Naver Cloud Platform 보안가이드

저작권

목차

Ⅰ. 개요

Naver Cloud Platform의 다양한 상품을 이용하여 서비스를 안전하게 구성/사용 할 있도록 보안 가이드를 제공 하고자 합니다.

가이드는 계정관리, 네트워크 보안, 서버 보안, 스토리지 보안, DB 보안, 안전한 접속 수단 총 7개의 카테고리로 구성되어 있으며, Naver Cloud Platform 설명서(https://docs.fin-ncloud.com/)를 바탕으로 보안설정을 해야하는 주요 항목에 대해 설정 방법을 설명하였습니다.

Naver Cloud Platform의 각 상품을 이용하는 방법에 대해서는 설명서를 참조하고, 보안 설정 및 보안 점검을 수행하는 경우 본 가이드를 참조 합니다.

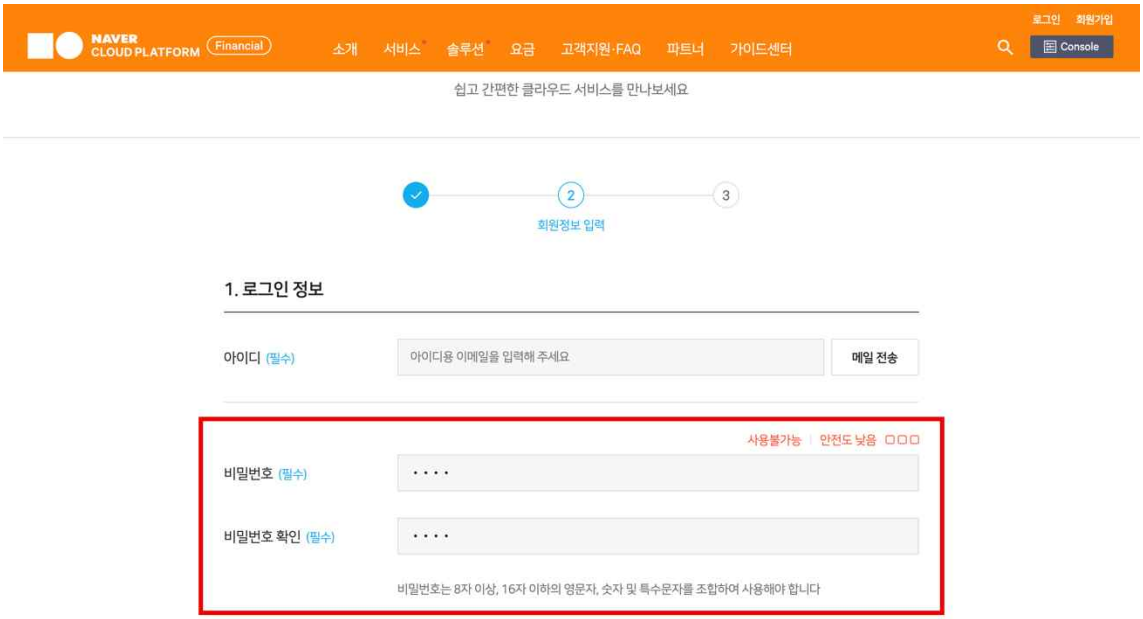
II. Naver Cloud Platform 보안 가이드 항목

중요도	내용
상	보안 설정 미비에 따라 고객의 클라우드 환경에 심각한 보안위협이 발생할 가능성이 있는 항목
중	보안 설정 미비에 따라 고객의 클라우드 환경에 보안위협이 발생할 가능성이 있는 항목
하	보안위협이 발생할 가능성은 낮지만 고객의 클라우드 환경에 보안 수준 향상을 위해 권고하는 항목

영역	항목번호	점검항목	중요도
1. 계정관리	AC-01	패스워드 복잡성 설정	-
	AC-02	패스워드 최소길이 설정	-
	AC-03	강화된 인증 방식 적용	중
	AC-04	API 인증키 관리	상
	AC-05	계정 권한 부여 방식	중
	AC-06	불필요한 계정 제거	중
2. 네트워크 보안	VP-01	VPC Naming 설정	하
	VP-02	서비스 목적에 따른 네트워크 분리	중
	VP-03	NACL 관리	중
	VP-04	NAT Gateway 관리	중
3. 서버 보안	SV-01	서비스 포트 관리	상
	SV-02	서버간 통신 제어	중
	SV-03	사용자 접근 통제	상
	SV-04	공인 IP 사용 제한	중
	SV-05	불필요한 서버 제거	중
	SV-06	OS 취약성 점검	중
4. 스토리지 보안	ST-01	버킷 공개 설정	중
	ST-02	불필요한 버킷 제거	중
	ST-03	NAS 접근제어	중
5. DB 보안	DB-02	DB 접근통제	상
	DB-03	DB Backup	중
6. 클라우드 환경 보안 감사	AU-02	리소스 기반 감사	중
7. 안전한 접속 수단	SE-01	안전한 접속 수단 설정	중

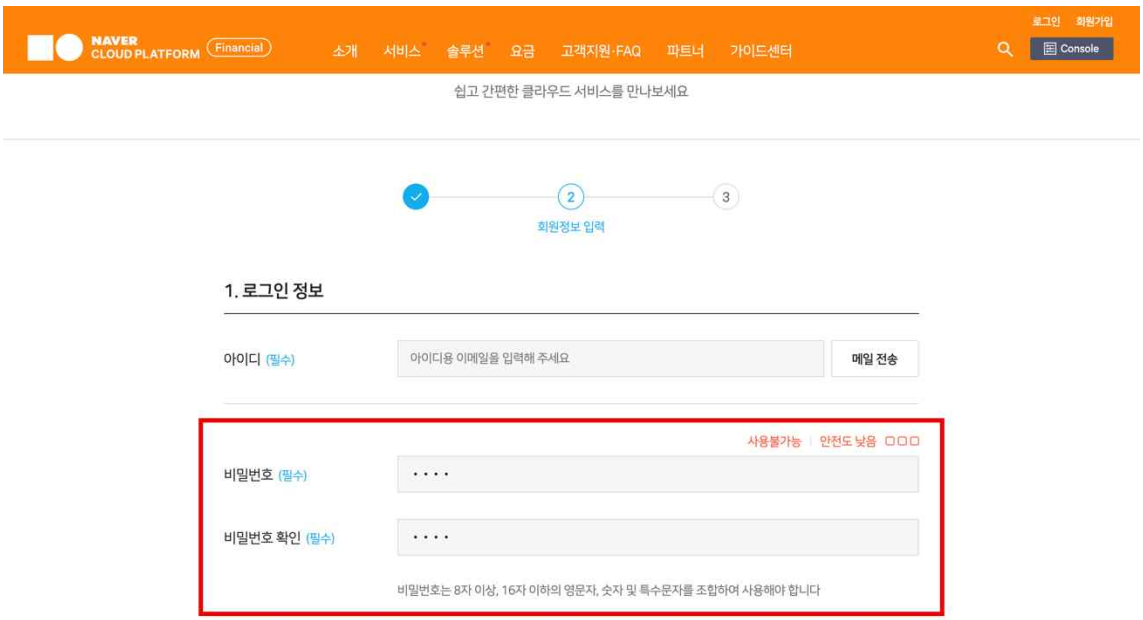
1. 계정관리

AC-01 패스워드 복잡성 설정

No.	AC-01	중요도	-	대상 서비스	Main 계정, Sub Account
서비스 개요	▪ Naver Cloud Platform 을 이용하기 위해 최초로 생성해야 되는 Console 계정 생성 시 사용되는 패스워드의 설정 항목 입니다.				
점검목적	▪ 패스워드가 단순하게 설정되어 있는 경우 비 인가자에 의한 brute-force, Dictionary attack 공격이 발생할 수 있으므로, 해당 공격을 예방하기 위해 패스워드의 복잡성 설정이 되어 있는지 점검 합니다.				
점검기준	▪ 양호 : 패스워드 영문자, 숫자 및 특수문자를 조합하여 8자 이상으로 설정되어 있는 경우 양호 합니다.				
권고사항	▪ Naver Cloud Platform은 8자 이상, 16자 이하의 영문자, 숫자 및 특수문자를 조합하여 패스워드를 생성 하게 되어 있습니다. 패스워드 생성 규칙을 준수하지 않을 경우 아래와 같이 사용 불가능 메시지가 출력 됩니다.  〈그림. 패스워드 복잡성 설정〉				
비고	▪ 참고 링크 : https://docs.fin-ncloud.com/ko/financial_guide/main_guide.html				

AC-02 패스워드 최소 길이 설정

No.	AC-02	중요도	-	대상 서비스	Main 계정, Sub Account
서비스 개요	▪ Naver Cloud Platform 을 이용하기 위해 최초로 생성해야 되는 Console 계정 생성 시 사용되는 패스워드의 설정 항목 입니다.				

점검목적	▪ 짧은 패스워드를 사용하는 경우 비 인가자에 의한 brute-force, Dictionary attack 공격이 발생할 수 있으므로, 해당 공격을 예방하기 위해 패스워드 길이가 최소 8자 이상 설정이 되어 있는지 점검 합니다.
점검기준	▪ 양호 : 패스워드 최소 길이가 8자 이상으로 설정되어 있는 경우 양호 합니다.
권고사항	▪ Naver Cloud Platform은 8자 이상, 16자 이하의 영문자, 숫자 및 특수문자를 조합하여 패스워드를 생성 하게 되어 있습니다. 패스워드 생성 규칙을 준수하지 않을 경우 아래와 같이 사용 불가능 메시지가 출력 됩니다.  〈그림. 패스워드 최소 길이 설정 설정〉
비고	▪ 참고 링크 : https://docs.fin-ncloud.com/ko/financial_guide/main_guide.html

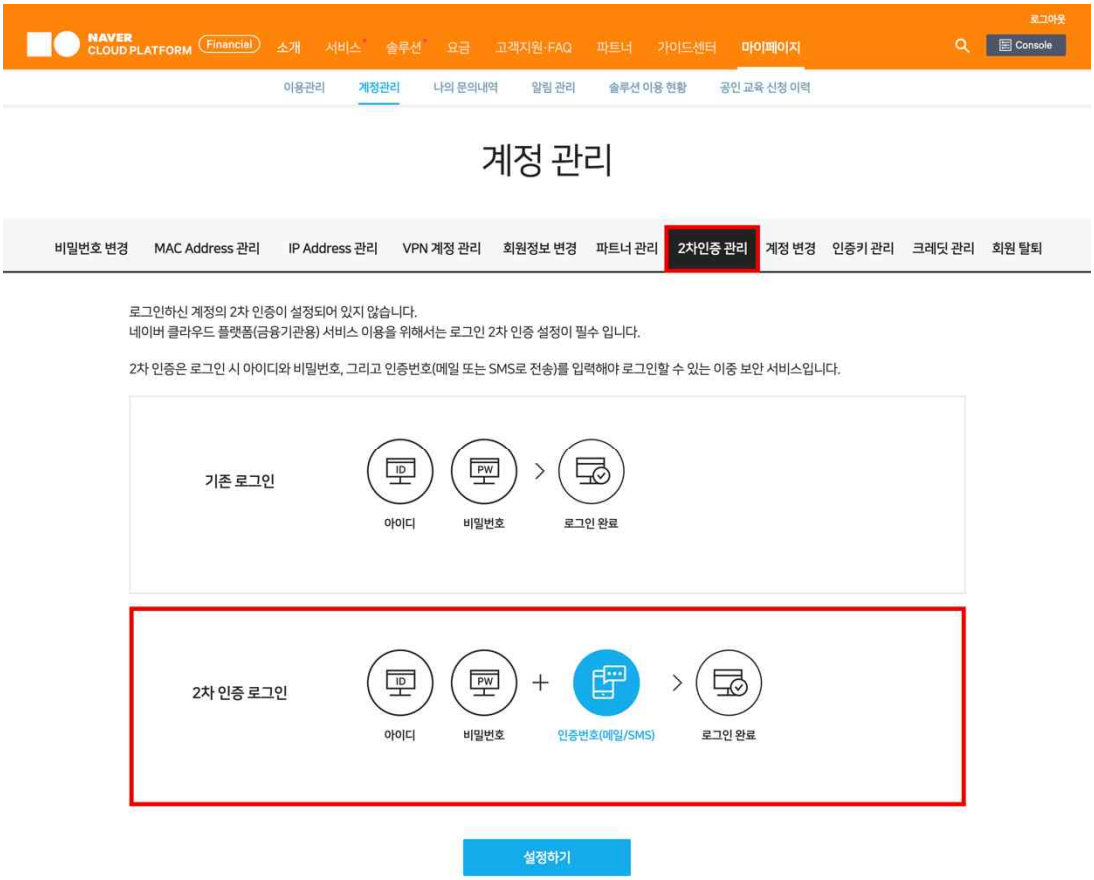
AC-03 강화된 인증방식 적용

No.	AC-03	**중요도**	중	**대상 서비스**	Main 계정, Sub Account
서비스 개요	▪ Naver Cloud Platform 의 안전한 이용을 위해 사용자 계정과 비밀번호 이외에 추가적인 인증 수단을 제공 합니다. NCP의 리소스를 생성, 삭제, 변경할 수 있는 계정에 대한 보안을 강화 합니다.				
점검목적	▪ 고객 클라우드 환경에서의 콘솔 계정은 리소스를 생성, 변경, 삭제 할 수 있는 권한을 가지고 있습니다. 따라서 계정의 보안강화를 위해 인증번호 또는 OTP로 2차인증이 설정되어 있는지 점검 합니다.				
점검기준	양호 : 메인 계정, Sub Account 모두 ID, Password 외 추가적인 인증 수단을 적용하고 있는 경우 양호 합니다.				

권고사항

▪ Naver Cloud Platform 계정 관리 메뉴 2 차인증 관리에서 설정 할 수 있습니다.
인증번호(휴대폰, 이메일 주소) 기반 2 차 인증을 선택하여 사용 하여 인증을 강화하는 것을 권고 합니다.

1) 2 차인증 설정 방법 : 마이페이지 -> 계정 관리 -> 2 차인증 관리



<그림. 2 차인증 설정 메뉴>

2) 인증번호 설정

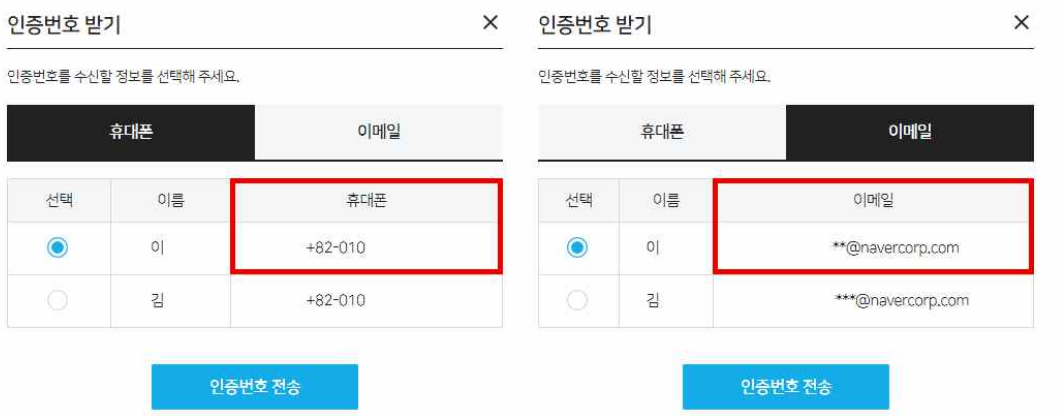
① 인증번호로 설정 -> 휴대폰 번호, 이메일 주소 중복 선택 가능하며, 단일 항목 선택 가능

〈그림. 2 차 인증 수단 선택〉

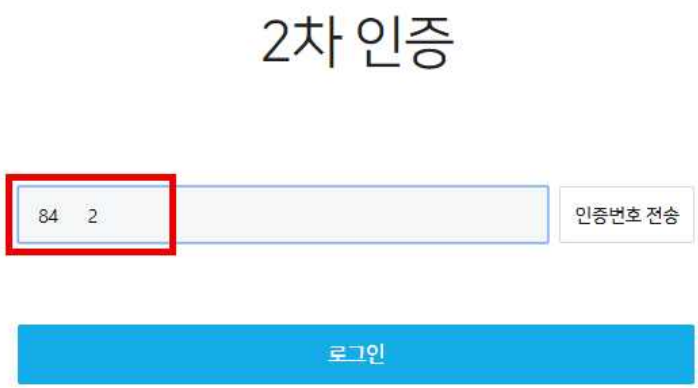
② 설정 완료 후 로그인 시 아이디, 패스워드 입력 후 로그인을 하면 2 차 인증 페이지 발생 -> 인증번호 전송 클릭

〈그림. 2 차 인증 번호 전송〉

③ 인증번호 받기에서, 사전 설정한 정보(휴대폰 번호 또는 이메일 주소)를 선택하여 인증번호 전송

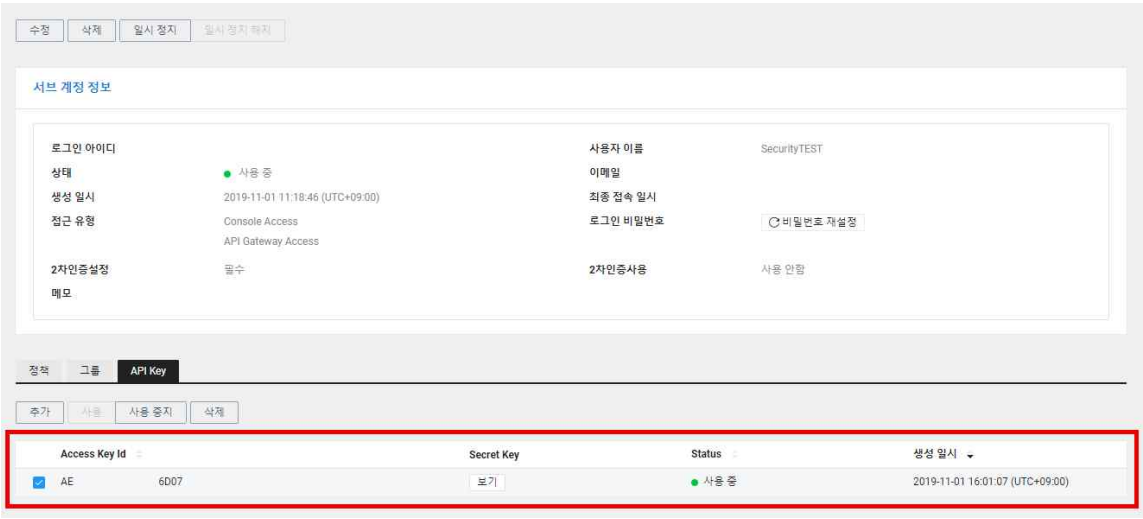


〈그림. 인증 번호 전송〉

	④ 전송 받은 인증번호 입력 후 로그인  〈그림. 인증 번호 사용 로그인〉
비고	▪ 참고 링크 : https://docs.fin-ncloud.com/ko/financial_guide/main_guide.html

AC-04 API 인증키 관리

No.	AC-04	**중요도**	상	**대상 서비스**	Main 계정, Sub Account
서비스 개요	▪ Naver Cloud Platform 은 제공하는 서비스를 안전하게 이용하도록 회원별 API 인증키를 발급하고 있습니다. API 인증키는 API 를 호출한 사용자가 권한을 가진 사용자인지 식별하는 도구입니다.				
점검목적	▪ Access Key를 이용하여 다양한 기능을 API로 제어할 수 있습니다. Key 유출 시 비 인가자가 기간 제한 없이 리소스를 등록, 수정, 조회할 수 있으므로 주기적으로 Key에 대해 관리(변경주기에 따라 교체)해야 합니다.				
점검기준	▪ 양호 : 메인 계정, Sub Account 모두 Access Key에 대해 주기적으로 관리하고 있는지 점검하고 있는 경우 양호 합니다.				
권고사항	▪ 네이버 플랫폼의 메인 계정은 모든 권한을 가지고 있는 강력한 계정이기 때문에 Key 유출 시 위험의 수준이 높습니다. 따라서 메일 계정에 대해서는 키 발급을 하는 것을 권고 하지 않습니다. Sub Account 를 통해 API Key 를 발급하고, Key 유출에 대비하여 주기적으로 교체하는 것을 권고 합니다. ▪ 키 관리 메뉴 : 메인 계정 : Console -> 마이페이지 -> 인증키 관리 ▪ 키 관리 메뉴 : Sub Account : Console -> Sub Account -> Sub Account ㄴ -> 개인 Sub Account -> API Key				

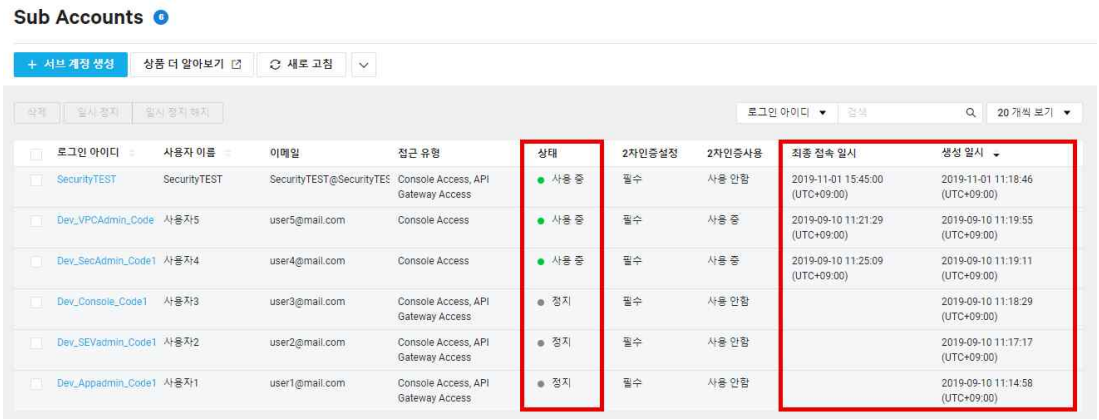
	 〈그림. API Key 상태 확인〉
비고	▪ 참고 링크 : https://docs.fin-ncloud.com/ko/financial_guide/main_guide.html

AC-05 계정 권한 부여 방식

No.	AC-05	**중요도**	중	**대상 서비스**	Main 계정, Sub Account
서비스 개요	▪ Naver Cloud Platform 의 Sub Account 는 그룹 자체에 권한을 부여할 수 있어 그룹 별로 권한을 부여한 후, 서브 계정을 그룹 내 추가/삭제하면서 편리하게 권한 관리를 할 수 있습니다.				
점검목적	▪ 그룹에 속하지 않은 특수권한의 계정이 존재하는지 여부를 확인하기 위함, 특수권한에 의한 오남용을 예방하기 위해 모든 계정이 그룹에 속해 있는지 여부를 점검 합니다.				
점검기준	▪ 양호 : Sub Account의 모든 계정이 그룹에 속해 있는 경우 양호 합니다.				
권고사항	▪ Naver Cloud Platform 의 Sub Account Group 메뉴를 통해 정책을 그룹에 반영하고 사용자 개별 서브 계정은 그룹을 통해 정책을 부여 받는 것을 권고 합니다. 그룹에 반영되어 있는 정책에 따라 해당 사용자의 권한을 식별할 수 있습니다. 예) Appliaction_Group, DB_Group, 서버_Group, Console_Admin 등 ▪ 그룹 권한 설정 메뉴 : Console -> Sub Account -> Groups  〈그림. 그룹 관리〉				

비고	▪ 참고 링크 : https://docs.fin-ncloud.com/ko/financial_guide/main_guide.html

AC-06 불필요한 계정 제거

No.	AC-06	중요도	중	대상 서비스	Main 계정, Sub Account
서비스 개요	▪ Sub Account는 Naver Cloud Platform에서 제공하는 무료 권한 관리 플랫폼으로, 본 계정 하위에 서브 계정을 생성할 수 있는 기능입니다				
점검목적	▪ 불필요한 계정(퇴직, 전직, 휴직 등의 사유로 사용하지 않는 계정 및 장기적으로 사용하지 않는 계정 등)이 존재하는지 점검하여 관리되지 않은 계정에 의한 침입에 대비하고 있는지 점검합니다.				
점검기준	▪ 양호 : Sub Account에 등록된 계정 중 불필요한 계정이 존재하지 않는 경우 양호 합니다.				
권고사항	▪ Naver Cloud Platform 의 Sub Account 사용자 계정 및 접근권한의 적정성 검토 기준, 검토주체, 검토방법, 주기 등을 수립하여 정기적 검토를 이행하여야 합니다. 미사용 계정, 직무 변경 사용자 계정에 대해 정기적으로 검토하여, 계정 사용 중지, 계정 삭제 처리를 합니다. 예) 30 일 동안 미사용 계정에 대한 비활성 화 45 일 동안 미사용 계정에 대한 삭제 퇴사, 직무 변경에 따라 즉시 삭제 ▪ Sub Account 계정 관리 : Console -> Sub Account -> Sub Accounts  〈그림. Sub Account 계정 관리〉				
비고					

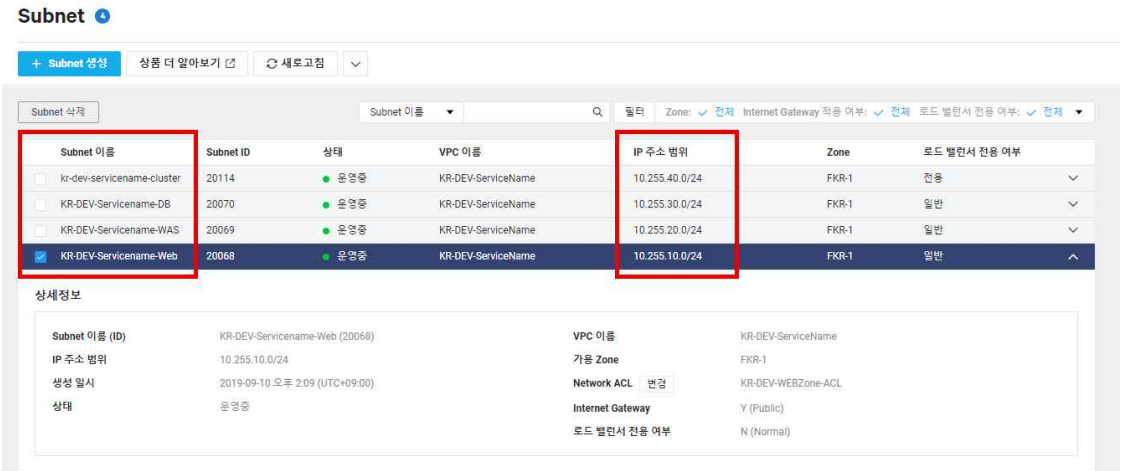
2. 네트워크 보안

VP-01 VPC Naming 설정

No.	VP-01	중요도	하	대상 서비스	VPC
서비스 개요	▪ Naver Cloud Platform Financial, VPC(Virtual Private Cloud)는 퍼블릭 클라우드 상에서 제공되는 고객 전용 사설 네트워크를 의미합니다. 고객의 계정마다 최대 3개의 VPC를 생성할 수 있으며, 각 VPC는 최대 넷마스크 0.0.255.255/16 (IP 65,536개) 크기의 네트워크 주소 공간을 제공합니다. VPC는 다른 VPC 네트워크와 논리적으로 분리되어 있으며, 기존 고객 데이터센터 네트워크와 유사하게 구현할 수 있습니다.				
점검목적	▪ VPC 내 모든 상품을 구성할 때 VPC를 지정해야 합니다. 잘못된 VPC 이름을 지정하는 경우 서비스 장애, 보안 위협이 발생할 수 있습니다. 따라서 VPC를 생성할 때 서비스를 식별할 수 있도록 네이밍이 되었는지 점검 합니다.				
점검기준	▪ 양호 : VPC 이름을 통해 서비스를 식별할 수 있는 경우 양호 합니다.				
권고사항	▪ 금융 클라우드에서 VPC 를 생성할 때 서비스를 식별할 수 있는 이름으로 설정 합니다. 서브넷 생성, 서버 생성 시 VPC 를 선택 하는 설정에서 서비스 이름으로 식별하여 리소스 생성 오류를 예방 할 수 있습니다. 예) 리전-서비스운영형태-서비스네임(KR-DEV-Potalservice) ▪ VPC 생성 메뉴 : Console -> VPC -> VPC Management -> VPC 생성  <그림. VPC 생성 메뉴>				
비고	▪ 참고 링크 : http://docs.fin-ncloud.com/ko/networking/vpc/vpc_overview.html				

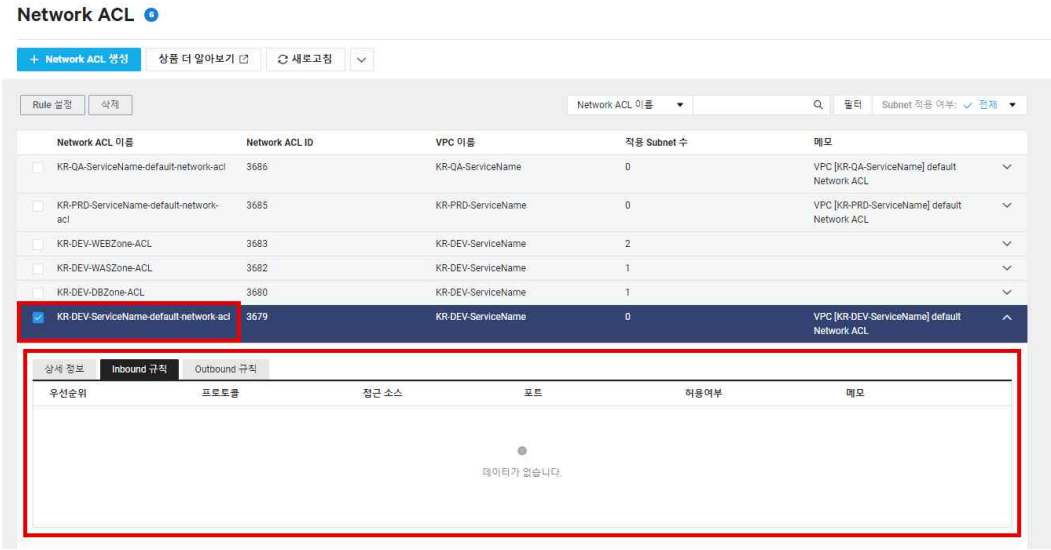
VP-02 서비스 목적에 따른 네트워크 분리

No.	VP-02	중요도	중	대상 서비스	VPC-Subnet
서비스 개요	▪ Naver Cloud Platform Financial, Subnet 은 VPC 네트워크 공간을 세분화하여 사용할 수 있는 기능입니다.				

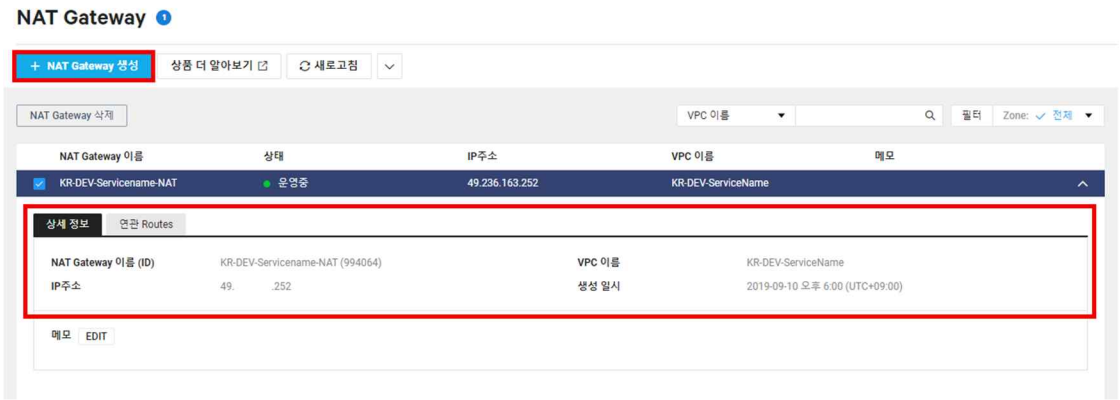
	공인 Subnet(Public Subnet) 또는 사설 Subnet(Private Subnet)으로 나누어 사용합니다. 고객 서비스의 최적화된 네트워크 아키텍처를 구성할 수 있으며, 서버(서버) 및 데이터베이스(Database)와 같은 Naver Cloud Platform 의 리소스를 Subnet 공간에 배치합니다
점검목적	▪ 특정 Subnet에 서비스가 침해가 발생되었을 때 각 Subnet간 접근통제로 2차 피해 예방을 위해 서비스 목적에 따라 Subnet이 분리되어야 합니다.
점검기준	▪ 양호 : 서비스 사용 목적에 따라 서브넷이 분리되어 있는 경우 양호 합니다.
권고사항	▪ 서비스 사용 목적에 따라 Subnet 을 분리 합니다. 분리된 Subnet 간 통신은 NACL, ACG 를 통해 통신을 제어하여 Subnet 간 비인가 통신에 대해 통제 합니다. 예) 10.255.30.0/24 - DB Zone, 10.255.20.0/24 - WAS Zone, 10.255.10.0/24 - Web Zone ▪ Subnet 설정 메뉴 : Console -> VCP -> Subnet management -> Subnet 생성  〈그림. Subnet 분리〉
비고	▪ 참고 링크 : https://docs.fin-ncloud.com/ko/networking/vpc/vpc_detailedsubnet.html

VP-03 NACL 관리

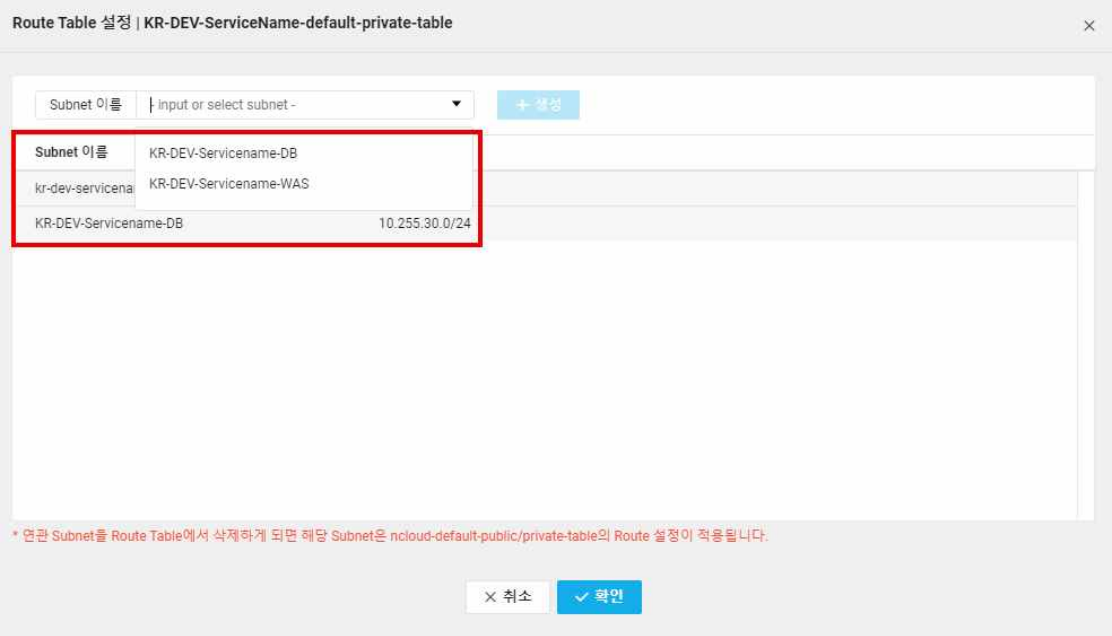
No.	VP-03	**중요도**	중	**대상 서비스**	VPC-NACL
서비스 개요	▪ Naver Cloud Platform, Network ACL 은 Subnet 레벨에서 작동하며 Inbound 및 Outbound 트래픽에 대하여 허용 또는 차단 규칙을 적용할 수 있습니다. Network ACL 을 이용하여 각 Subnet 을 독립적인 네트워크로 구분 합니다.				
점검목적	▪ 특정 Subnet에 서비스가 침해가 발생되었을 때 각 Subnet간 접근통제로 2차 피해 예방을 위해 서비스 목적에 따라 Subnet이 분리되어야 합니다.				
점검기준	▪ 양호 : Network ACL에 정책이 없는 경우 허용 상태 입니다. 따라서 전체 차단 정책 적용 되어 있으며, 서비스에 필요한 IP, Port에 대해서만 허용되어 있는 경우 양호 입니다.				

권고사항	▪ Network ACL 정책은 Black List Deny 형태로 관리/운영 할 수 있습니다. Network ACL 에 정책을 추가하지 않으면 전체 Allow 상태 입니다. 따라서 내외부와 통신이 필요하지 않은 IP, Port 를 제한하는데 사용할 수 있습니다. 또한 Network ACL 을 통해 Subnet 간 서버통신제어를 ACG 과 함께 2 차적으로 제어할 수 있습니다. ▪ ACL 설정 메뉴 : Console -> VPC -> Network ACL -> Network ACL 생성 1) VPC 를 생성하게 되면 Default ACL 이 자동으로 생성 됩니다. 자동 생성된 Default ACL 은 정책이 없으며, 즉 모두 허용 상태 입니다.  〈그림. Network 기본 정책〉 2) Network ACL 은 Stateless 방식이기 때문에 반환 트래픽이 규칙에 의해 명시적으로 허용되어야 합니다. 예) 외부 IP(211.xx.xx.200) NCP 내부에 있는 서버에 22 포트로 접속이 필요한 경우 - Inbound 211.xx.xx.200 22 허용 - Outbound 211.xx.xx.200 1-65535 허용  〈그림. ACL 정책 설정〉
비고	▪ 참고 링크 : https://docs.fin-ncloud.com/ko/networking/vpc/vpc_security.html

VP-04 NAT Gateway 관리

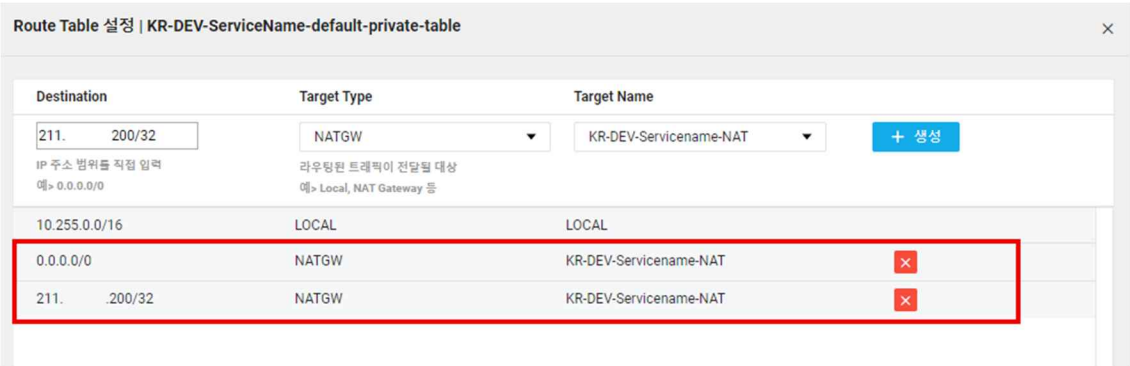
No.	VP-04	중요도	중	대상 서비스	VPC-NAT Gateway
서비스 개요	▪ NAT 는 네트워크 주소 변환(Network Address Translation)의 약자로, 비 공인 네트워크에 속한 여러 개의 호스트가 하나의 공인 IP 주소를 사용하여 인터넷에 접속하는 방법이고 NAT 를 처리해 주는 장치를 NAT Gateway 라고 부릅니다. NAT Gateway 는 비 공인 IP 를 가진 다수의 서버에게 대표 공인 IP 를 이용한 외부 접속을 제공합니다.				
점검목적	▪ 외부 통신 사용이 지속적으로 연결되어 있는 경우 해당 서버가 침해사고가 발생되었을 때 외부로 정보를 전송할 수 있는 위협이 존재 합니다. 따라서 사용 목적이 완료되어 더 이상 외부로의 통신이 필요 없는 서버들에 대해서는 NAT Gateway 설정에서 제외 합니다.				
점검기준	▪ 양호 : 외부 통신 사용이 완료된 서버가 없는 경우 양호 합니다.				
권고사항	▪ NAT Gateway 사용 목적은 Public IP 가 없는 서버의 외부와의 통신을 위해 사용하는 기능 이기 때문에 통신이 필요한 시점에서만 NAT Gateway 를 통해 외부 오픈을 하고 통신 제어는 ACG 를 통해 제어하는 것을 권고 합니다. ▪ NAT Gateway 생성 후 Route Table 메뉴에서 외부로 통신이 필요한 연관 Subnet 설정과 목적지 설정을 해주어야 합니다. 또한 Network ACL, ACG 허용 설정을 해주어야 외부로의 통신이 가능 합니다. 1) NAT Gateway 를 생성 합니다.  〈그림. NAT Gateway 생성〉				

2) Route Table 메뉴에서 NAT Gateway 를 사용할 연관 Subnet 을 설정 합니다.



〈그림. NAT Gateway Subnet 설정〉

3) Destion(목적지) 항목에 연결할 외부 네트워크 주소를 CIDR 형태로 입력 합니다.
   - 특정 목적지 주소를 입력 할 수 있습니다.
   - 모든 인터넷 연결을 허용하기 위해서는 0.0.0.0/0 으로 설정 합니다.



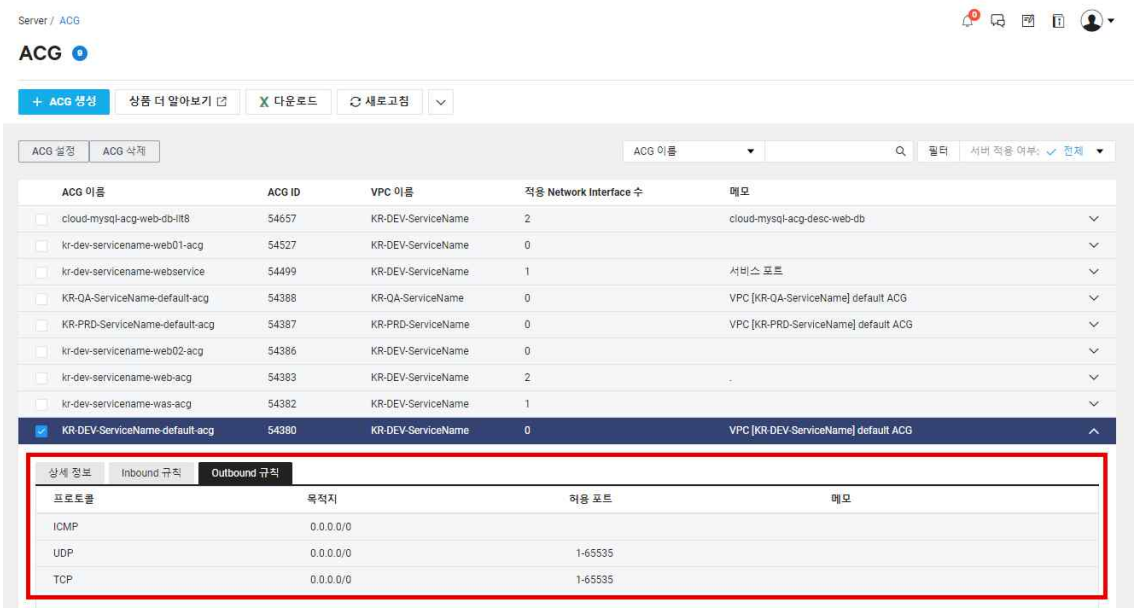
〈그림. NAT Gateway 목적지 설정〉

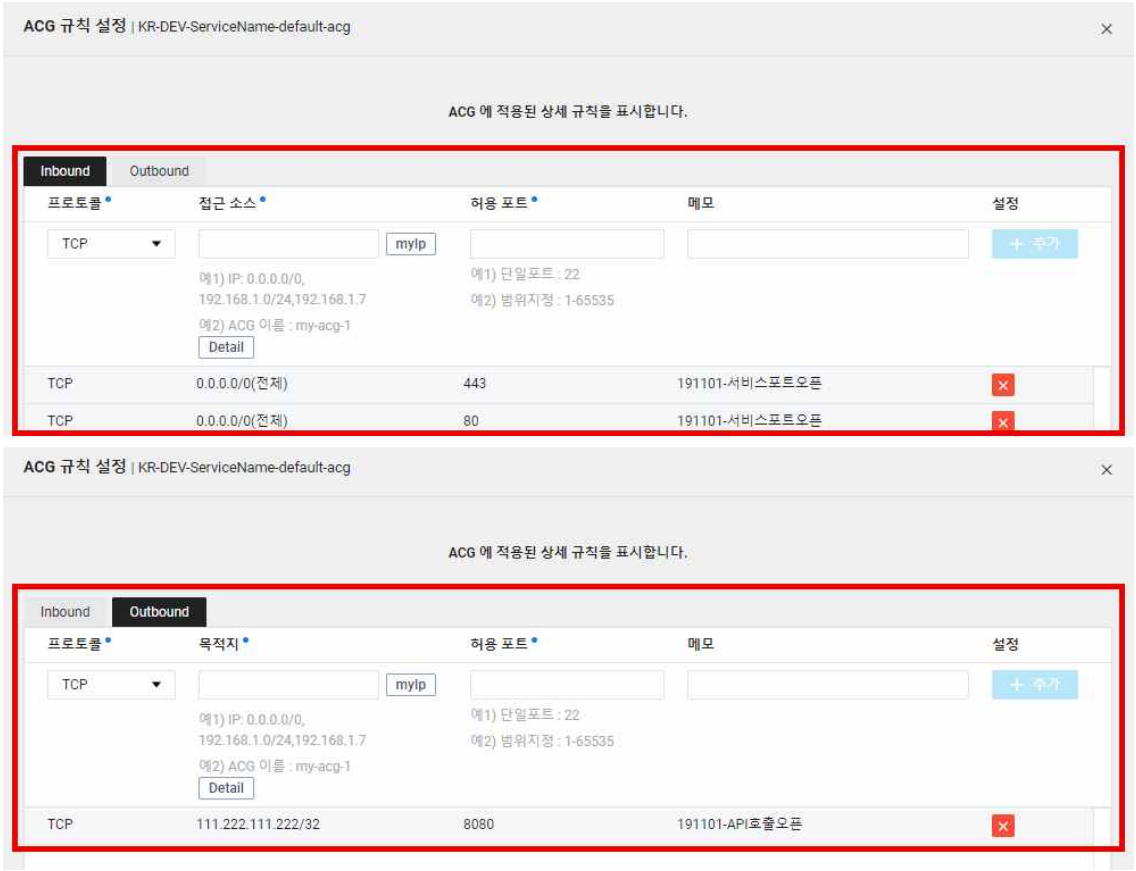
비고

▪ 참고 링크 : https://docs.fin-ncloud.com/ko/networking/vpc/vpc_security.html

3. 서버 보안

SV-01 서비스 포트 관리

No.	SV-01	중요도	상	대상 서비스	서버-ACG
서비스 개요	▪ Naver Cloud Platform ACG(Access Control Group)는 서버 간 네트워크 접근 제어 및 관리를 할 수 있는 IP/Port 기반 필터링 방화벽 서비스입니다. 고객은 기존 방화벽 (iptables, ufw, 윈도우 방화벽)을 개별적으로 관리할 필요 없이 서버 그룹에 대한 ACG Rule 을 손쉽게 설정하고 관리할 수 있습니다. ACG 는 Stateful 방식이기 때문에 규칙에 관계없이 반환 트래픽은 자동으로 허용 됩니다.				
점검목적	▪ 서비스에 필요하지 않은 IP, Port 허용으로 침해위협이 발생할 수 있습니다. 따라서 정기적으로 사용하지 않는 IP, Port에 대해 허용되어 있는지 점검하여 침해사고를 예방 합니다.				
점검기준	▪ 양호 : 서비스에 필요한 IP, Port에 대해서만 허용되어 있는 경우 양호 합니다.				
권고사항	▪ ACG 정책은 White List Allow 형태로 관리/운영 할 수 있습니다. Default ACG 초기 상태는 모든 Outbound 규칙이 허용 처리 되어 있습니다.. 따라서 서비스에 필요한 IP, Port 만 허용하고 사용해야 합니다. ACG 에 정책이 없는 경우에는 모든 IP, Port 가 차단 됩니다. ▪ ACG 설정 메뉴 : Console -> 서버 -> ACG  <그림. Default ACG 상태>				

	▪ ACG 설정은 서비스에 필요한 포트만 오픈해야 합니다.  〈그림. 서비스에 필요한 포트 오픈〉
비고	▪ 참고 링크: https://docs.fin-ncloud.com/ko/security/acg/acg_console.html

SV-02 서버간 통신 제어

No.	SV-02	**중요도**	중	**대상 서비스**	서버-ACG
서비스 개요	▪ ACG(Access Control Group)는 서버 간 네트워크 접근 제어 및 관리를 할 수 있는 IP/Port 기반 필터링 방화벽 서비스입니다. 고객은 기존 방화벽 (iptables, ufw, 윈도우 방화벽)을 개별적으로 관리할 필요 없이 서버 그룹에 대한 ACG Rule 을 손쉽게 설정하고 관리할 수 있습니다. ACG 는 Stateful 방식이기 때문에 규칙에 관계없이 반환 트래픽은 자동으로 허용 됩니다.				
점검기준	▪ 특정 서버가 침해사고가 발생했을 경우, 서버간 허용된 IP, Port에 의해 침해사고가 전파될 수 있습니다. 2차 피해 예방을 위해 서비스 목적에 필요한 IP, Port에 대해 서버간 허용되어 있는지 점검 합니다.				
점검기준	▪ 양호 : 서버간 통신에 대해 프로세스에 의해 승인된 정책에 대해서만 ACG가 허용되어 있는 경우 양호 합니다.				

권고사항

▪ Naver Cloud Platform ACG 는 최대 100 까지만 생성이 가능 하기 때문에 동일한 목적의 서버인 경우 ACG 를 그룹화 하여 관리하는 것을 권고합니다. 동일한 서브넷의 서버간 통신은 ACG 를 사용하여 통제 할 수 있습니다.(메모 기능을 사용하여 사용기간, 승인번호등 증적을 기입 합니다.)

Ex. [2대의 서버가 각각의 ACG를 사용하고 있는 경우] 10.250.10.10 -> 10.250.10.20 : 8888

① WEB01 ACG Outbound 규칙 적용

<그림. 다른 ACG사용시 Out Bound 규칙 설정>

② WEB02 ACG Inbound 규칙 적용

<그림. 다른 ACG사용시 In Bound 규칙 설정>

Ex. [2대의 서버가 하나의 ACG를 사용하고 있는 경우] 10.250.10.10 -> 10.250.10.20 : 8888

① 접속을 시도 하는 IP에 대한 허용 처리

<그림. 동일 ACG사용시 In Bound 규칙 설정>

② 접속 대상이 되는 IP에 대한 허용 처리

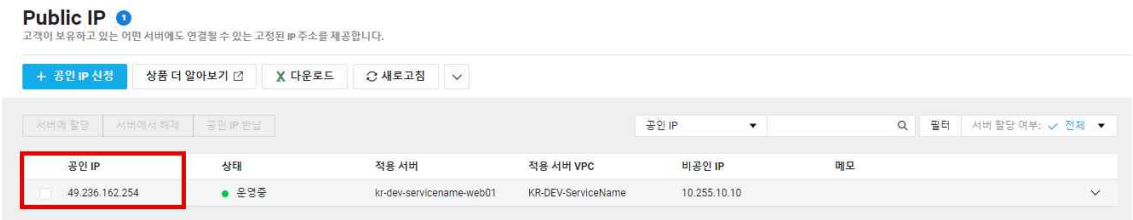
	 〈그림. 동일 ACG사용시 Out Bound 규칙 설정〉
비고	▪ 참고 링크: https://docs.fin-ncloud.com/ko/security/acg/acg_console.html

SV-03 사용자 접근 통제

No.	SV-03	**중요도**	상	**대상 서비스**	서버
서비스 개요	▪ Naver Cloud Platform 의 서버 상품은 서비스 규모와 사용 목적에 적합한 성능의 서버를 선택할 수 있도록 Standard, High Memory 와 같은 다양한 서버 타입을 제공합니다. 또한 CentOS, Ubuntu, RHEL, Windows, MySQL, MSSQL 등 다양한 이미지를 제공하고 있으므로 다양한 버전의 운영체제를 선택할 수 있습니다.				
점검목적	▪ 인증키 사용시 패스워드가 탈취될 가능성이 없기 때문에 ID, Password 를 직접 입력해서 서버에 로그인 하는 방식에 비해 인증키를 통한 서버 접속을 하는 경우 더욱 안전 합니다. 따라서 서버 접속 시 인증키 사용하고 있는지 여부를 점검 합니다.(인증키가 유출되지 않도록 유의해야 합니다.)				
점검기준	▪ 양호 : 서버 접근시 인증키를 통해 서버 접속을 하고 있는 경우 양호 합니다.				
권고사항	▪ Naver Cloud Platform 의 서버 접속 환경 설정은, SSL VPN, IPSec VPN, 서버의 공인 IP, Bastion 서버 등으로 접속 환경을 설정 할 수 있습니다. 서버 접속 환경 설정 중 권고 방안은 SSL VPN 과 IPSeC VPN 입니다. 온프라미스와 네이버 클라우드 서버간 지속적인 통신이 필요한 경우에는 IPSeC VPN 을 권고 합니다. 서버 접속 환경 설정이 완료 되면 실제 사용하게 될 서버 접속에 접속을 합니다. 서버 접속 방법은 인증키 사용 방법과, ID, Password 인증 방식이 있으며, 인증키 사용 방법을 권고 합니다. ▪ 인증키를 사용한 서버 접속 방법에 대해서는 하기 링크를 참조 합니다. https://docs.fin-ncloud.com/ko/compute/server/server_console.html ▪ NCP IPsec 을 연동했을 경우 Legacy 환경 출발지 IPSec 에서 서버접근(IP, Port)에 대해 사용자 접근통제를 합니다.				

	▪ Bastion 서버 형태로 서버접근통제를 하는 경우, 출발지의 IP 를 NACL, ACG 를 사용하여 통제하는 것을 권고 합니다. ▪ 3rd-party 서버접근통제 솔루션을 이용하여 솔루션의 ID, Password + 2차인증 방식을 이용해 서버에 접근하는 경우에는 안전하다고 할 수 있습니다.
비고	▪ Naver Cloud Platform Financial : VPC 와 Subnet 이 없다면 서버 생성이 불가능합니다. VPC 와 Subnet 부터 생성해야 합니다.

SV-04 공인 IP 사용 제한

No.	SV-04	**중요도**	중	**대상 서비스**	서버
서비스 개요	고객이 보유하고 있는 어떤 서버에도 연결될 수 있는 고정된 IP 주소인 공인 IP 를 제공합니다. 공인 IP 는 고객이 지정한 서버에 할당할 수 있습니다. 할당된 공인 IP 는 필요에 따라 고객이 보유한 다른 서버로 변경해 할당할 수 있습니다. 기존 서버를 신규 서버로 이전할 때, 준비된 신규 서버에 기존과 동일한 환경을 구축한 후 기존 서버의 공인 IP 를 신규 서버에 할당하기만 하면 짧은 서비스 중단 시간 이후 서비스를 연속적으로 제공할 수 있습니다.				
점검목적	▪ Private Zone 에 위치한 서버에 Public IP 가 할당된 경우 해당 IP 로 침해위협이 발생될 가능성이 있으며, 동일한 Subnet 대역에 있는 서버들의 정보 또한 외부 유출 가능성이 존재 합니다. 따라서 Private Zone 에 위치한 서버에 Public IP 할당되지 않도록 주기적으로 점검 합니다. * NCP VPC Private Subnet 의 경우 Public IP 가 할당되지 않습니다.				
점검기준	▪ 양호 : Private Zone 에 위치한 NCP 서버 중 Public IP 가 할당된 경우가 없다면 양호 합니다.				
권고사항	▪ Private Zone 에 위치한 서버는 Public IP 를 사용하지 않습니다. 외부와의 통신이 필요한 경우 NAT Gateway 를 통해 통신 하는 것을 권고 합니다. 외부와의 지속적인 In/Out 통신이 필요하여, Public IP 를 사용해야 하는 경우 해당 서버를 Public Zone 으로 이동하는 등의 Architecture 재구성에 대한 고려가 필요 합니다.  〈그림. 서버 공인 IP 확인〉
비고	▪ 참고 링크 : https://docs.fin-ncloud.com/ko/compute/server/server_console.html				

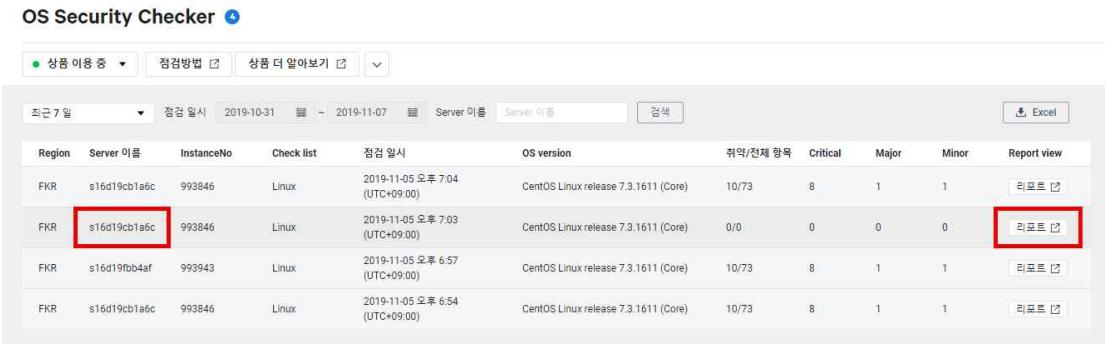
SV-05 불필요한 서버 제거

No.	SV-05	**중요도**	중	**대상 서비스**	서버

서비스 개요	▪ Naver Cloud Platform 의 서버(서버) 상품은 서비스 규모와 사용 목적에 적합한 성능의 서버를 선택할 수 있도록 Standard, High Memory 와 같은 다양한 서버 타입을 제공합니다. 또한 CentOS, Ubuntu, RHEL, Windows, MySQL, MSSQL 등 다양한 이미지를 제공하고 있으므로 다양한 버전의 운영체제를 선택할 수 있습니다.
점검기준	▪ 불필요한 서버(사용 목적이 완료된)가 존재하는지 점검하여 관리되지 않은 서버에 대해 침입에 대비하고 있는지 점검 합니다.
점검기준	▪ 양호 : 사용 목적이 완료되어, 불필요한 서버에 대해 정기적 검토를 통해 반납 처리가 되고 있는 경우 양호 합니다.
권고사항	▪ 사용 목적이 완료되어, 불필요한 서버에 대해 정기적 검토한 내용을 문서화 하고, 서버 설정 내 메모를 통해 서버에 대한 점검 식별을 할 수 있도록 합니다.  〈그림. 불필요한 서버에 대한 점검〉
비고	

SV-06 OS 취약성 점검

No.	SV-06	**중요도**	중	**대상 서비스**	서버
서비스 개요	▪ Naver Cloud Platform 의 서버(서버) 상품은 서비스 규모와 사용 목적에 적합한 성능의 서버를 선택할 수 있도록 Standard, High Memory 와 같은 다양한 서버 타입을 제공합니다. 또한 CentOS, Ubuntu, RHEL, Windows, MySQL, MSSQL 등 다양한 이미지를 제공하고 있으므로 다양한 버전의 운영체제를 선택할 수 있습니다.				
점검목적	▪ OS 의 취약한 설정으로 인해 발생할 수 있는 침해 사고를 예방하기 위해 주기적으로 OS 취약성 점검을 수행 합니다.				
점검기준	▪ 양호 : 주기적으로 OS 취약성 점검을 이행하고 있는 경우 양호 합니다.				
권고사항	▪ 서버를 생성하고, 시스템을 대내외적으로 오픈 하기 전 OS 취약한 설정이 있는지 점검하는 것을 권고 합니다. 또한 시스템 오픈 이후에도 OS 설정에 변경사항이 발생할 수 있으므로 정기적으로 취약성 점검을 수행 합니다.				

	▪ Naver Cloud Platform 의 보안 서비스 중 System Security Checker 을 통해 빠르고 간편하게 점검을 OS 취약성 점검을 수행 할 수 있습니다. ▪ System Security Checker 이용 신청 후 각 OS 에서 Agent 를 다운 받아 실행 합니다. ▪ 점검 시간은 일반적인 경우 최대 5 초를 넘지 않습니다. ▪ 점검 결과는 Console -> Security -> System Security Checker -> OS Security Checker 에서 확인 가능 하면 서버이름을 클릭하면 취약성에 대해 확인 할 수 있으면 리포트 버튼을 통해 세부적인 내용과 보안 권고 사항을 확인 할 수 있습니다.  〈그림. OS Security Checker 결과〉
비고	▪ 참고 링크 : https://docs.fin-ncloud.com/ko/security/systemsecuritychecker/systemsecuritychecker_overview.html

4. 스토리지 보안

ST-01 버킷 공개 설정

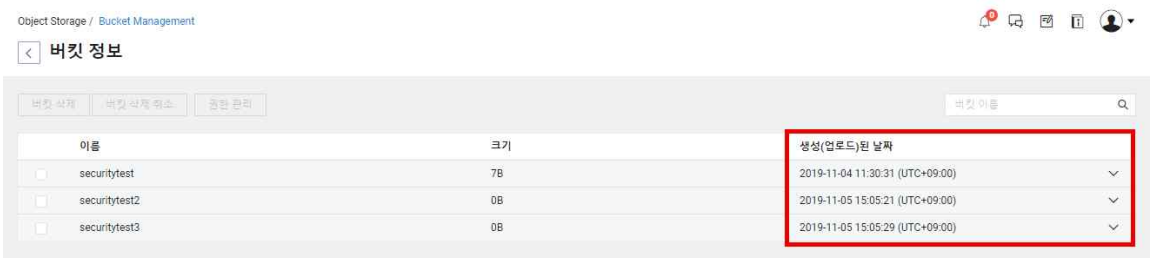
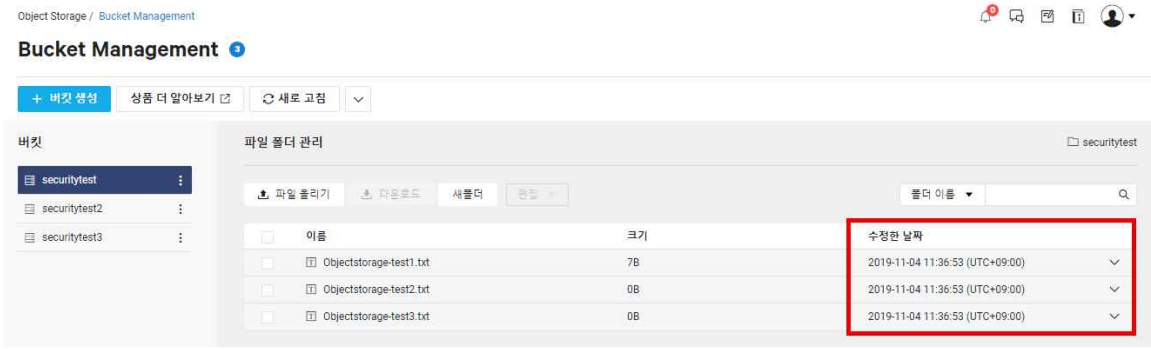
No.	ST-01	중요도	중	대상 서비스	Object Storage
서비스 개요	▪ Naver Cloud Platform Object Storage 는 사용자가 언제 어디서나 원하는 데이터를 저장하고 탐색할 수 있도록 파일 저장 공간을 제공하는 서비스입니다.				
점검목적	▪ 고객 클라우드 환경에서 가장 빈번하게 정보유출 사고가 발생하는 사례가 버킷의 설정 오류로 인한 사고 입니다. 따라서 중요 정보가 보관된 버킷이 외부에 공개로 설정되어 있는지 여부를 주기적으로 점검 합니다.				
점검기준	▪ 중요정보를 보관하고 있는 버킷이 비공개로 설정되어 있는 경우 양호 합니다.				
권고사항	▪ 버킷에 대해 공개 설정할 경우 버킷의 네임, 버킷 내 Object 정보등이 노출 됩니다. 중요정보를 보관하고 있는 버킷에 대해서는 공개여부를 비공개로 설정을 권고 합니다. ▪ 파일에 대한 공개 여부는 개별 파일에서 설정합니다. 버킷의 공개여부가 비공개일 경우라도, 버킷 내 업로드 된 파일 권한이 공개일 경우 외부에서 해당 파일에 접근 할 수 있습니다. ▪ 버킷 생성 메뉴 : Console -> Object Storage -> Bucket Management -> 버킷 생성  〈그림. 버킷 공개 설정〉				

〈그림. 버킷 공개 설정 시 노출 정보〉

비고	▪ 참고 링크 : https://docs.fin-ncloud.com/ko/storage/objectstorage/objectstorage_overview.html

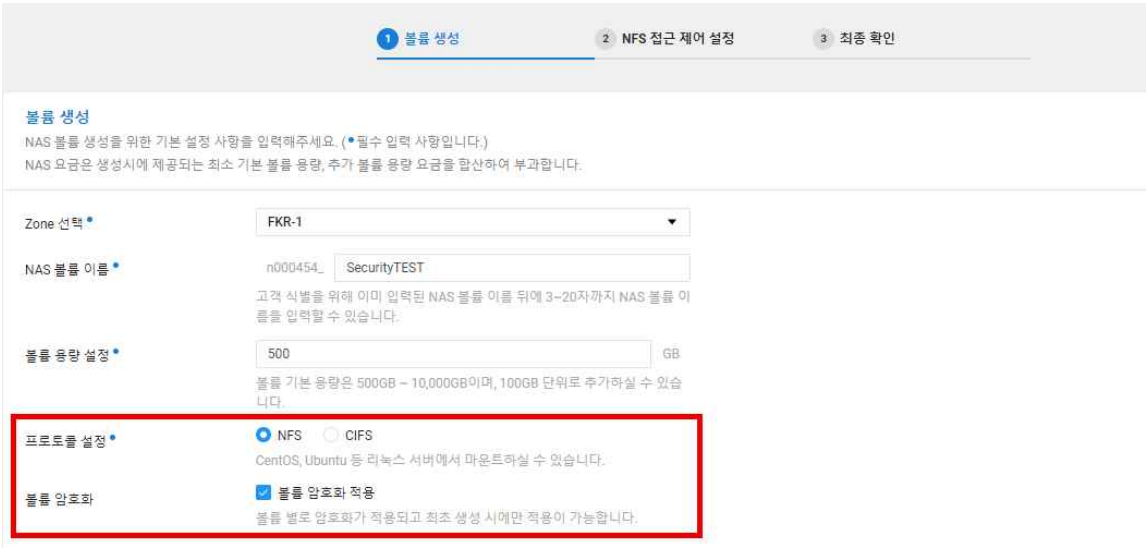
ST-02 불필요한 버킷 제거

No.	ST-02	**중요도**	중	**대상 서비스**	Object Storage
서비스 개요	▪ Naver Cloud Platform Object Storage 는 사용자가 언제 어디서나 원하는 데이터를 저장하고 탐색할 수 있도록 파일 저장 공간을 제공하는 서비스입니다.				
점검기준	▪ 불필요한 버킷(사용 목적이 완료된)이 존재하는지 점검하여 관리되지 않은 버킷에 대해 침입에 대비하고 있는지 점검 합니다.				
점검기준	▪ 양호 : 사용 목적이 완료되어, 불필요한 버킷에 대해 정기적 검토를 통해 삭제 처리가 되고 있는 경우 안전 합니다.				
권고사항	▪ 버킷의 사용 현황을 점검하여, 파일 또는 폴더가 없는 버킷의 경우에는 삭제 처리, 최근 업로드된 내역을 업는 버킷에 대해서는 기존 데이터를 백업 후 삭제등 Data 의 보관 주기 프로세스를 수립하여 운영하는 것을 권고 합니다.				

	▪ 버킷 생성 정보 확인  〈그림. 버킷의 생성 정보〉 ▪ 버킷 내 파일에 대한 생성 및 수정 정보  〈그림. 버킷 내 파일의 변경 정보〉
비고	

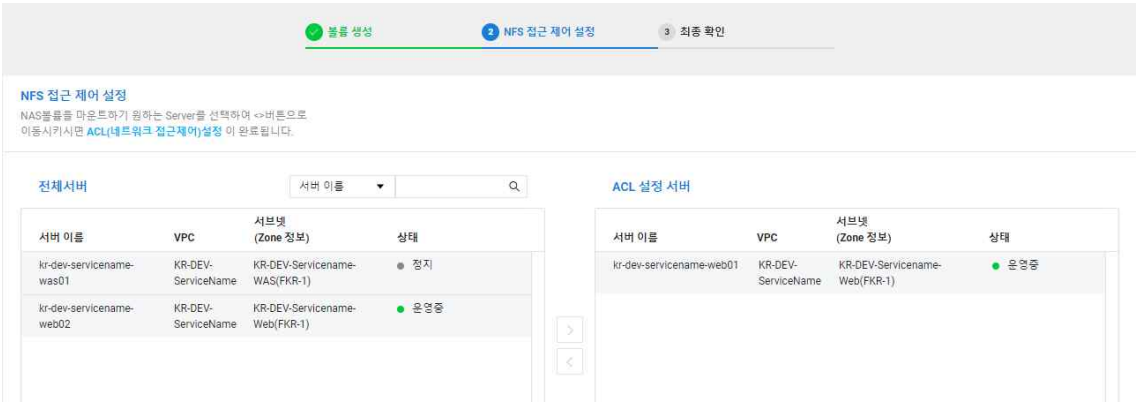
ST-03 NAS 접근제어

No.	ST-03	**중요도**	중	**대상 서비스**	NAS
서비스 개요	▪ Naver Cloud Platform 에서 제공하는 NAS 는 서버 간 데이터 공유, 대용량 스토리지, 유연한 용량 확대/축소, 스냅샷 백업 등 NAS 상품의 주요 기능을 활용해 사용자가 안전하고 편리하게 데이터를 관리할 수 있습니다. 특히, 프로토콜에 따른 인증 설정으로 높은 보안성을 제공하고, 이중화된 Controller 및 Disk Array Raid 구성으로 강력한 서비스 안정성을 확보하고 있습니다.				
점검목적	▪ NAS 에 사용 목적이 완료되어 중지된 서버가 NAS 에 마운트가 해제되어 있는지 점검 합니다. ▪ NAS 에 사용 목적에 따라 공유되어서는 안되는 서버가 마운트 되어 있는지 점검 합니다.				
점검기준	▪ 양호 : 사용 중지된 서버 또는 공유 되어서는 안되는 서버가 NAS에 마운트 되어 있는지 주기적으로 점검하고 있는 경우 양호 합니다.				
권고사항	▪ NAS 접근이 허용된 리눅스 서버에 대해 정기적으로 검토하여, 사용이 중지 되거나 NAS 를 통해 공유되어서는 안될 서버가 있는지 점검 하고 NFS 접근제어 설정을 통해 제어를 수행 합니다. ▪ Windows 서버의 경우 CIFS 설정을 통해 접근 허용 패스워드를 주기적으로 변경 합니다. ▪ 프로토콜 설정 시 리눅스 계열 서버는 NFS, Windows 서버 계열은 CIFS 를 선택하고, 볼륨 암호화 옵션을 활성화 하는 것을 권고 합니다.				



<그림. NAS 볼륨 생성 옵션 설정>

▪ Linux 계열의 서버는 NAS 볼륨 생성 NFS 접근 제어 설정에서 마운트를 원하는 서버를 선택 할 수 있습니다. 볼륨 생성이 완료된 이후에도 NFS 접근 제어를 설정 할 수 있습니다.



<그림 NFS 접근 제어 설정>

	▪ Windows 계열의 서버는 NAS 마운트 시 ID, Password 인증방식을 사용 합니다. 패스워드를 주기적으로 변경하여 사용하는 것을 권고 합니다.  〈그림 CIFS 접근 제어 설정〉
비고	참고 링크 : https://docs.fin-ncloud.com/ko/storage/nas/nas_overview.html

5. DB 보안

DB-01 DB 접근통제

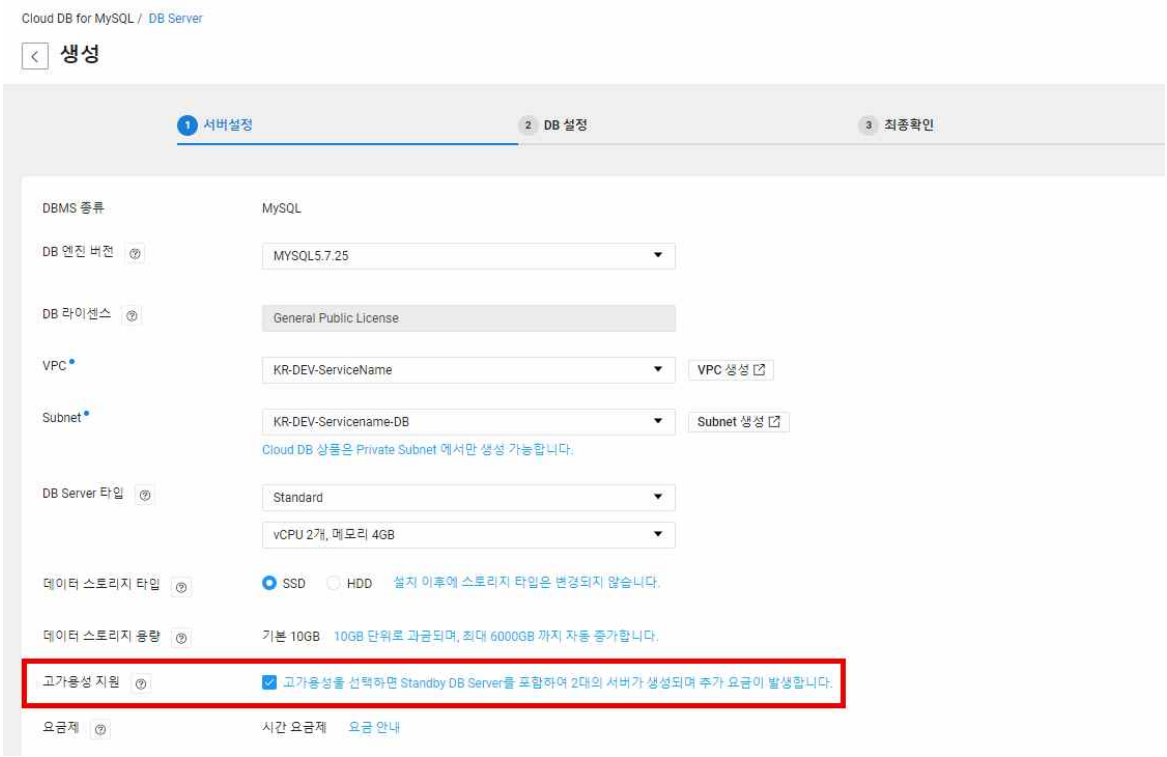
No.	DB-01	중요도	상	대상 서비스	Cloud DB for MySQL / MxSQL 설치형
서비스 개요	▪ Cloud DB for XX 는 몇 가지 설정과 클릭만으로 간편하게 구축하고, 네이버의 최적화 설정을 통해 안정적으로 운영하며, 장애가 발생하면 자동 복구하는 완전 관리형 클라우드 서비스입니다. ▪ Naver Cloud Platform 에서 제공하는 xxSQL 설치형 서비스에서는 기본 설치 수준의 기 설치된 이미지를 지원해줍니다.				
점검기준	▪ 데이터베이스 내 정보에 접근이 필요한 응용프로그램, 정보시스템(서버) 및 사용자를 명확히 식별하고 접근통제 정책에 따라 통제하고 있는지 점검 합니다.				
점검기준	▪ 양호 : 데이터베이스 내 정보에 접근이 필요한 응용프로그램, 정보시스템(서버) 및 사용자를 명확히 식별하고 접근통제 정책에 따라 통제하고 있는 경우 안전 합니다.				
권고사항	▪ DB 서버 사용자 접속은 SSL VPN 을 통해 접속하는 방법을 권고 합니다. SSL VPN 을 통해 개별 사용자를 식별 할 수 있습니다. ▪ VPC 의 Subnet 을 통해 DB Zone 을 구성하고 Network ACL 과 ACG 를 통해 접근통제를 수행하고, DB 서버의 직접 접속은 SSL VPN 을 통해 사용자를 식별하여 접속하는 것을 권고 합니다. ▪ 개인정보 및 중요정보를 보관하는 DB 의 경우에는 3rd-party 솔루션을 활용하여 안전하게 접근하는 방법에 대해서도 고려해야 합니다.				
비고	▪ 참고 링크 : https://docs.fin-ncloud.com/ko/security/sslvpn/sslvpn_overview.html				

DB-02 DB Backup

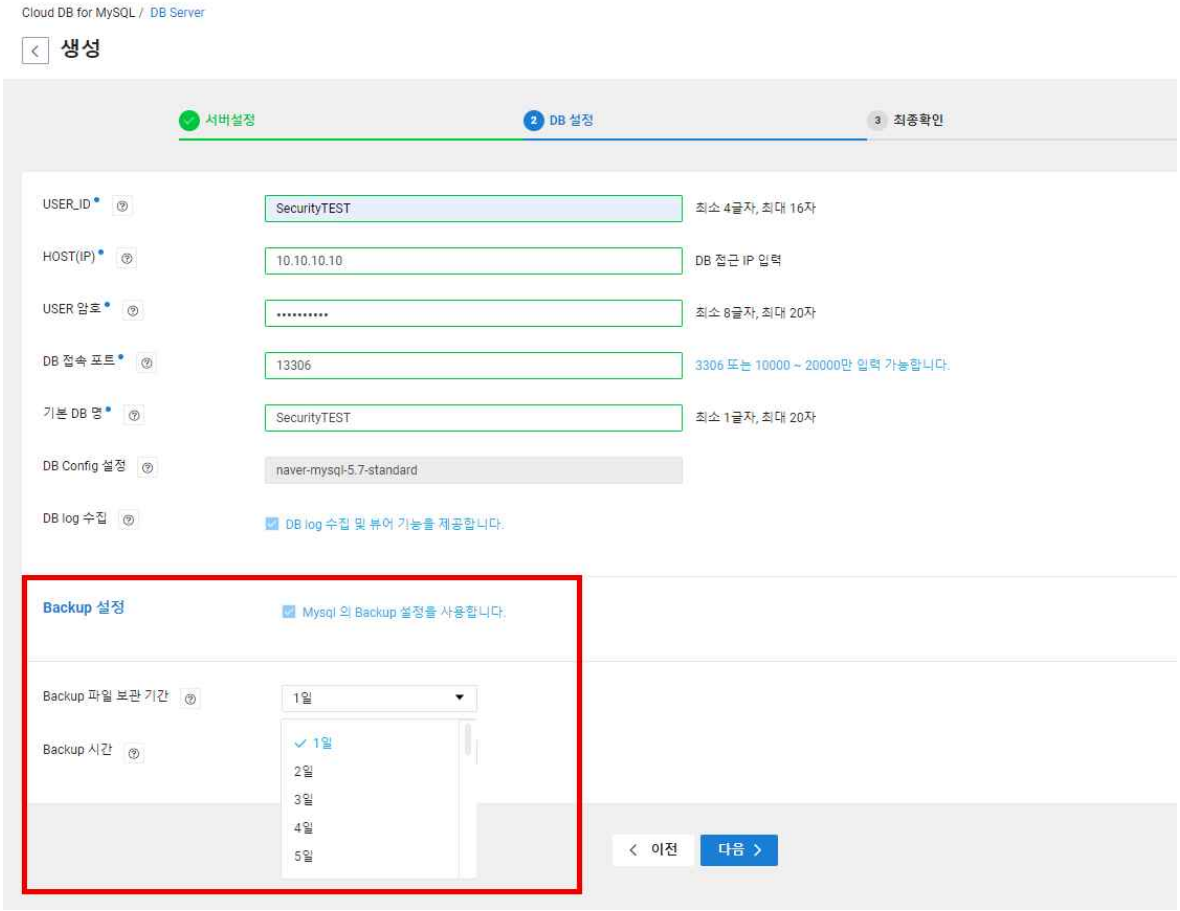
No.	DB-02	중요도	중	대상 서비스	Cloud DB for MySQL / MxSQL 설치형
서비스 개요	▪ Cloud DB for MySQL 은 몇 가지 설정과 클릭만으로 간편하게 구축하고, 네이버의 최적화 설정을 통해 안정적으로 운영하며, 장애가 발생하면 자동 복구하는 완전 관리형 클라우드 서비스입니다. ▪ Naver Cloud Platform 에서 제공하는 xxSQL 설치형 서비스에서는 기본 설치 수준의 기 설치된 이미지를 지원해줍니다.				
점검목적	데이터의 침해, 장애발생으로 인한 데이터 손실에 대응을 위해 DB 이중화 구성 및 백업 절차를 마련하고 있는지 점검 합니다.				
점검기준	▪ 양호 : 데이터의 가용성 및 무결성을 유지하기 위하여 이중화 구성 및 백업 절차를 마련하고 있는 경우 안전 합니다.				
권고사항	▪ Cloud DB for MySQLd 은 DB 생성시 이중화 설정 옵션을 통해서 고 가용성 설정을 권고 합니다..				

또한 Backup 파일에 대한 보관 기간을 설정하여 Backup 을 수행하는 것을 권고 합니다.
추가적으로 파일을 보관해야 하는 경우 Object Storage 로 전송하여 보관 할 수 있습니다.

▪ Cloud DB for MySQL 생성 메뉴에서 고가용성 지원을 옵션으로 설정 할 수 있습니다.



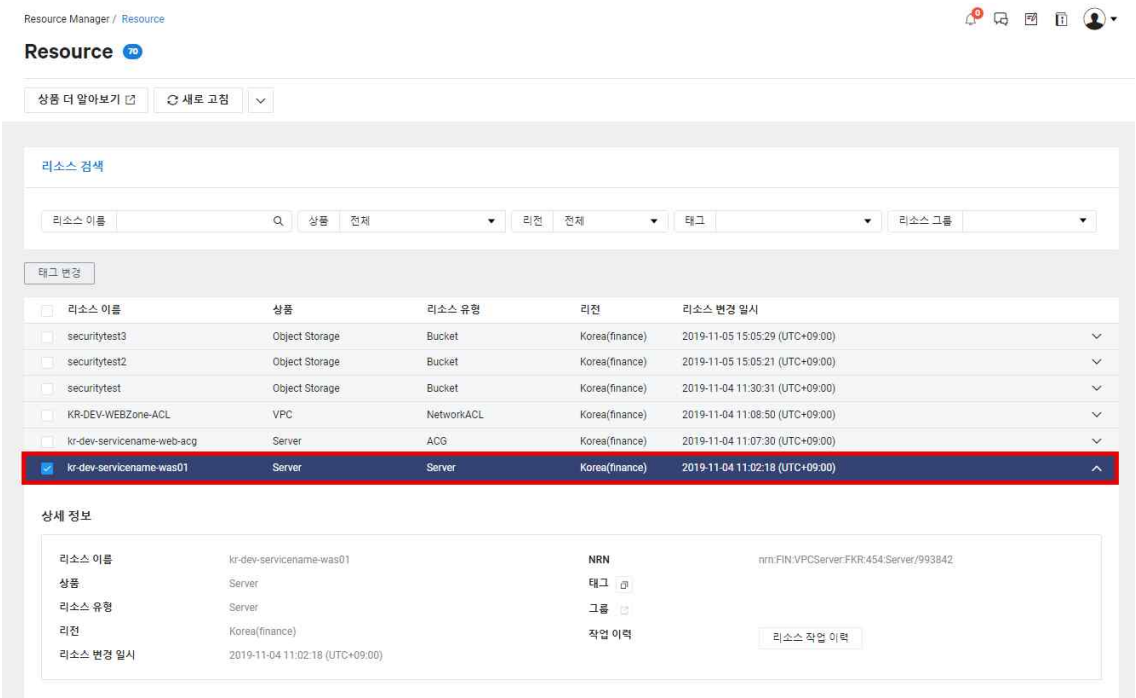
〈그림. Cloud DB for MySQL 고가용성 설정〉

	▪ Cloud DB for MySQL 생성 메뉴에서 Backup 설정과, Backup 파일의 보관 기간을 설정할 수 있습니다.  〈그림. Cloud DB for MySQL Backup 설정〉
비고	▪ 참고 링크 : https://docs.fin-ncloud.com/ko/database/cdb_mysql/cdb_mysql_setting.html

6. 클라우드 환경 보안 감사

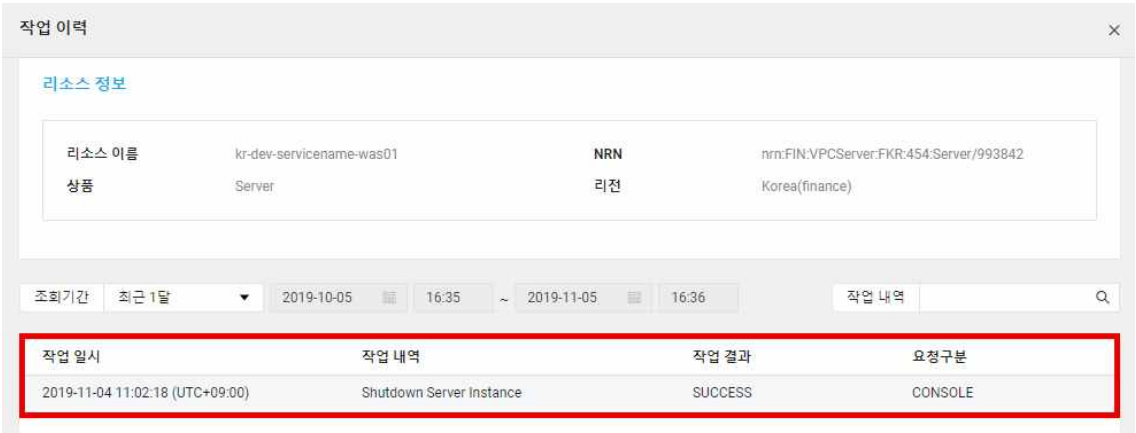
AU-01 리소스 기반 감사

No.	AU-01	중요도	중	대상 서비스	Resource Manager
서비스 개요	▪ Naver Cloud Platform 에서 사용자가 생성하고 관리하고 삭제할 수 있는 주요 리소스를 통합적으로 관리할 수 있는 서비스입니다. 생성된 전체 리소스 현황을 한 번에 확인할 수 있으며 개별 리소스의 작업 이력을 확인할 수 있습니다. 또한 개별 리소스에 대한 Tag 를 설정하여 논리적인 검색 및 관리할 수 있으며, 사용 목적에 따라 리소스를 그룹핑하여 체계적으로 리소스를 관리할 수 있습니다. ▪ 리소스는 사용자가 Naver Cloud Platform 에서 생성한 자원의 단위입니다.				
점검목적	▪ 승인되지 않은 리소스 생성/변경/삭제 등 고객 클라우드 환경의 오남용을 예방하기 위해 정기적으로 리소스 로그를 점검 합니다.				
점검기준	▪ 양호 : 인가되지 않은 리소스에 대한 생성, 변경, 삭제가 발생하였는지 적정성 검토를 정기적으로 이행하고 있는 경우 양호 합니다.				
권고사항	▪ Resource Manager 발생하는 로그를 주기적으로 감사하여 비인가 행위 여부를 점검하는 것을 권고 합니다. 감사 방안에 대해서는 아래의 예시를 참고 합니다. ▪ 예) Resource Manager 를 통해 서버의 변경 이력을 확인하여 정상적인 변경 여부 확인 ① 서버 상품 중 KR-PRD-Service-was01 에 대해 변경이 발생되었습니다.				



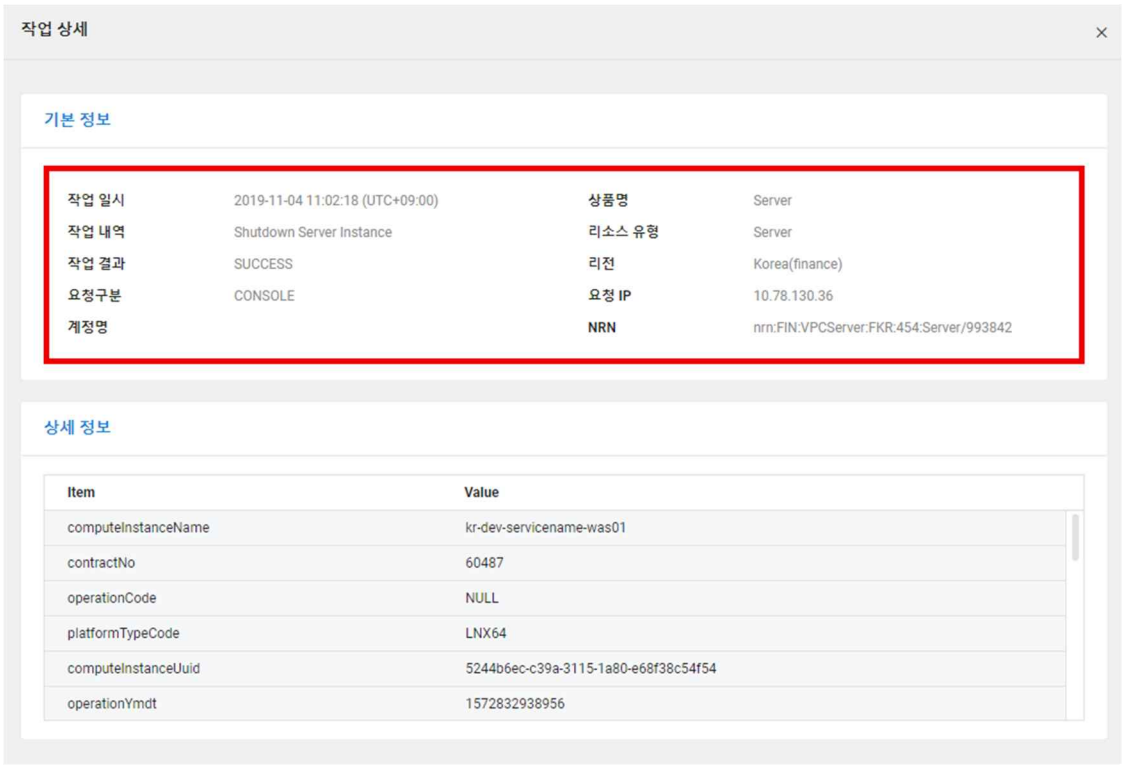
〈그림. 최근 리소스 변경 이력〉

② 리소스 작업 이력을 통해 어떤 변경 작업이 발생되었는지 확인 합니다. 최근에 변경 작업이 발생한 이력은 서버 중지 작업 입니다.



〈그림. 리소스 작업 이력 확인〉

③ Resource Manager 히스토리 메뉴에서 작업을 수행한 계정과, 요청 IP 등 추가적인 정보를 확인하여 인가된 작업인지 여부를 확인 합니다.



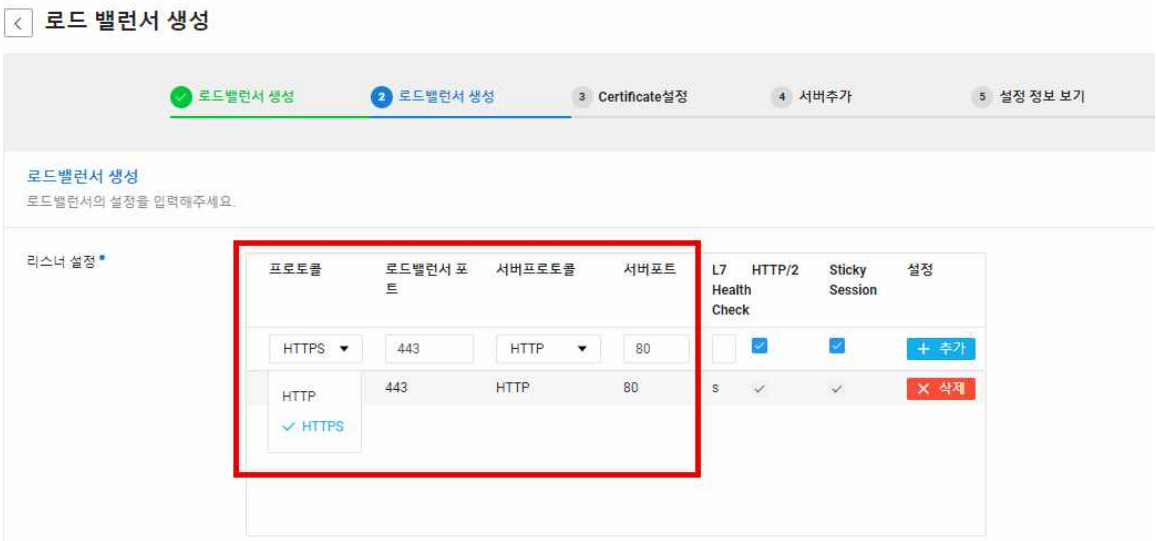
〈그림. 리소스 변경 정보 확인〉

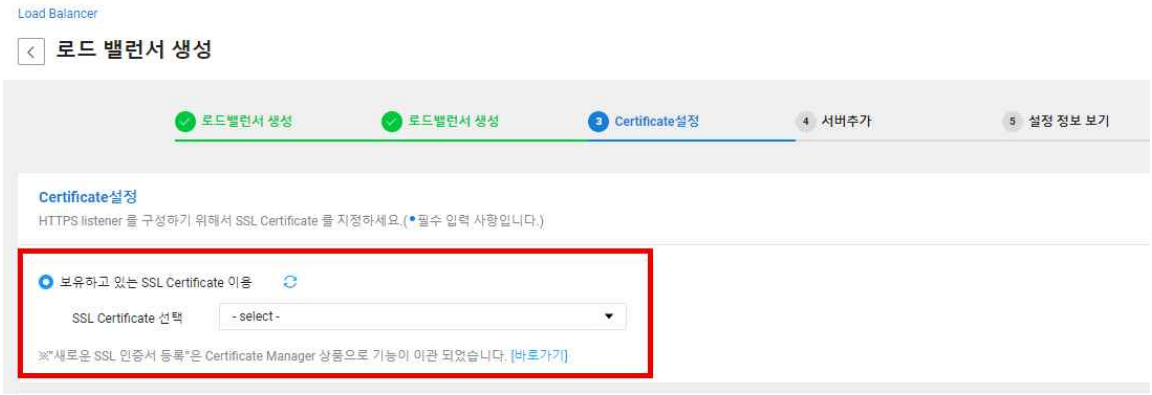
비고

▪ 참고 링크 : https://docs.fin-ncloud.com/ko/management/resourcemanager/resourcemanager_overview.html

7. 안전한 접속 수단

SE-01 안전한 접속 수단 설정

No.	SE-01	중요도	중	대상 서비스	Certificate Manager/ SSL VPN/ IPsec VPN
서비스 개요	▪ 네이버 클라우드 플랫폼은 안전하게 정보자산에 접근 할 수 있도록 Certificate Manager, SSL VPM, IPsec VPN 을 제공합니다.				
점검목적	▪ 정보자산에 접속하는 패킷값을 암호화하여 외부의 공격자로부터 데이터를 보호하기 위해 안전한 접속 수단을 제공/이용하고 있는지 점검 합니다.				
점검기준	▪ 정보자산에 접속이 필요한 경우에는 안전한 접속 수단을 적용하고 있는 경우 양호 합니다.				
권고사항	▪ Naver Cloud Platform 에서 운영중인 웹 서비스에 접속 시 이용자들의 안전한 접속을 위해 보안 인증서(SSL 인증서)를 적용하는 것을 권고 합니다. Certificate Manager 상품을 통해 Load Balanacer, CDN+에 보안 인증서를 적용할 수 있습니다. ▪ 인증서 적용 메뉴 : Console -> Certificate Manager 인증서 등록 -> LB, CDN 인증서 사용 설정 ▪ 로드 밸랜서 생성 시 프로토콜을 HTTPS, SSL 을 선택하는 경우 Certificate Manager 등록되어 있는 인증서를 사용할 수 있습니다.  〈그림. LoadBalance SSL 인증서 적용 사전 작업〉				

<table>
<tr>
<td></td>
<td>


〈그림. Load Balance SSL 인증서 적용 〉

▪ Naver Cloud Platform 에서 운영중인 서버, DB 접근시에는 SSL VPN, IPSec VPN 상품을 통해 안전하게 접속하는 것을 권고 합니다.

▪ SSL VPN 사용 방법: SSL VPN 생성 -> 사용자 설정 -> 사용자 VPN Client 연결 -> 접속 대상 서버 ACG 허용(SSL VPN IP 허용) -> 서버 접속

▪ IPsec VPN 사용 방법: IPsec VPN Gateway 생성 -> IPSec VPN Tunnel 구성 -> 서버 ACG 허용(SSL VPN IP 허용) -> 접속 대상 서버 ACG 허용(SSL VPN IP 허용) -> 서버 접속
</td>
</tr>
<tr>
<td>비고</td>
<td>▪ 참고 링크 : https://docs.fin-ncloud.com/ko/security/sslvpn/sslvpn_overview.html
▪ 참고 링크 : https://docs.fin-ncloud.com/ko/networking/ipsecvpn/ipsecvpn_overview.html</td>
</tr>
</table>