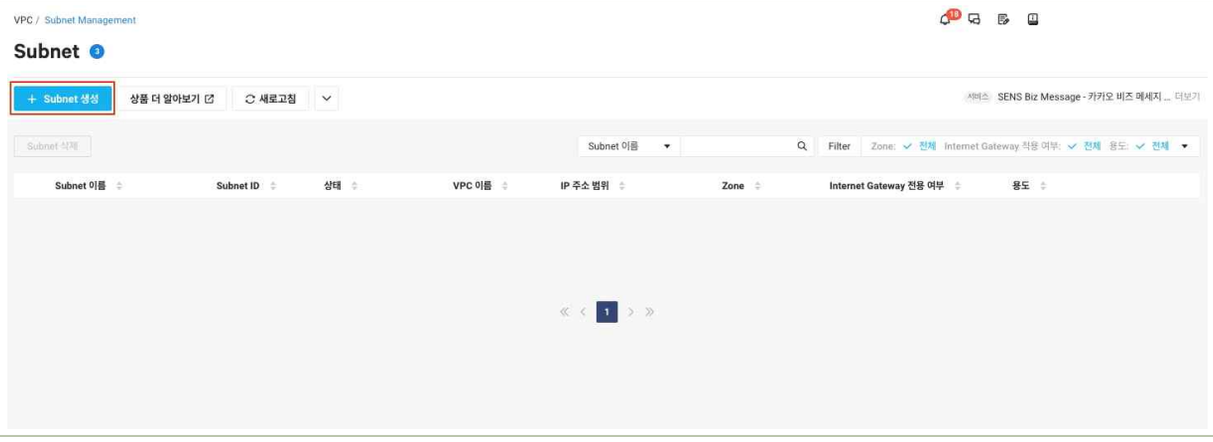
- 네이버 클라우드 플랫폼은 사용자의 가상자원(Server, Cloud DB 등)이 안전하게 가용성을 유지할 수 있도록 이중화(Multi Zone) 구성을 지원합니다. Zone은 금융 클라우드 Region 내에 물리적으로 분리되어 구성된 데이터센터 및 네트워크를 말하며, 사용자는 각각의 Server와 Cloud DB 가상자원을 서로 다른 Zone에 구성하여 하나의 Zone에 가용성에 문제가 발생하더라도 다른 Zone의 가상자원은 정상적인 서비스가 될 수 있도록 이중화 구성을 적용할 수 있습니다.

Multi Zone 구성을 위한 Subnet 생성

① **(가상자원관리시스템)** ‘Services’ → ‘VPC’ 상품을 선택합니다.

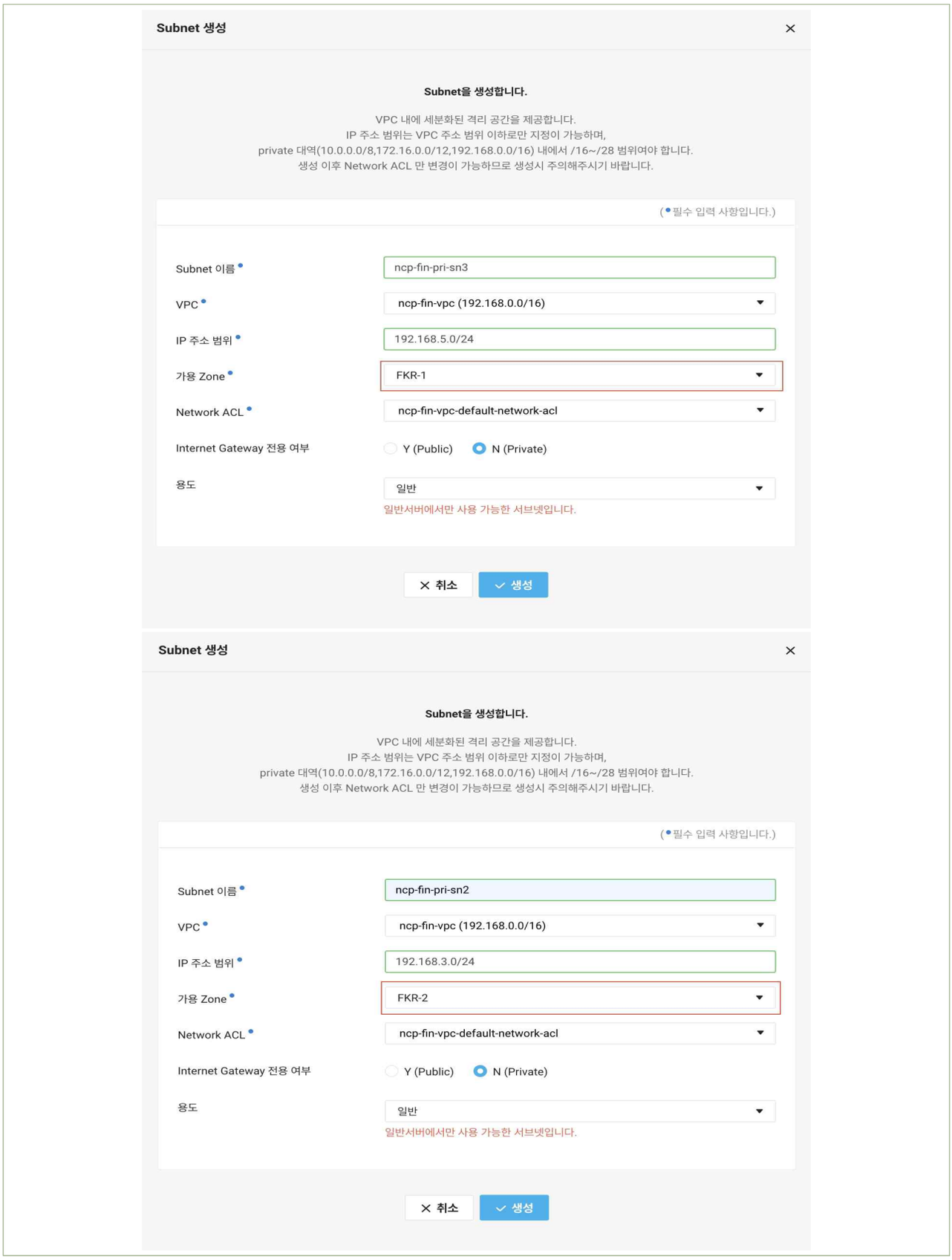
| 그림 8-7-1 | VPC 상품 선택

② **(가상자원관리시스템)** ‘Subnet Management’ → ‘+ Subnet 생성’을 선택합니다.



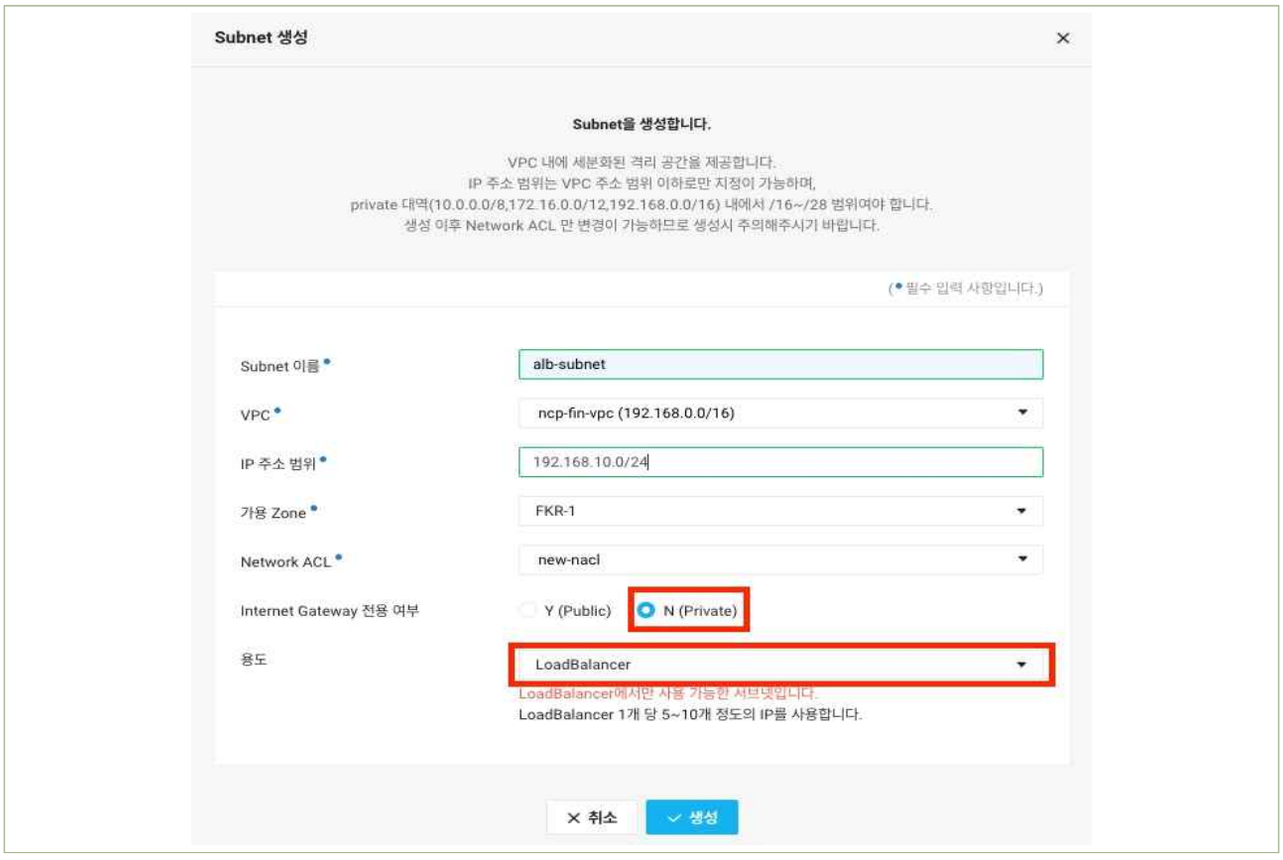
| 그림 8-7-2 | Subnet 관리 콘솔

③ **(가상자원관리시스템)** '가용 Zone' 이 서로 다른 Subnet을 2개 생성합니다.



| 그림 8-7-3 | Zone 별 Subnet 생성 예시

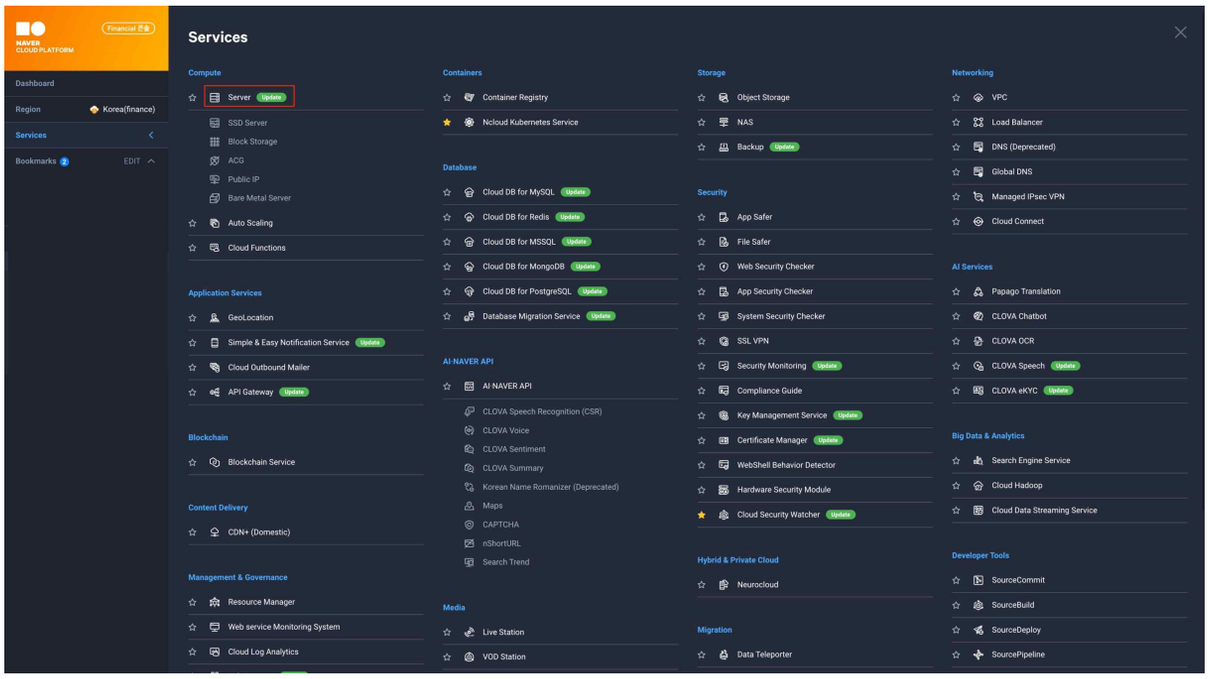
④ **(가상자원관리시스템)** 위와 동일한 방법을 통해 2대의 Server를 연결할 Application Load Balancer를 구성할 신규 Private Subnet을 생성합니다.



| 그림 8-7-4 | Application Load Balancer Subnet 생성 예시

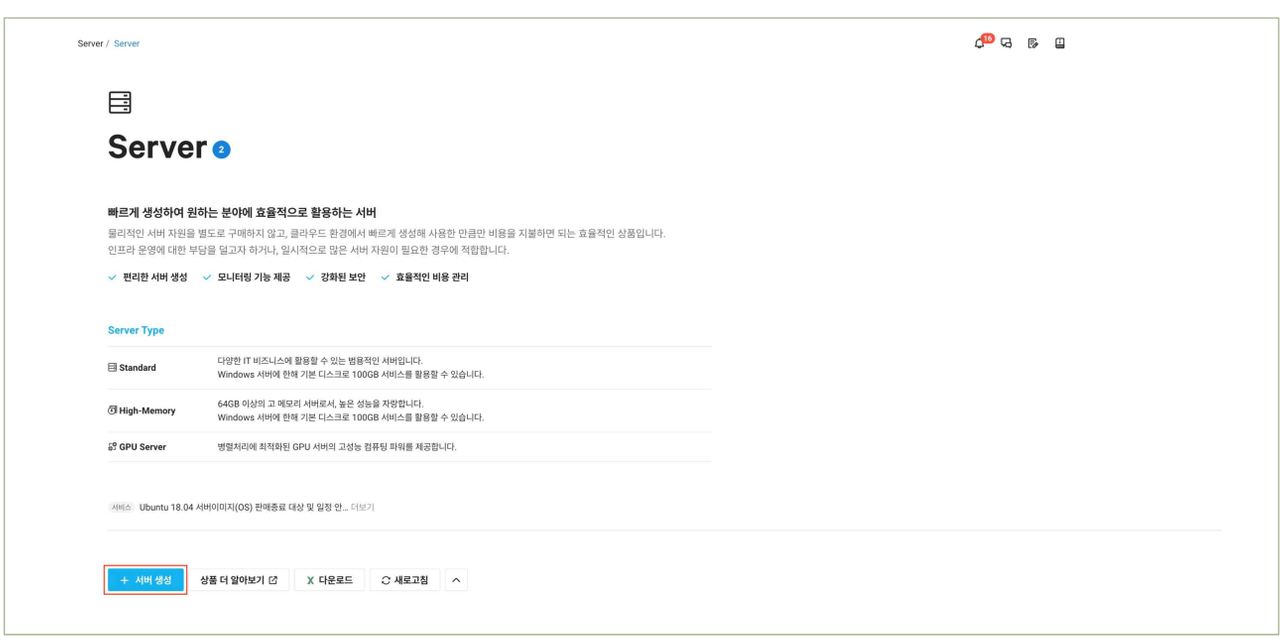
Server의 이중화(Multi Zone) 구성

① **(가상자원관리시스템)** ‘Services’ → ‘Server’ 상품을 선택합니다.



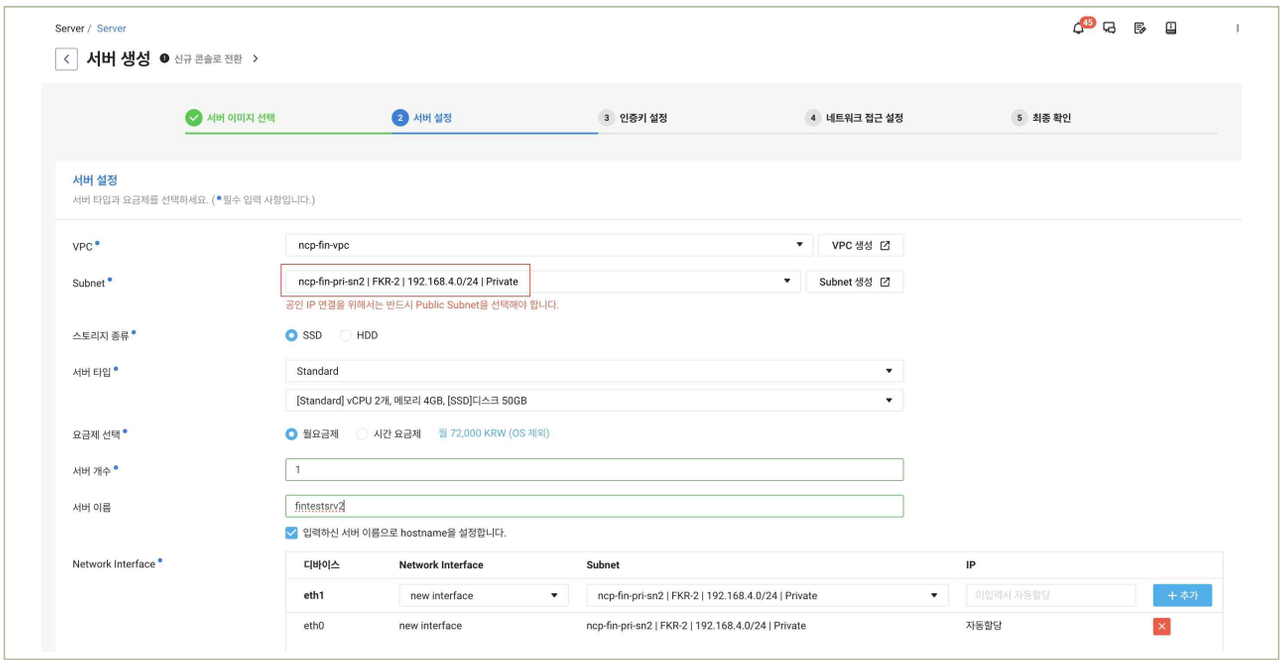
| 그림 8-7-5 | Server 상품 선택

② **(가상자원관리시스템)** ‘Server’ → ‘+ 서버 생성’을 클릭하여 가상자원(Server)를 생성합니다.



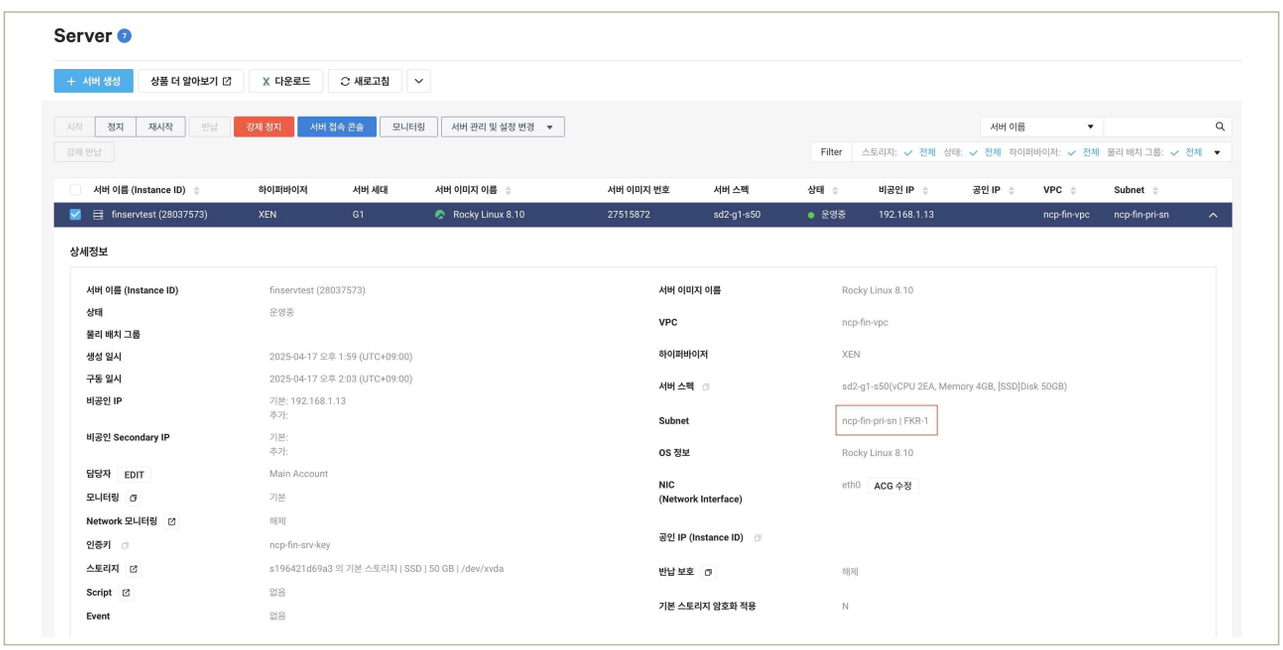
| 그림 8-7-6 | Server 생성

③ **(가상자원관리시스템)** Server 생성 과정에서 이중화 구성을 위해 각 서버가 서로 다른 Subnet과 Zone에 위치하도록 Subnet을 선택하여 Server 2대 생성합니다.



| 그림 8-7-7 | Server 이중화 구성 예시

④ **(가상자원관리시스템)** 2대의 Server 가 Server 목록의 상세 정보에서 Subnet이 서로 다른 위치로 구성되어 있는지 확인합니다.

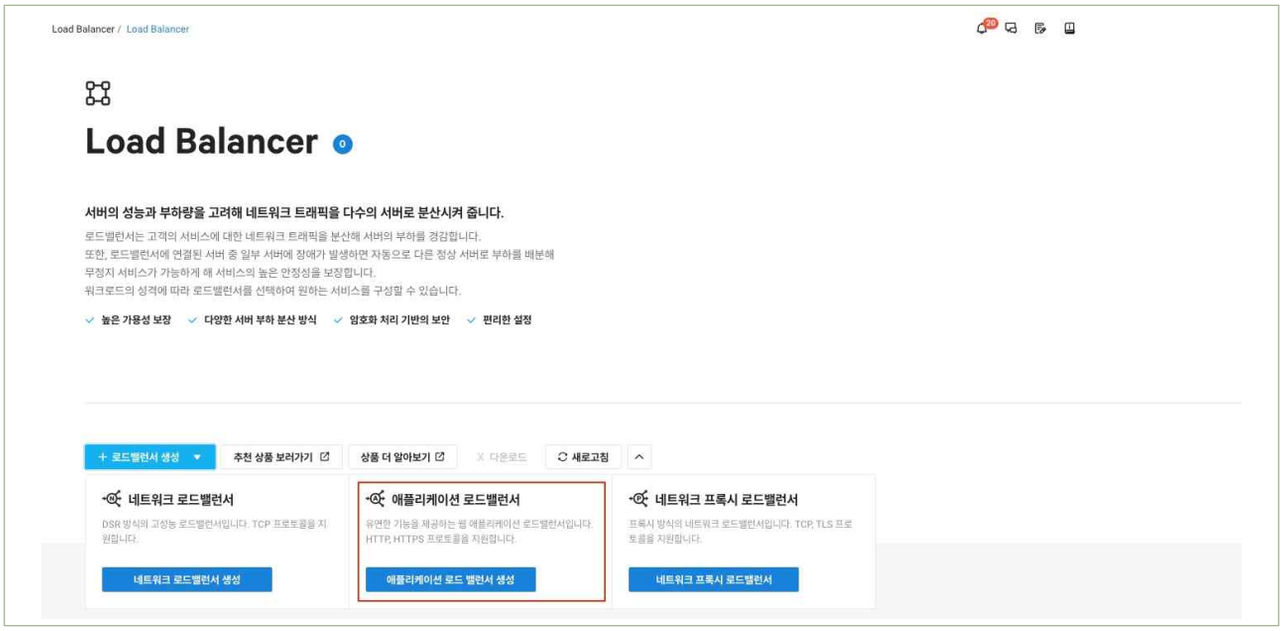


| 그림 8-7-8 | Server 이중화 구성 확인

⑤ **(가상자원관리시스템)** 2대의 Server를 연결하기 위한 Application Load Balancer를 생성하기 위해 'Services' → 'Load Balancer' 상품을 선택합니다.

| 그림 8-7-9 | Load Balancer 상품 선택

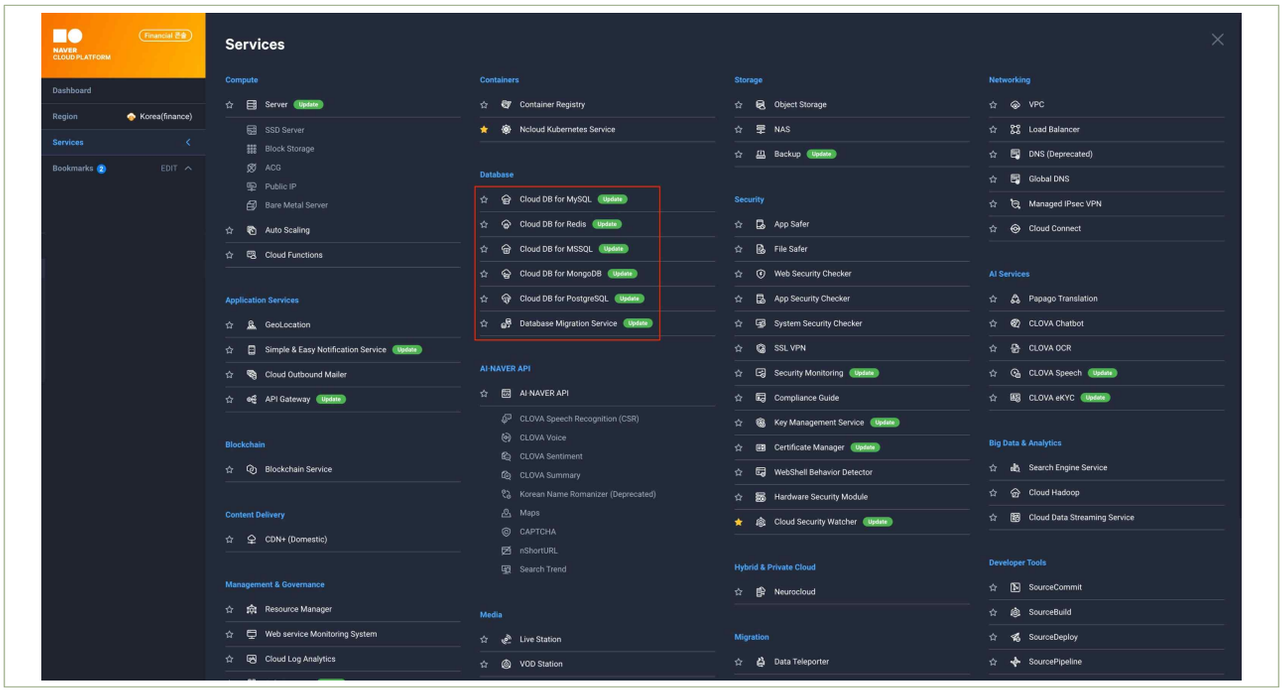
⑥ **(가상자원관리시스템)** '+ 로드밸런서 생성' → '애플리케이션 로드 밸런서 생성'을 클릭하여 2대의 Server Target을 연결합니다. Application Load Balancer에 연결된 2대의 Server들은 서로 다른 Zone에 위치하므로, 특정 Zone에 문제가 발생하더라도 서비스 연속성을 유지할 수 있습니다.



| 그림 8-7-10 | Application Load Balancer 생성

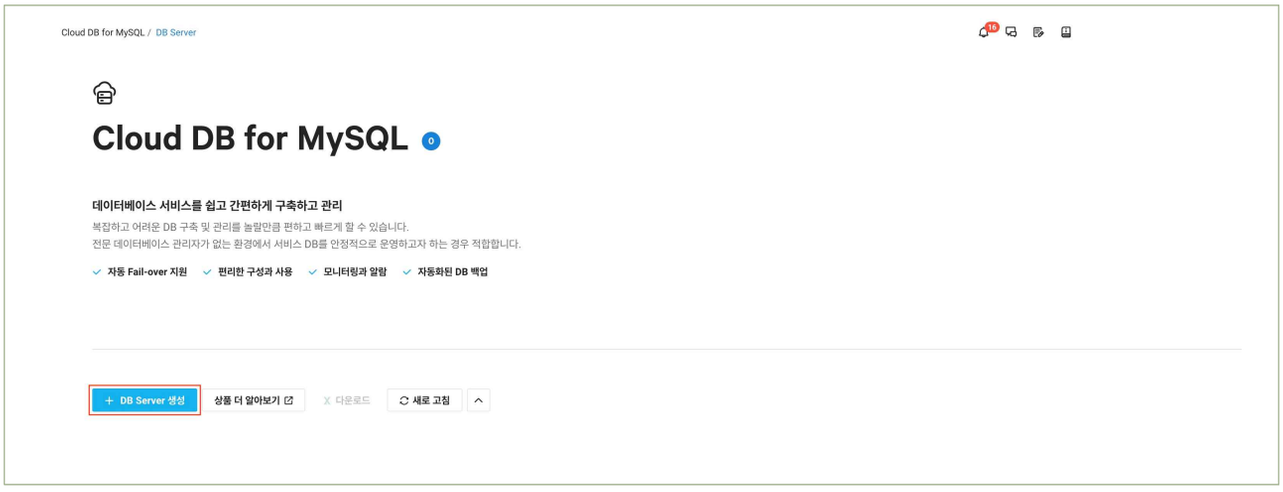
Cloud DB의 이중화(Multi Zone) 구성

① **(가상자원관리시스템)** ‘Services’ → ‘Cloud DB’ 상품을 선택합니다.



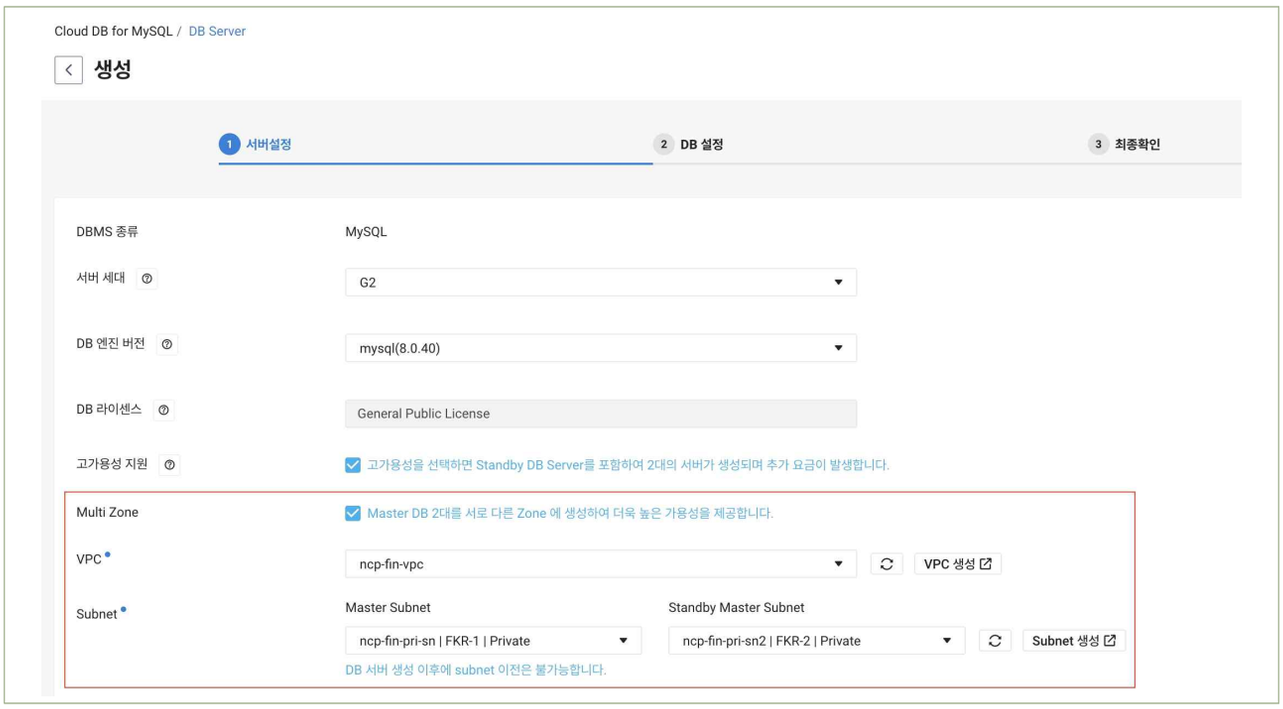
| 그림 8-7-11 | Cloud DB 상품 선택

② **(가상자원관리시스템)** ‘DB Server’ → ‘+DB Server 생성’을 클릭하여 가상자원(Cloud DB)을 생성합니다.



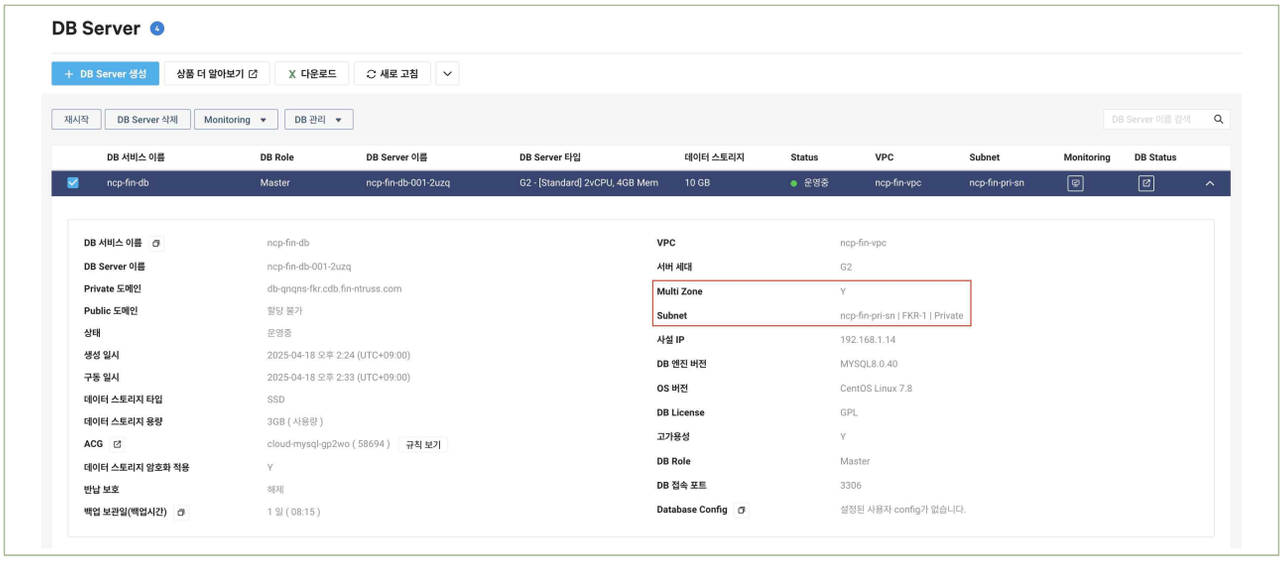
| 그림 8-7-12 | Cloud DB 신규 생성

③ **(가상자원관리시스템)** Cloud DB 생성 과정에서 Multi Zone 구성을 선택하여 Cloud DB를 생성합니다.



| 그림 8-7-13 | Cloud DB의 이중화 구성

④ **(가상자원관리시스템)** Cloud DB 목록의 상세 정보에서 Cloud DB의 Multi Zone 값이 'Y'이고, Master Server와 Standby Server의 Subnet 값에 Zone이 서로 다르게 구성되어 있는지 확인합니다.



| 그림 8-7-14 | Cloud DB의 이중화 구성 확인

API를 통한 Server 이중화(Multi Zone) 구성

① **(API(CLI))** 'createServerInstances' API를 통해 Server 생성 시, 'subnetNo' 파라미터를 통해 2대의 Server를 서로 다른 Subnet에 구성합니다.

- 요청 예시

```
GET https://fin-ncloud.apigw.fin-ntruss.com/vserver/v2/createServerInstances
?regionCode=FKR
&serverImageProductCode=SW.VSVR.OS.LNX64.CNTOS.0703.B050
&vpcNo=***04
&subnetNo=***43
&serverProductCode=SVR.VSVR.STAND.C002.M004.NET.SSD.B050.G001
&feeSystemTypeCode=MTRAT
&serverCreateCount=1
&serverName=test-***
&networkInterfaceList.1.networkInterfaceOrder=0
&networkInterfaceList.1.accessControlGroupNoList.1=***63
&placementGroupNo=***61
&isProtectServerTermination=false
&initScriptNo=***44
&loginKeyName=test-***
&associateWithPublicIp=true
& isEncryptedBaseBlockStorageVolume=ture
```

| 그림 8-7-15 | Server의 Multi Zone 구성 API 예시

API를 통한 Cloud DB의 이중화(Multi zone) 구성

① **(API(CLI))** 'createCloudMysqlInstance' API를 통해 가상자원(Cloud DB) 생성 시, 'inMultiZone 파라미터를 이용하여 Cloud DB를 Multi Zone에 구성합니다

- 요청 예시

```
GET https://fin-ncloud.apigw.fin-ntruss.com/vmysql/v2/createCloudMysqlInstance
?regionCode=FKR
&vpcNo=****83
&cloudMysqlImageProductCode=SW.VDBAS.DBAAS.LNX64.CNTOS.0708.MYSQL.8025.B050
&cloudMysqlProductCode=SVR.VDBAS.STAND.C002.M008.NET.HDD.B050.G002
&dataStorageTypeCode=SSD
&isHa=true
&isMultiZone=true
&isStorageEncryption=true
&isBackup=true
&backupFileRetentionPeriod=10
&backupTime=02:00
&isAutomaticBackup=false
&cloudMysqlServiceName=test-****
&cloudMysqlServerNamePrefix=test-****
&cloudMysqlUserName=test-****
&cloudMysqlUserPassword=********
&hostIp=192.168.0.%
&cloudMysqlPort=13306
&cloudMysqlDatabaseName=test-****
&subnetNo=****91
&standbyMasterSubnetNo=****93
```

| 그림 8-7-16 | Cloud DB 생성 시 Multi zone 구성 API 예시

4 참고 사항

- [참고1] Subnet 생성 사용자 가이드
- [참고2] Application Load Balancer 생성 사용자 가이드
- [참고3] Server 생성 사용자 가이드
- [참고4] Cloud DB 생성 사용자 가이드
- [참고5] Server 생성 API 가이드
- [참고6] Cloud DB 생성 API 가이드

금융분야 상용 클라우드컴퓨팅서비스 보안 관리 참고서 (NAVER Cloud)

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

〈비 매 품〉

금융분야
상용 클라우드컴퓨팅서비스 보안 관리 참고서