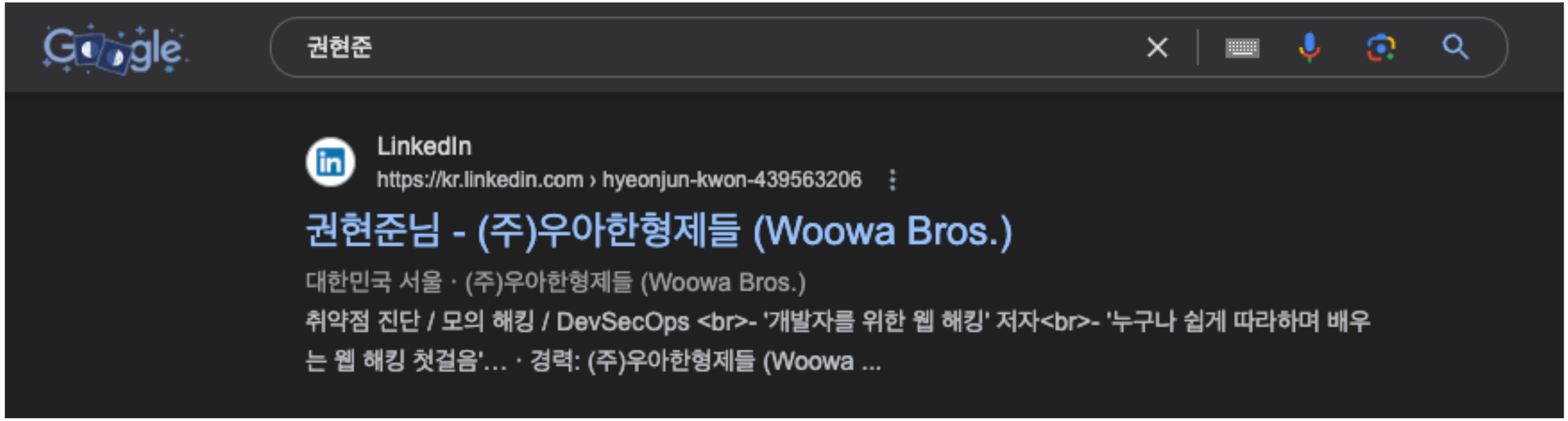
VPC Endpoint를 활용한

세상 하찮은 CCE 진단 자동화

제 소개는... 링크드인으로 대체합니다 ㅎㅎ

https://www.linkedin.com/in/hyeonjun-kwon-439563206/



F180

	B	C	D	E	F	G
178	**2.11.**	**사고 예방 및 대응**	2.11.1	사고 예방 및 대응체계 구축	침해사고 및 개인정보 유출 등을 예방하고 사고 발생 시 신속하고 효과적으로 대응할 수 있도록 내·외부 침해시도의 탐지·대응·분석 및 공유를 위한 체계와 절차를 수립하고, 관련 외부기관 및 전문가들과 협조체계를 구축하여야 한다.	침해사고 및 개인정보 유출사고를 예방하고 사고 발생 시 신속하고 효과적으로 대응하기 위한 체계와 절차를 마련하고 있는가?
179						보안관제서비스 등 외부 기관을 통해 침해사고 대응체계를 구축·운영하는 경우 침해사고 대응절차의 세부사항을 계약서에 반영하고 있는가?
180						침해사고의 모니터링, 대응 및 처리를 위하여 외부전문가, 전문업체, 전문기관 등과의 협조체계를 수립하고 있는가?
181			2.11.2	취약점 점검 및 조치	정보시스템의 취약점이 노출되어 있는지를 확인하기 위하여 정기적으로 취약점 점검을 수행하고 발견된 취약점에 대해서는 신속하게 조치하여야 한다. 또한 최신 보안취약점의 발생 여부를 지속적으로 파악하고 정보시스템에 미치는 영향을 분석하여 조치하여야 한다.	정보시스템 취약점 점검 절차를 수립하고 정기적으로 점검을 수행하고 있는가?
182						발견된 취약점에 대한 조치를 수행하고 그 결과를 책임자에게 보고하고 있는가?
183						최신 보안취약점 발생 여부를 지속적으로 파악하고 정보시스템에 미치는 영향을 분석하여 조치하고 있는가?
184						취약점 점검 이력을 기록관리하여 전년도에 도출된 취약점이 재발생하는 등의 문제점에 대해 보호대책을 마련하고 있는가?

전자금융감독규정

[시행 2024. 9. 15.] [금융위원회고시 제2024-44호, 2024. 9. 10., 일부개정]

제37조의2(전자금융기반시설의 취약점 분석 · 평가 주기, 내용 등) ① 전자금융기반시설의 취약점 분석 · 평가는 총자산이 2조원 이상이고, 상시 종업원 수(「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자를 기준으로 한다. 이하 같다) 300명 이상인 금융회사 또는 전자금융업자이거나 「수산업협동조합법」, 「산림조합법」, 「신용협동조합법」, 「상호저축은행법」 및 「새마을금고법」에 따른 중앙회의 경우 연 1회 이상(홈페이지에 대해서는 6개월에 1회 이상) 실시하여야 한다.

② 금융회사 및 전자금융업자는 취약점 분석 · 평가를 위하여 정보보호최고책임자(정보보호최고책임자가 없는 경우 최고경영자가 지정한다)를 포함하여 5인 이상으로 자체전담반을 구성하여야 하며, 구성원 중 100분의 30 이상은 「정보보호산업의 진흥에 관한 법률 시행규칙」 제8조의 정보보호 전문서비스 기업 지정기준에서 정한 고급 기술인력 이상의 자격을 갖춘 자이어야 한다. 다만, 제37조의3제1항에 따른 평가전문기관에 위탁하는 경우에는 자체전담반을 구성하지 아니할 수 있다. <개정 2016. 6. 30.>

③ 제1항에 따른 금융회사 및 전자금융업자 이외의 자의 경우 연 1회 이상(홈페이지에 대해서는 6개월에 1회 이상) 실시하되 자체전담반을 구성하지 아니할 수 있다. 이 경우 취약점 분석 · 평가의 내용은 금융감독원장이 정한다.

④ 금융회사 및 전자금융업자는 해당 주기 내에 평가 대상 시설과 평가기간을 나누어 평가할 수 있다.

⑤ 금융회사 또는 전자금융업자는 취약점 분석 · 평가에 따라 이행계획을 수립 · 시행하여야 하며 다음 각 호의 사항을 준수하여야 한다.

1. 취약점 분석 · 평가 결과에 따른 취약점의 제거 또는 이에 상응하는 조치의 시행
2. 취약점의 제거 또는 이에 상응하는 조치가 불가한 경우에는 최고경영자 승인을 득할 것
3. 이행계획의 시행 결과는 최고경영자에게 보고할 것

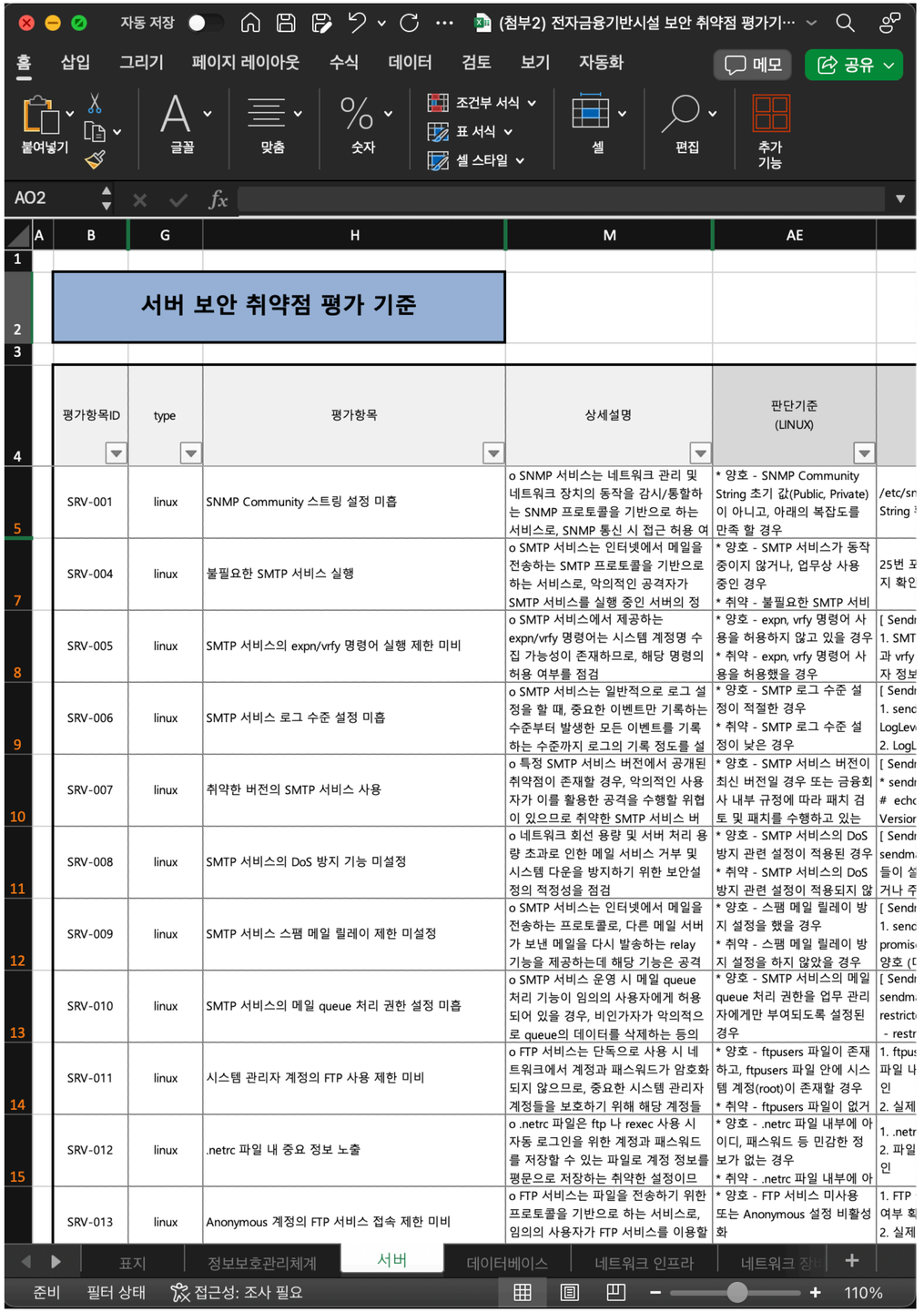
⑥ 금융회사 또는 전자금융업자는 제1항 또는 제3항에 따른 의무의 이행을 위하여 전자금융보조업자에게 협조를 요청할 수 있다. <신설 2018. 12. 21.>

제37조의3(전자금융기반시설의 취약점 분석 · 평가 전문기관의 지정 등) ① 전자금융기반시설의 취약점 분석 · 평가를 위한 평가전문기관은 다음 각 호의 자로 한다.

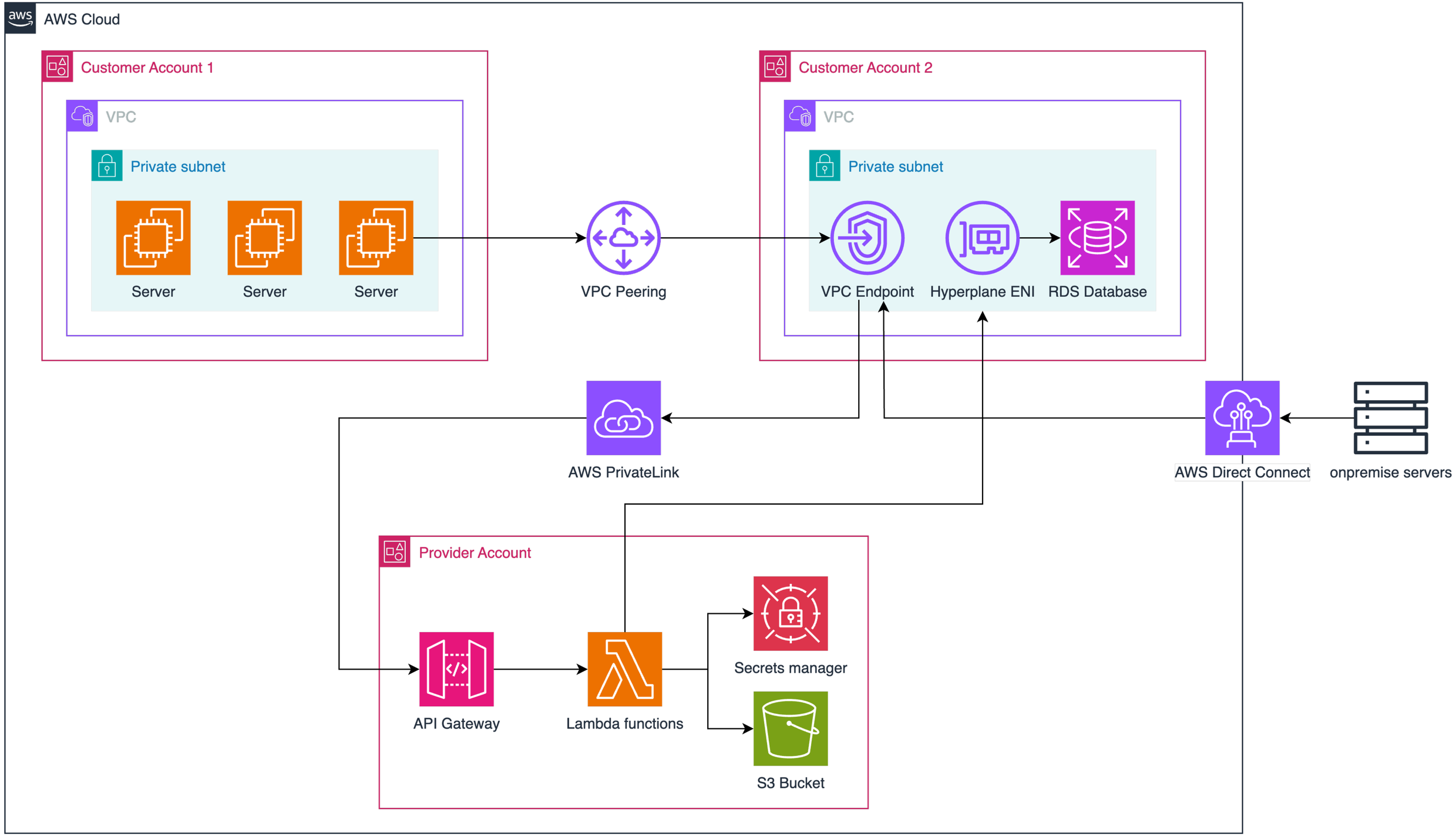
1. 「정보통신기반 보호법」 제16조에 따라 금융분야 정보공유 · 분석센터로 지정된 자
2. 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 정보보호전문서비스 기업 <개정 2016. 6. 30.>
3. 침해사고대응기관
4. 금융위원장이 지정하는 자

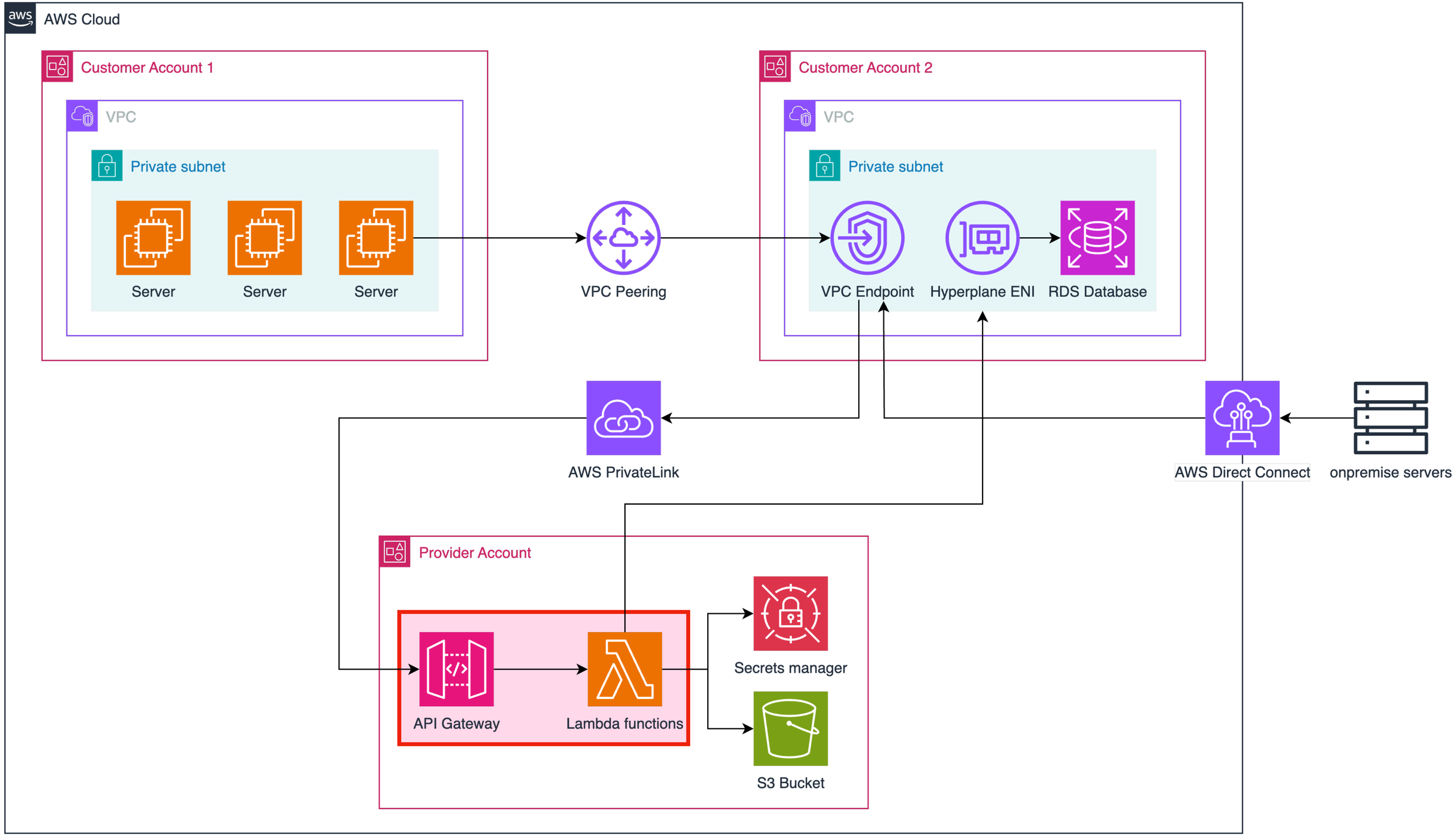
② 금융회사 및 전자금융업자는 시행령 제11조의5제3항에 따른 전자금융기반시설의 취약점 분석 · 평가 결과보고서를 금융위원장에게 제출하여야 하며, 금융감독원장은 결과보고서를 분석하여 매분기 1개월 이내에 금융위원장에게 보고하여야 한다.

③ 금융위원장은 취약점 분석 · 평가 결과보고서에 근거하여 필요시 금융회사 및 전자금융업자에 대하여 개선 · 보완을 요구할 수 있다.



평가항목ID	type	평가항목	상세설명	판단기준 (LINUX)	
SRV-001	linux	SNMP Community 스트링 설정 미흡	o SNMP 서비스는 네트워크 관리 및 네트워크 장치의 동작을 감시/통합하는 SNMP 프로토콜을 기반으로 하는 서비스로, SNMP 통신 시 접근 허용 여	* 양호 - SNMP Community String 초기 값(Public, Private)이 아니고, 아래의 복잡도를 만족 할 경우	/etc/sn String
SRV-004	linux	불필요한 SMTP 서비스 실행	o SMTP 서비스는 인터넷에서 메일을 전송하는 SMTP 프로토콜을 기반으로 하는 서비스로, 악의적인 공격자가 SMTP 서비스를 실행 중인 서버의 정	* 양호 - SMTP 서비스가 동작 중이지 않거나, 업무상 사용 중인 경우 * 취약 - 불필요한 SMTP 서비	25번 포 지 확인
SRV-005	linux	SMTP 서비스의 expn/vrfy 명령어 실행 제한 미비	o SMTP 서비스에서 제공하는 expn/vrfy 명령어는 시스템 계정명 수집 가능성이 존재하므로, 해당 명령의 허용 여부를 점검	* 양호 - expn, vrfy 명령어 사용을 허용하지 않고 있을 경우 * 취약 - expn, vrfy 명령어 사용을 허용했을 경우	[Sendr 1. SMT 과 vrfy 자 정보
SRV-006	linux	SMTP 서비스 로그 수준 설정 미흡	o SMTP 서비스는 일반적으로 로그 설정을 할 때, 중요한 이벤트만 기록하는 수준부터 발생한 모든 이벤트를 기록하는 수준까지 로그의 기록 정도를 설	* 양호 - SMTP 로그 수준 설정이 적절한 경우 * 취약 - SMTP 로그 수준 설정이 낮은 경우	[Sendr 1. senc LogLev 2. LogL
SRV-007	linux	취약한 버전의 SMTP 서비스 사용	o 특정 SMTP 서비스 버전에서 공개된 취약점이 존재할 경우, 악의적인 사용자가 이를 활용한 공격을 수행할 위협이 있으므로 취약한 SMTP 서비스 버	* 양호 - SMTP 서비스 버전이 최신 버전일 경우 또는 금융회사 내부 규정에 따라 패치 검토 및 패치를 수행하고 있는	[Sendr * sendr # echo Versior
SRV-008	linux	SMTP 서비스의 DoS 방지 기능 미설정	o 네트워크 회선 용량 및 서버 처리 용량 초과로 인한 메일 서비스 거부 및 시스템 다운을 방지하기 위한 보안설정의 적정성을 점검	* 양호 - SMTP 서비스의 DoS 방지 관련 설정이 적용된 경우 * 취약 - SMTP 서비스의 DoS 방지 관련 설정이 적용되지 않	[Sendr sendm 들이 설 거나 주
SRV-009	linux	SMTP 서비스 스팸 메일 릴레이 제한 미설정	o SMTP 서비스는 인터넷에서 메일을 전송하는 프로토콜로, 다른 메일 서버가 보낸 메일을 다시 발송하는 relay 기능을 제공하는데 해당 기능은 공격	* 양호 - 스팸 메일 릴레이 방지 설정을 했을 경우 * 취약 - 스팸 메일 릴레이 방지 설정을 하지 않았을 경우	[Sendr 1. senc promis 양호 (
SRV-010	linux	SMTP 서비스의 메일 queue 처리 권한 설정 미흡	o SMTP 서비스 운영 시 메일 queue 처리 기능이 임의의 사용자에게 허용되어 있을 경우, 비인가자가 악의적으로 queue의 데이터를 삭제하는 등의	* 양호 - SMTP 서비스의 메일 queue 처리 권한을 업무 관리자에게만 부여되도록 설정된 경우	[Sendr sendm restrict - restr
SRV-011	linux	시스템 관리자 계정의 FTP 사용 제한 미비	o FTP 서비스는 단독으로 사용 시 네트워크에서 계정과 패스워드가 암호화되지 않으므로, 중요한 시스템 관리자 계정들을 보호하기 위해 해당 계정들	* 양호 - ftpusers 파일이 존재하고, ftpusers 파일 안에 시스템 계정(root)이 존재할 경우 * 취약 - ftpusers 파일이 없거	1. ftpus 파일 나 인 2. 실제
SRV-012	linux	.netrc 파일 내 중요 정보 노출	o .netrc 파일은 ftp 나 rexec 사용 시 자동 로그인을 위한 계정과 패스워드를 저장할 수 있는 파일로 계정 정보를 평문으로 저장하는 취약한 설정이므	* 양호 - .netrc 파일 내부에 아이디, 패스워드 등 민감한 정보가 없는 경우 * 취약 - .netrc 파일 내부에 아	1. .netr 2. 파일 인
SRV-013	linux	Anonymous 계정의 FTP 서비스 접속 제한 미비	o FTP 서비스는 파일을 전송하기 위한 프로토콜을 기반으로 하는 서비스로, 임의의 사용자가 FTP 서비스를 이용할	* 양호 - FTP 서비스 미사용 또는 Anonymous 설정 비활성화	1. FTP 여부 확 2. 실제


AWS Cloud
Customer Account 1
VPC
Private subnet
Server
Server
Server
VPC Peering
Customer Account 2
VPC
Private subnet
VPC Endpoint
Hyperplane ENI
RDS Database
AWS PrivateLink
AWS Direct Connect
onpremise servers
Provider Account
API Gateway
Lambda functions
Secrets manager
S3 Bucket


AWS Cloud
Customer Account 1
VPC
Private subnet
Server
Server
Server
VPC Peering
Customer Account 2
VPC
Private subnet
VPC Endpoint
Hyperplane ENI
RDS Database
AWS PrivateLink
AWS Direct Connect
onpremise servers
Provider Account
API Gateway
Lambda functions
Secrets manager
S3 Bucket

왜 API Gateway + Lambda를...?

API Gateway란?

클라이언트와 서버 간의 중개 역할을 하는 서비스로, API 요청을 수신하고 이를 적절한 백엔드 서비스로 전달하는 기능을 수행

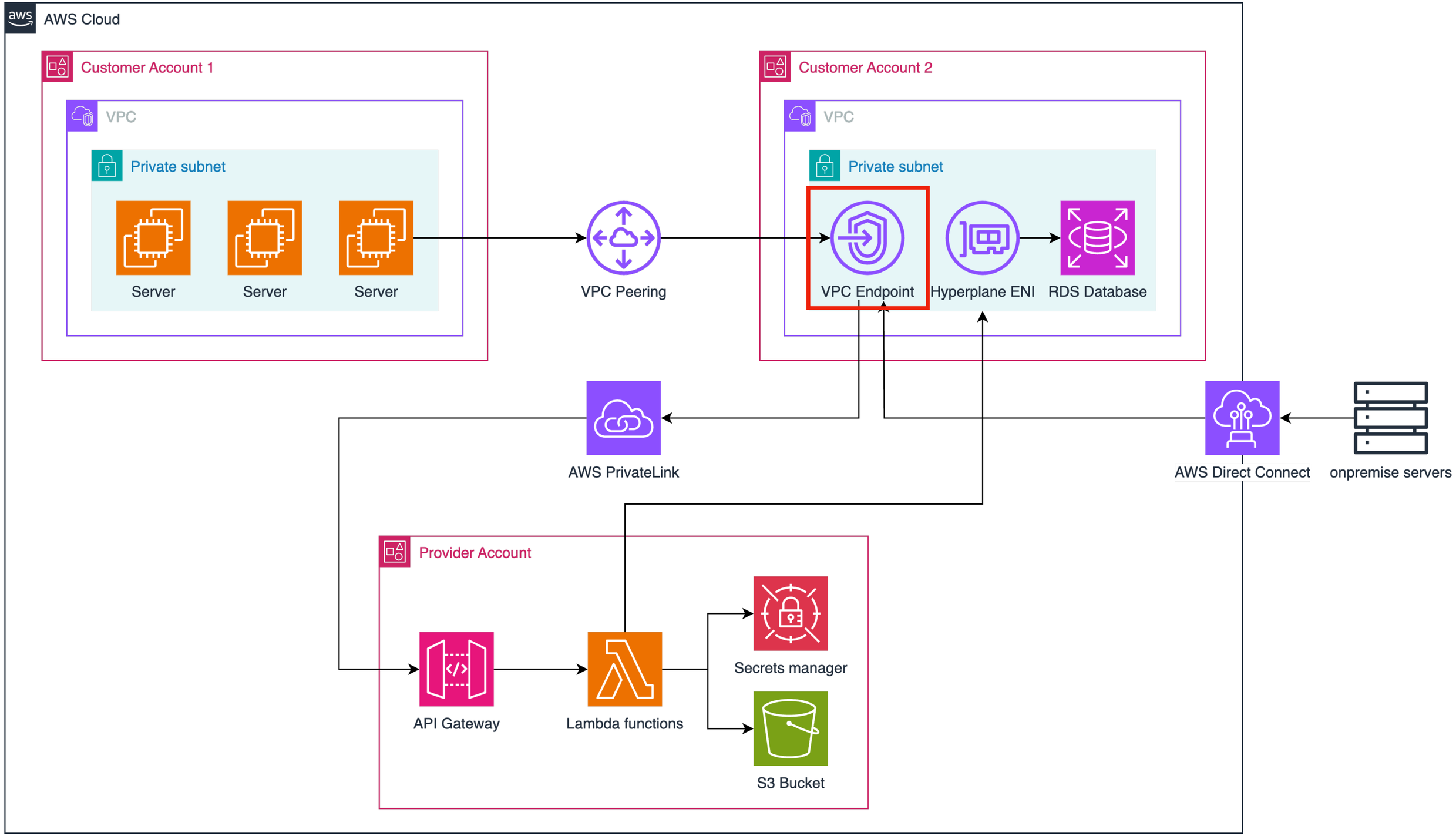
서버리스 아키텍처에서 많이 사용됨

Lambda란?

서버를 구성하고 관리할 필요 없이 코드를 실행 시킬 수 있도록

AWS에서 제공하는 서비스 (PaaS라고도, FaaS라고도 함)

- 서버를 구축할 필요가 없음
- 사용한 만큼만 지불하면 됨
- 개발 시간 단축


AWS Cloud
Customer Account 1
VPC
Private subnet
Server
Server
Server
VPC Peering
Customer Account 2
VPC
Private subnet
VPC Endpoint
Hyperplane ENI
RDS Database
AWS PrivateLink
AWS Direct Connect
onpremise servers
Provider Account
API Gateway
Lambda functions
Secrets manager
S3 Bucket

VPC Endpoint란?

- VPC 내에서 AWS 서비스에 안전하게 연결할 수 있도록 해주는 기능

- VPC Endpoint를 사용하면 인터넷을 거치지 않고도 AWS 서비스에 접근할 수 있어 보안과 성능을 향상시킬 수 있음

- VPC Endpoint에는 ENI를 생성하여 AWS PrivateLink 기능을 활용해 Internal 통신을 수행하는 Interface Endpoint 방식과 VPC내 라우팅 테이블을 수정하여 바로 AWS Service로 접근 가능하게 하는 Gateway Endpoint 방식이 있음

VPC Endpoint는 왜 썼을까?

불필요한 Public call을 만들지 않으려고!

Public Call이란?

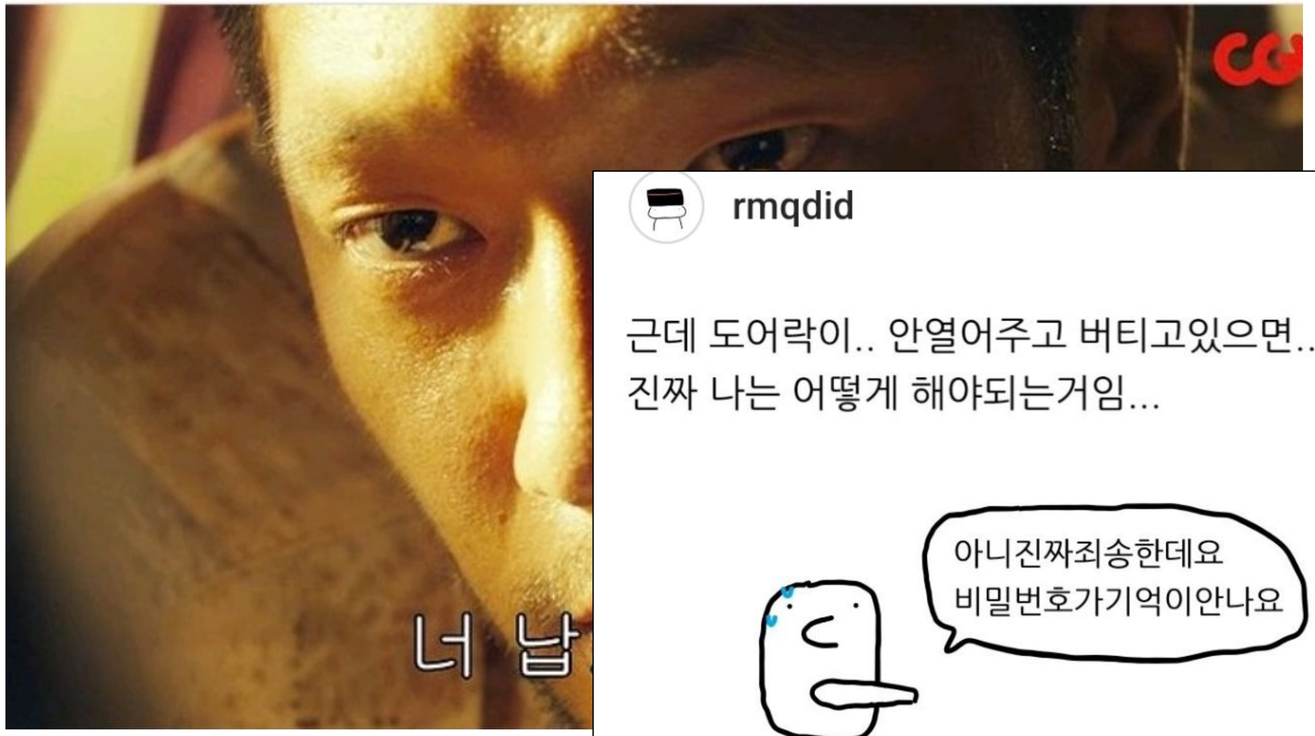
외부 네트워크를 통해 이루어지는 통신

불필요한 Public Call이란?

내부 네트워크에서 직접 통신할 수 있는 상황에서 외부 네트워크를 통해 통신하는 것

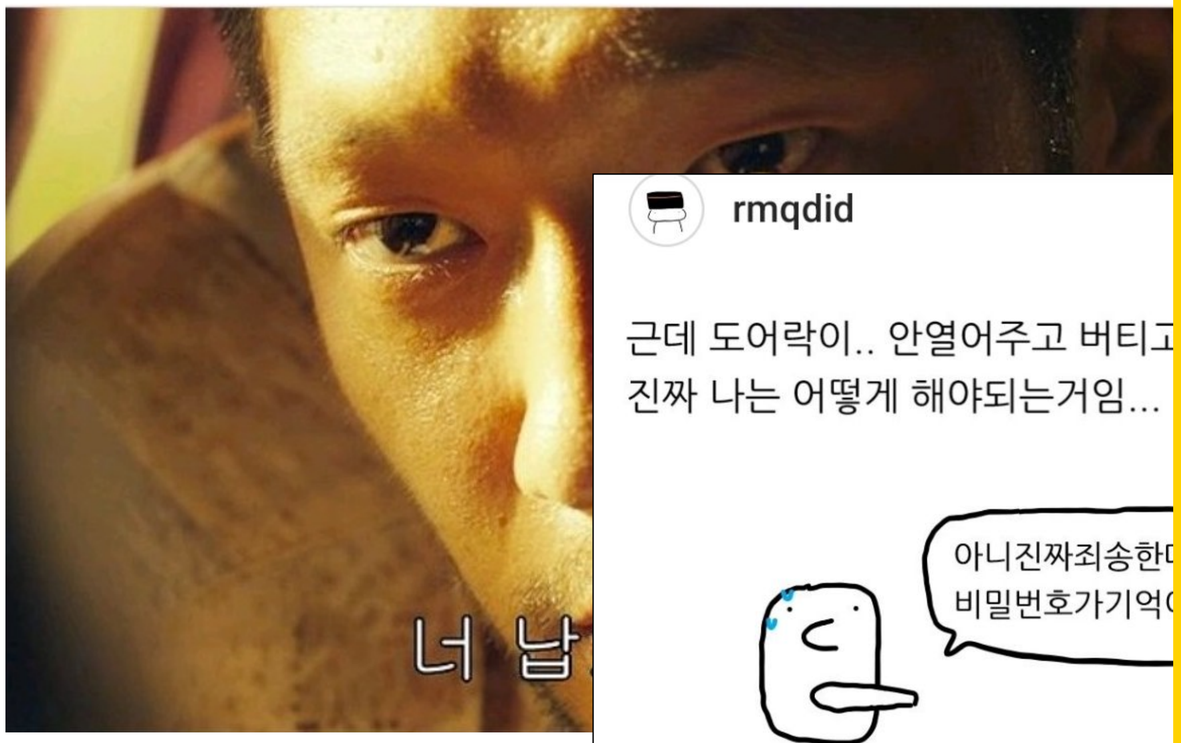

와서 불 좀 꺼줘


너 납치된거야



rmqdid

근데 도어락이.. 안열어주고 버티고있으면..
진짜 나는 어떻게 해야되는거임...



rmqdid

근데 도어락이.. 안열어주고 버티고
진짜 나는 어떻게 해야되는거임...

체력 쓰레기들 특징

Feat. 얜뭐지?

알바천국

보안 위험 증가

데이터가 공격자에게 노출될 위험이 커지며, 이는 데이터 유출, 변조, 또는 서비스 거부 공격(DoS) 등의 보안 위협을 초래할 수 있음

성능 저하

외부 네트워크를 통한 통신은 내부 네트워크보다 지연(latency)이 발생할 가능성이 높아, 데이터 전송 속도 저하와 응답 시간 증가로 이어질 수 있으며, 이는 전체 시스템 성능에 부정적인 영향을 줌

비용 증가

외부 네트워크를 통해 데이터를 전송하는 경우, 트래픽 발생 비용 또는 리소스 사용 비용이 과도하게 발생할 수 있음

복잡한 관리

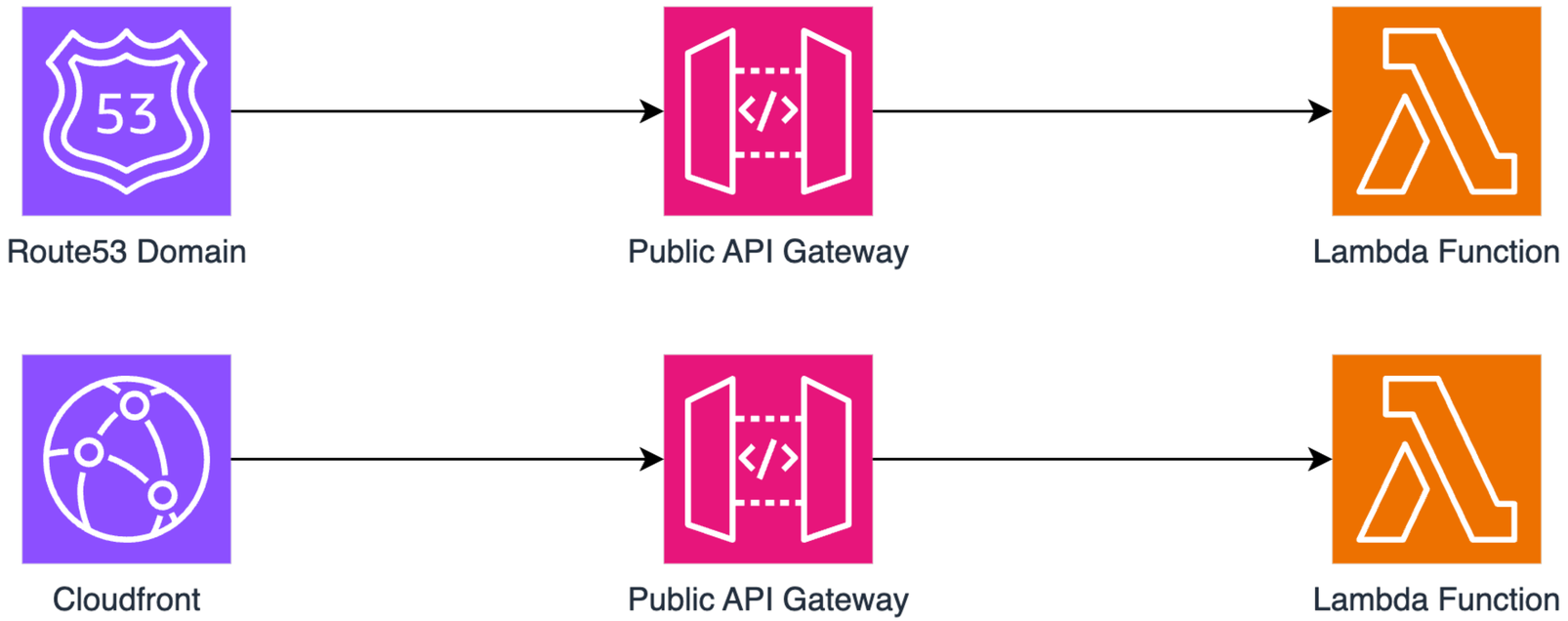
API 버전 관리, 인증 및 권한 부여, 데이터 형식 변환, 보안성 검토 등 추가적인 작업이 필요해짐

규제 및 컴플라이언스 문제:

특정 산업에서는 데이터가 외부로 전송되는 것을 제한하는 규제가 존재하여, 이를 준수하지 않을 경우 법적 문제가 발생할 수 있음


굳이... 할 필요가

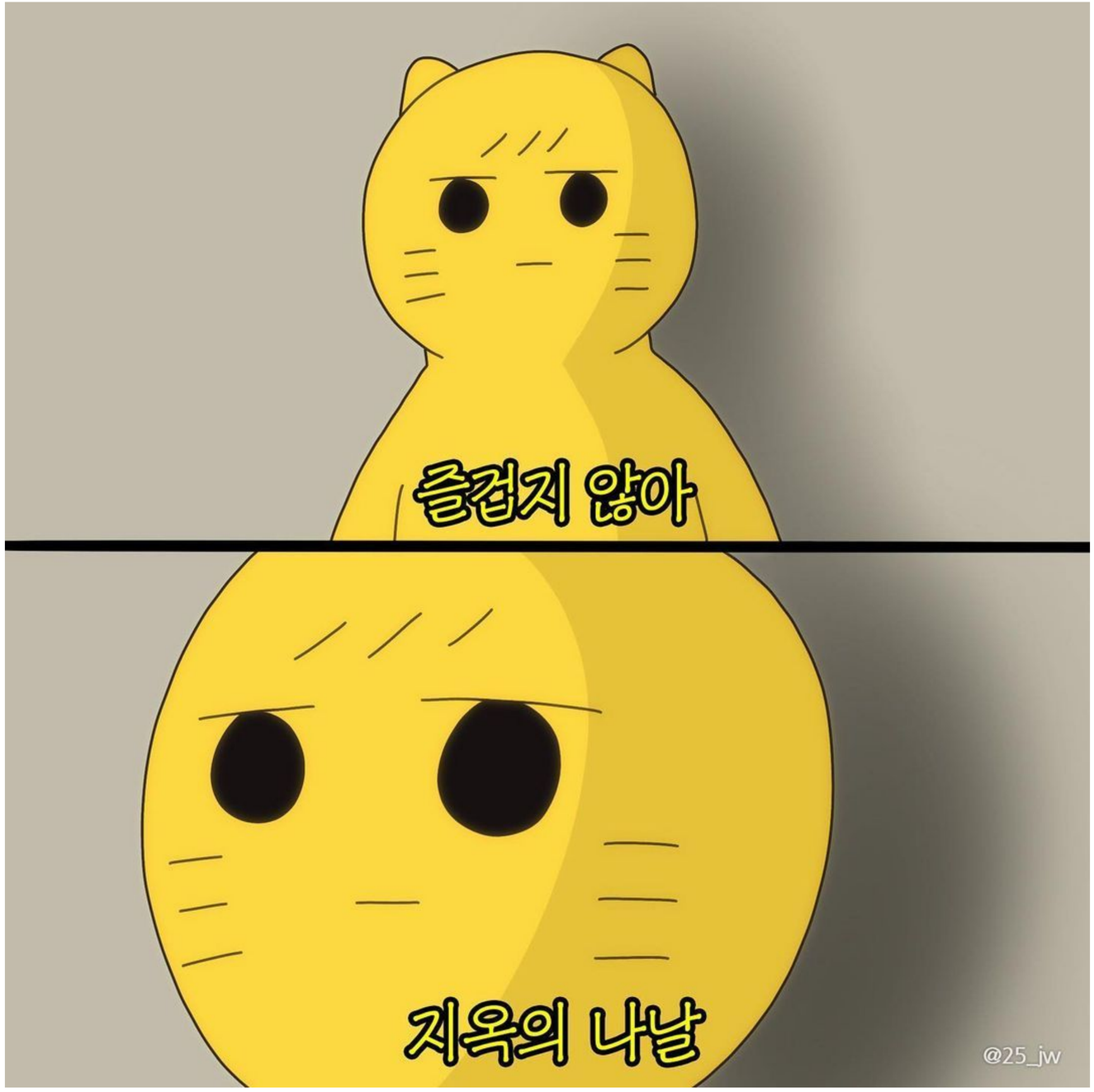
Public Call 예시



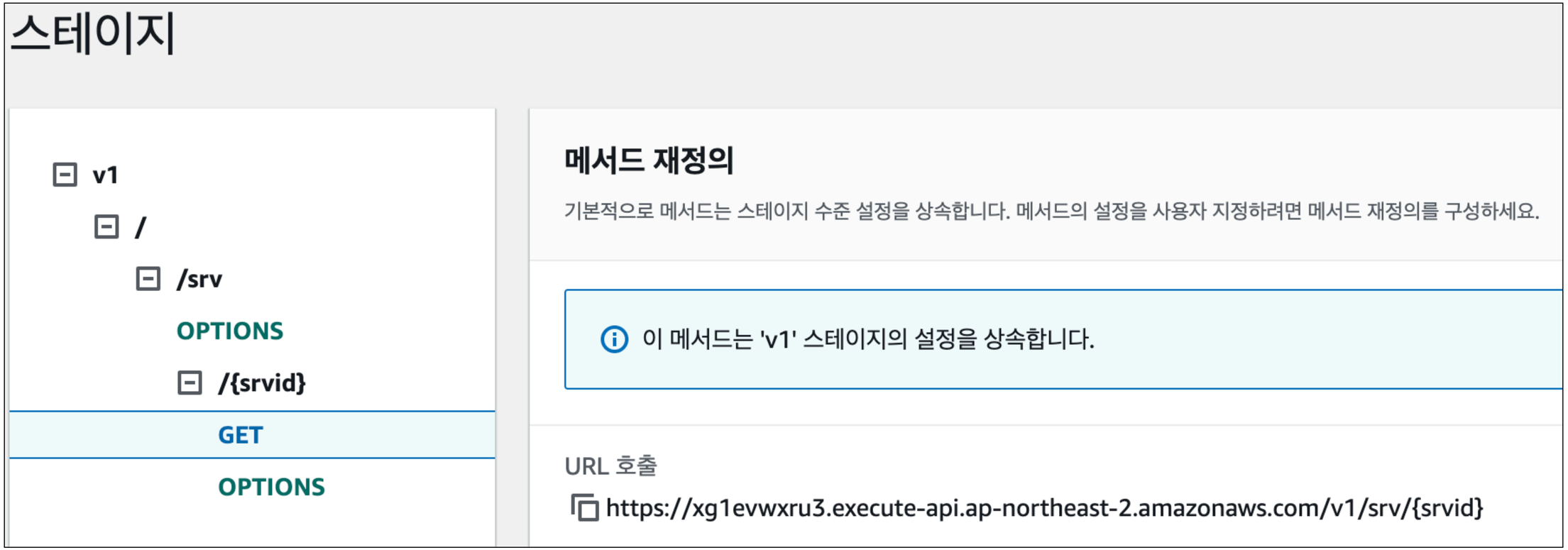
External 서비스를 운영한다면 문제없는 구성이지만,

Internal 서비스라면 이는 불필요한 Public Call을 유발함

API Gateway를 프라이빗으로 바꾸면 되잖아요!


즐겁지 않아
지옥의 나날
@25_jw

먼저 VPC Endpoint를 만들자




```
[ec2-user@ip-10-111-1-38 ~]$ curl https://xg1evwxru3.execute-api.ap-northeast-2.amazonaws.com/v1/srv/1
-H "X-api-key: 63LS9P3p3b6KKcqQN8Yrc4cPAUQThjx83rHaUglM"
{"aws_account_id": "385423560848", "aws_account_name": "X01", "instance-id": "i-123123123", "os": "linu
x", "version": "Ubuntu 22.04 LTS", "ip": "192.168.0.2", "name": "kwon-blue-leader", "service": "test-se
rvice", "role": "test-service-role", "alive": 1, "etc": "for server comment"}[ec2-user@ip-10-111-1-38 ~
]$
```

vpce-00dd553ddfb9d9452 / kwon-apigw-endpoint

세부 정보 | 서브넷 | 보안 그룹 | 알림 | 정책 | 모니터링 | 태그

세부 정보

엔드포인트 ID
vpce-[redacted]

VPC ID
[redacted]

DNS 레코드 IP 유형
ipv4

프라이빗 DNS 전용 인바운드 해석기 엔드포인트
–

상태
대기 중

상태 메시지
–

IP 주소 유형
ipv4

생성 시간
2024년 10월 24일 목요일 04시 28분 9초 GMT+9

서비스 이름
com.amazonaws.ap-northeast-2.execute-api

DNS 이름
vpce-[redacted]

vpce-[redacted]

엔드포인트 유형
Interface

프라이빗 DNS 이름 활성화됨
예

프라이빗 DNS 이름
*.execute-api.ap-northeast-2.amazonaws.com

```
[ec2-user@ip-10-111-1-38 ~]$ curl https://xg1evwxru3.execute-api.ap-northeast-2.amazonaws.com/v1/srv/1
-H "X-api-key: 63LS9P3p3b6KKcqQN8Yrc4cPAUQThjx83rHaUglM"
{"message":"Forbidden"}[ec2-user@ip-10-111-1-38 ~]$
```

VPC Endpoint를 만들면...

VPC -> Public API Gateway

통신이 안된다..!

즉 장애가 날 수 있다..!

여차저차해서 VPC Endpoint를 만들었다..

이제 API Gateway를 프라이빗으로!

API 설정

API 세부 정보

API 이름
kwon-apigw-test

설명
-

API 키 소스
Header

콘텐츠 인코딩
비활성

ARN
arn:aws:apigateway:ap-northeast-2::/restapis/xg1evwxru3

기본 엔드포인트
활성
https://xg1evwxru3.execute-api.ap-northeast-2.amazonaws.com

API 엔드포인트 유형
Private

```
[ec2-user@ip-10-111-1-38 ~]$ curl https://xg1evwxru3.execute-api.ap-northeast-2.amazonaws.com/v1/srv/1
-H "X-api-key: 63LS9P3p3b6KKcqQN8Yrc4cPAUQThjx83rHaUglM"
{"aws_account_id": "385423560848", "aws_account_name": "X01", "instance-id": "i-123123123", "os": "linu
x", "version": "Ubuntu 22.04 LTS", "ip": "192.168.0.2", "name": "kwon-blue-leader", "service": "test-se
rvice", "role": "test-service-role", "alive": 1, "etc": "for server comment"}[ec2-user@ip-10-111-1-38 ~
]$
```

성공!

이제 Direct connect랑 다른 VPC에서 테스트 해볼까?

```
hjkwon0825 ~ curl https://xg1evwxru3.execute-api.ap-northeast-2.amazonaws.com/v1/srv/1
-H "X-api-key: 63LS9P3p3b6KKcqQN8Yrc4cPAUQThjx83rHaUglM"
curl: (6) Could not resolve host: xg1evwxru3.execute-api.ap-northeast-2.amazonaws.com
```

```
hjkwon0825 ~ nslookup
> xg1evwxru3.execute-api.ap-northeast-2.amazonaws.com
Server:         8.8.8.8
Address:        8.8.8.8#53

** server can't find xg1evwxru3.execute-api.ap-northeast-2.amazonaws.com: NXDOMAIN
>
```

Private API Gateway는
VPC Endpoint가 설정된 VPC 안에서만
호출이 되는 것이었다...

삽질 1. 도메인을 통한 직접 연결 시도

API Gateway의 REST API에 대한 사용자 지정 도메인 이름

PDF | RSS

*사용자 지정 도메인 이름*은 API 사용자에게 제공할 수 있는 더 간단하고 직관적인 URL입니다.

API를 배포한 후 사용자 및 사용자 고객은 다음 형식의 기본 URL을 사용하여 API를 호출할 수 있습니다.

```
https://api-id.execute-api.region.amazonaws.com/stage
```

여기서 `api-id`는 API Gateway에서 생성되고 `region`은 AWS 리전이며 `stage`는 API를 배포할 때 사용자가 지정합니다.

URL의 호스트 이름 부분(즉, `api-id.execute-api.region.amazonaws.com`)은 API 엔드포인트를 가리킵니다. 기본 API 엔드포인트는 임의로 생성되므로 기억하기가 어려우며 사용자 친화적이지 않습니다.

사용자 지정 도메인 이름을 사용하면 API의 호스트 이름을 설정하고 기본 경로(예: `myservice`)를 선택하여 대체 URL을 API에 매핑할 수 있습니다. 예를 들어, 더 사용자 친화적인 API 기본 URL은 다음과 같습니다.

```
https://api.example.com/myservice
```

고려 사항

다음 고려 사항은 사용자 지정 도메인 이름 사용에 영향을 미칠 수 있습니다.

- 사용자 지정 도메인 이름은 프라이빗 API에 사용할 수 없습니다.

삽질 1. 도메인을 통한 직접 연결 시도

API Gateway의 REST API에 대한 사용자 지정 도메인 이름

PDF | RSS

*사용자 지정 도메인 이름*은 API 사용자에게 제공할 수 있는 더 간단하고 직관적 니다.

API를 배포한 후 사용자 및 사용자 고객은 다음 형식의 기본 URL을 사용하여 API 있습니다.

```
https://api-id.execute-api.region.amazonaws.com/stage
```

여기서 *api-id*는 API Gateway에서 생성되고 *region*은 AWS 리전이며 *stage*는 API 사용자가 지정합니다.

URL의 호스트 이름 부분(즉, *api-id*.execute-api.*region*.amazonaws.co 를 가리킵니다. 기본 API 엔드포인트는 임의로 생성되므로 기억하기가 어려우며 사용자 친화적이지 않습니다.

사용자 지정 도메인 이름을 사용하면 API의 호스트 이름을 설정하고 기본 경로(예: m)를 선택 L을 API에 매핑할 수 있습니다. 예를 들어, 더 사용자 친화적인 API 기본 URL은 다음과 같습니다.

```
https://api.example.com/myservice
```

고려 사항

다음 고려 사항은 사용자 지정 도메인 이름 사용에 영향을 미칠 수 있습니다.

- 사용자 지정 도메인 이름은 프라이빗 API에 사용할 수 없습니다.

삽질 2. NLB를 통한 VPC Endpoint 직접 연결 시도

vpce-029c03d6091cea68b / kwon-apigw-endpoint

세부 정보 | 서브넷 | 보안 그룹 | 알림 | 정책 | 모니터링 | 태그

세부 정보

엔드포인트 ID
vpce-029c03d6091cea68b

VPC ID
vpc-02f52e24ee170ef78 (vpc-x02-play-default-use)

DNS 레코드 IP 유형
ipv4

프라이빗 DNS 전용 인바운드 해석기 엔드포인트
–

상태
사용 가능

상태 메시지
–

IP 주소 유형
ipv4

생성 시간
2024년 10월 24일 목요일 04시 54분 41초 GMT+9

서비스 이름
com.amazonaws.ap-northeast-2.execute-api

DNS 이름
vpce-029c03d6091cea68b-qyyngyhn.execute-api.ap-northeast-2.vpce.amazonaws.com
- (Z27UANNT0PRK1T)
vpce-029c03d6091cea68b-qyyngyhn-ap-northeast-2c.execute-api.ap-northeast-2.vpce.amazonaws.com
- (Z27UANNT0PRK1T)

엔드포인트 유형
Interface

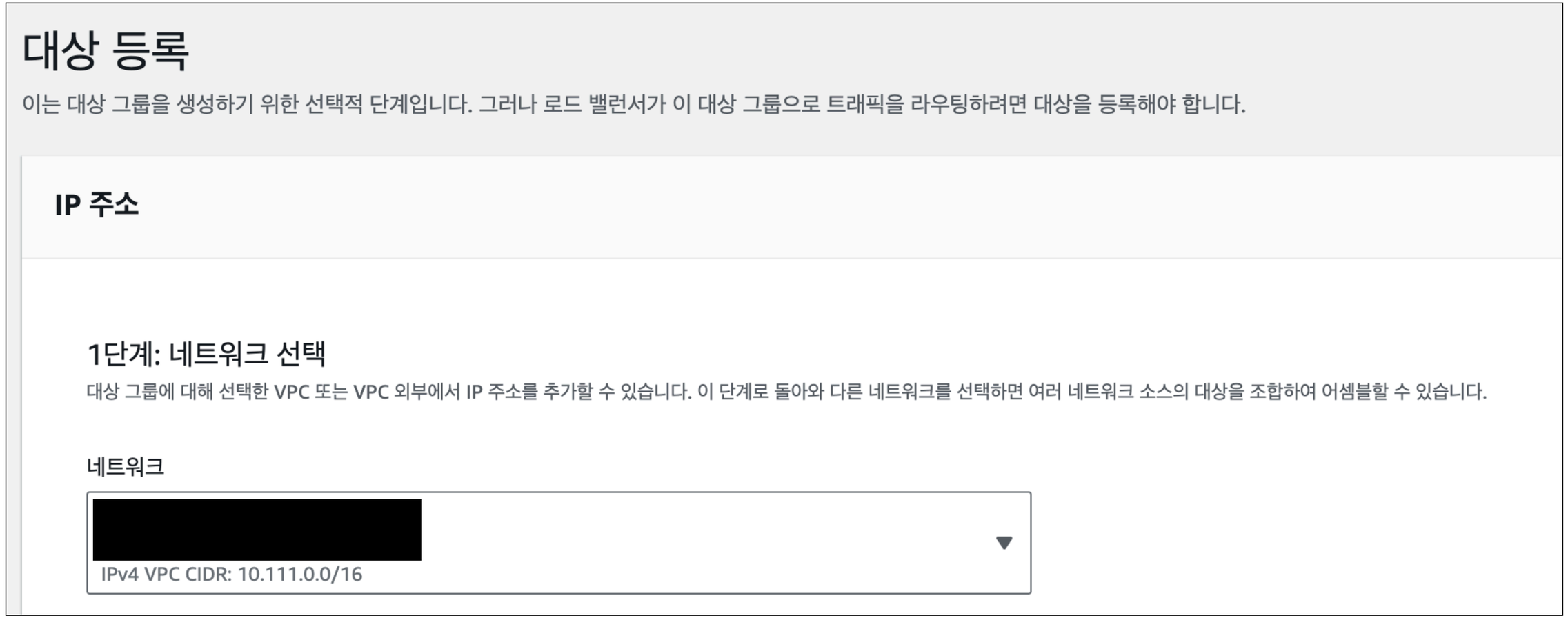
프라이빗 DNS 이름 활성화됨
예

프라이빗 DNS 이름
*.execute-api.ap-northeast-2.amazonaws.com

```
[ec2-user@ip-10-111-1-38 ~]$ nslookup
> vpce-                  -qyyngyhn.execute-api.ap-northeast-2.vpce.amazonaws.com
Server:         169.254.169.253
Address:        169.254.169.253#53

Non-authoritative answer:
Name:   vpce-                  -qyyngyhn.execute-api.ap-northeast-2.vpce.amazonaws.com
Address: 10.111.4.238
Name:   vpce-                  -qyyngyhn.execute-api.ap-northeast-2.vpce.amazonaws.com
Address: 10.111.0.213
>
```

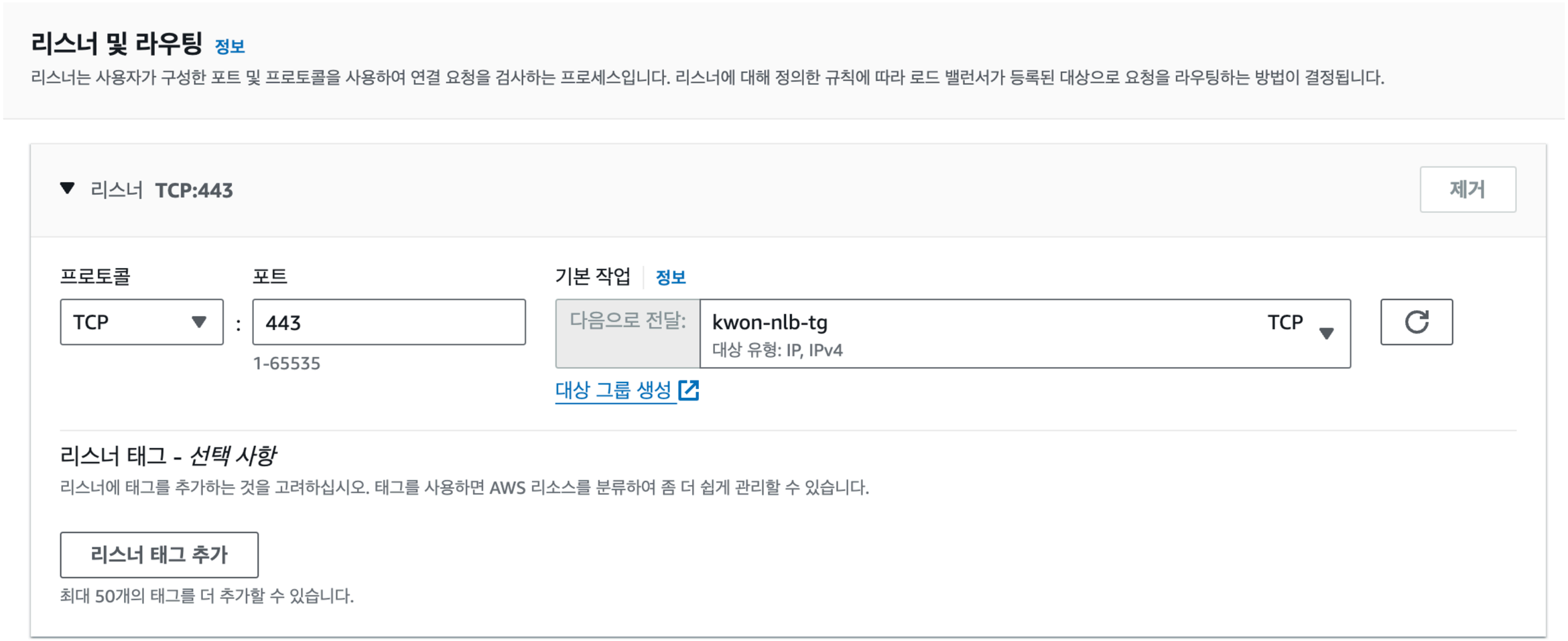
삽질 2. NLB를 통한 VPC Endpoint 직접 연결 시도



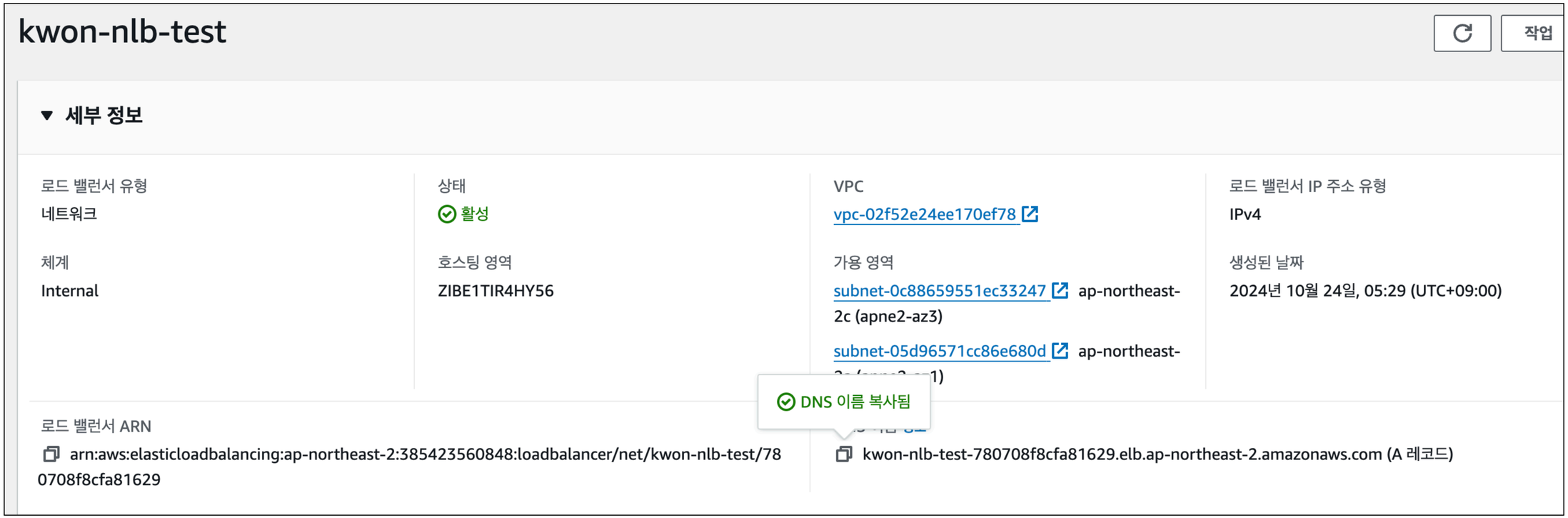
삽질 2. NLB를 통한 VPC Endpoint 직접 연결 시도

삽질 2. NLB를 통한 VPC Endpoint 직접 연결 시도

삽질 2. NLB를 통한 VPC Endpoint 직접 연결 시도



삽질 2. NLB를 통한 VPC Endpoint 직접 연결 시도




```
hjkwon0825 ~ nslookup
> kwon-nlb-test-780708f8cfa81629.elb.ap-northeast-2.amazonaws.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   kwon-nlb-test-780708f8cfa81629.elb.ap-northeast-2.amazonaws.com
Address: 10.111.11.135
>
```

삽질 2. NLB를 통한 VPC Endpoint 직접 연결 시도

엔드포인트별 퍼블릭 DNS 호스트 이름을 사용하여 프라이빗 API 간접 호출

엔드포인트 특정한 DNS 호스트 이름을 사용하여 프라이빗 API에 액세스할 수 있습니다. 이들 이름은 프라이빗 API에 대한 VPC 엔드포인트 ID 또는 API ID가 포함된 퍼블릭 DNS 호스트 이름입니다.

생성된 기본 URL의 형식은 다음과 같습니다.

```
https://{public-dns-hostname}.execute-api.{region}.vpce.amazonaws.com/{stage}
```

예를 들어 `test` 스테이지에 대한 `GET /pets` 메서드를 설정하고 REST API ID가 `abc1234`, 퍼블릭 DNS 호스트 이름이 `vpce-def-01234567`, 리전이 `us-west-2`인 경우 cURL 명령으로 `Host` 헤더를 사용하여 VPCe ID로 프라이빗 API를 간접적으로 호출할 수 있습니다.

```
curl -v https://vpce-def-01234567.execute-api.us-west-2.vpce.amazonaws.com/test/pets
```

또는 다음 형식의 cURL 명령으로 `x-apigw-api-id` 헤더를 사용하여 API ID를 통해 프라이빗 API를 간접적으로 호출할 수 있습니다.

```
curl -v https://{public-dns-hostname}.execute-api.{region}.vpce.amazonaws.com/{stage}
```

삽질 2. NLB를 통한 VPC Endpoint 직접 연결 시도

```
hjkwon0825 ~ curl https://kwon-nlb-test-780708f8cfa81629.elb.ap-northeast-2.amazonaws.com/v1/srv/1 -H 'x-apigw-api-id:xg1evwxru3' -H "X-api-key: 63LS9P3p3b6KKcqQN8Yrc4cPAUQThjx83rHaUglM"
curl: (60) SSL: no alternative certificate subject name matches target host name 'kwon-nlb-test-780708f8cfa81629.elb.ap-northeast-2.amazonaws.com'
More details here: https://curl.se/docs/sslcerts.html

curl failed to verify the legitimacy of the server and therefore could not
establish a secure connection to it. To learn more about this situation and
how to fix it, please visit the web page mentioned above.
```

```
hjkwon0825 ~ curl https://kwon-nlb-test-780708f8cfa81629.elb.ap-northeast-2.amazonaws.com/v1/srv/1 -H 'x-apigw-api-id:xg1evwxru3' -H "X-api-key: 63LS9P3p3b6KKcqQN8Yrc4cPAUQThjx83rHaUglM" -k
{"aws_account_id": "385423560848", "aws_account_name": "X01", "instance-id": "i-123123123", "os": "linux", "version": "Ubuntu 22.04 LTS", "ip": "192.168.0.2", "name": "kwon-blue-leader", "service": "test-service", "role": "test-service-role", "alive": 1, "etc": "for server comment"}%
```

삽질 2. NLB를 통한 VPC Endpoint 직접 연결 시도

삽질 2. NLB를 통한 VPC Endpoint 직접 연결 시도

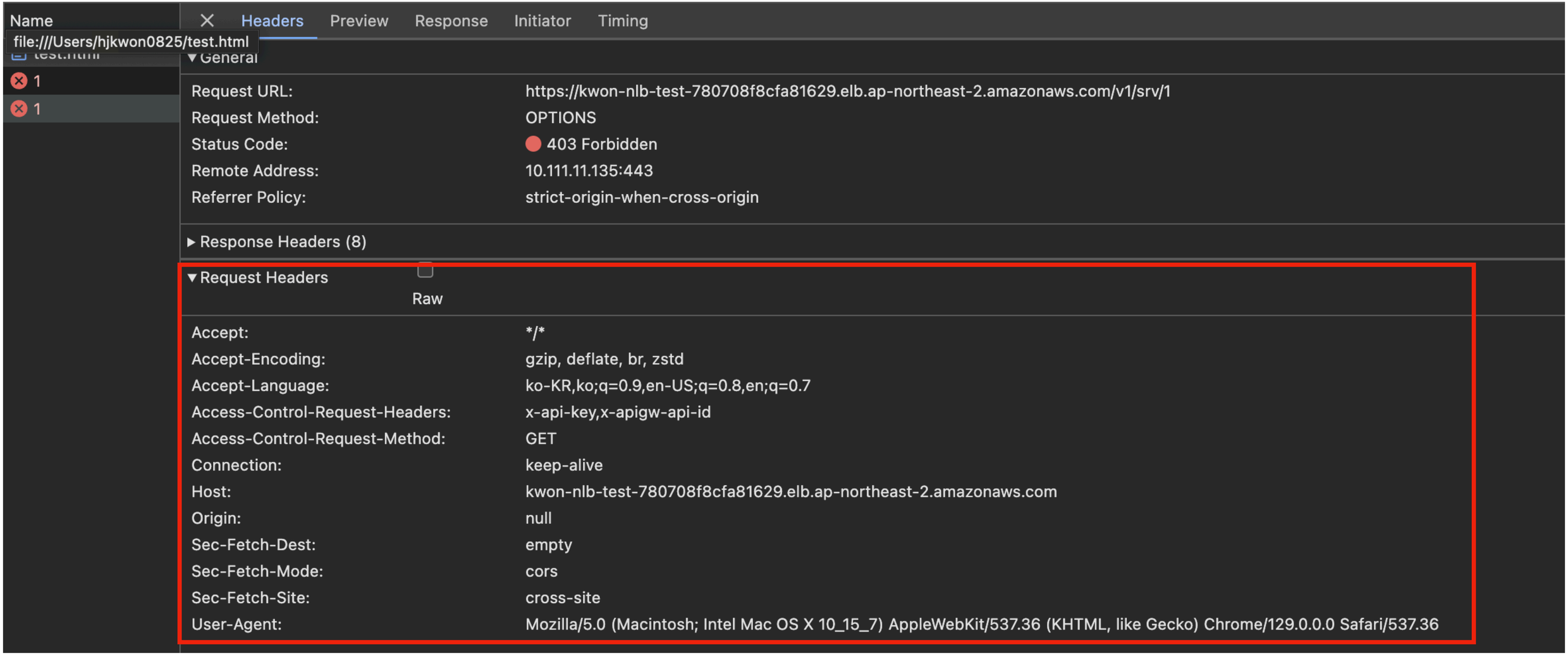
삽질 2. NLB를 통한 VPC Endpoint 직접 연결 시도

```html
<html>
  <head>
    <script>
      const url = 'https://kwon-nlb-test-780708f8cfa81629.elb.ap-northeast-2.amazonaws.com/v1/srv/1';
      const headers = {
        'x-apigw-api-id': 'xg1evwxru3',
        'X-api-key': '63LS9P3p3b6KKcqQN8Yrc4cPAUQThjx83rHaUglM'
      };
      fetch(url, {
        method: 'GET',
        headers: headers
      }).then(response => {
        if (!response.ok) {
          throw new Error('Network response was not ok ' + response.statusText);
        }
        return response.json();
      }).then(data => {
        console.log(data);
      }).catch(error => {
        console.error(error);
      });
    </script>
  </head>
  <body></body>
</html>
```

삽질 2. NLB를 통한 VPC Endpoint 직접 연결 시도

Name	Status	Type
test.html	200	document
1	CORS error	fetch
1	403	preflight

삽질 2. NLB를 통한 VPC Endpoint 직접 연결 시도



삽질 2. NLB를 통한 VPC Endpoint 직접 연결 시도

기껏 성공한줄 알았건만...

Preflight 때 필수헤더를 추가할 수 없어,

CORS 이슈가 해결되지 않음

삽질 2. NLB를 통한 VPC Endpoint 직접 연결 시도

어떻게든 편리하게
도메인을 연결하고자 했으나
포기... 시키는대로 하자 :)

결론. Route53 별칭 활용

Route53 별칭을 사용하여 프라이빗 API 간접 호출

VPC 엔드포인트를 프라이빗 REST API와 연결하거나 연결 해제할 수 있습니다. 자세한 내용은 (선택 사항) VPC 엔드포인트를 프라이빗 API와 연결 또는 연결 해제 단원을 참조하십시오.

VPC 엔드포인트를 프라이빗 API와 연결한 후 다음 기본 URL을 사용하여 API를 간접적으로 호출할 수 있습니다.

```
https://{rest-api-id}-{vpce-id}.execute-api.{region}.amazonaws.com/{stage}
```

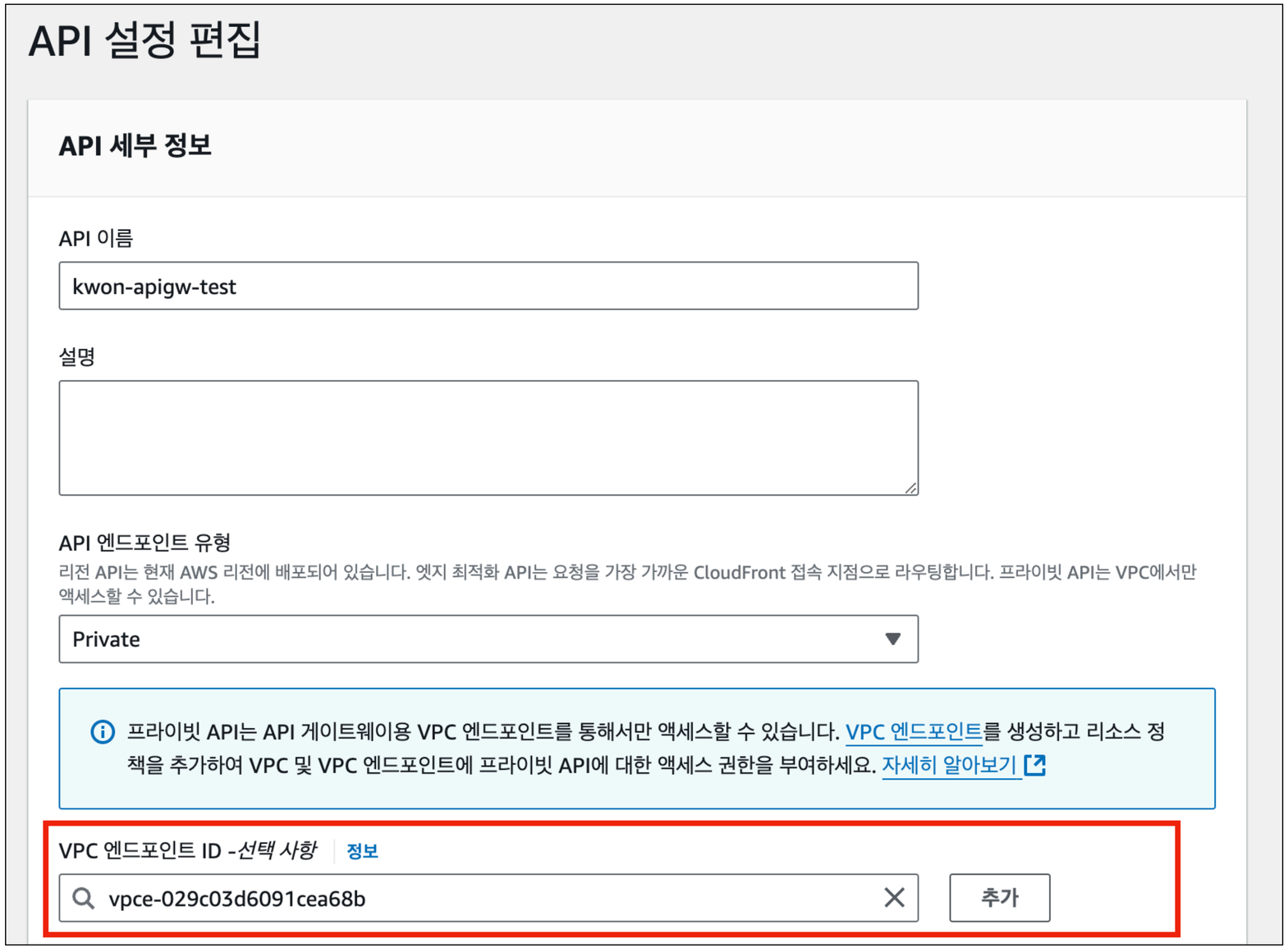
예를 들어 `test` 스테이지에 `GET /pets` 메서드를 설정하고 REST API ID가 `01234567ab`, VPC 엔드포인트 ID가 `vpce-01234567abcdef012`, 리전이 `us-west-2`인 경우 다음과 같이 API를 간접적으로 호출할 수 있습니다.

```
curl -v https://01234567ab-vpce-01234567abcdef012.execute-api.us-west-2.amazonaws.com/test/pets
```

REST API ID : xg1evwxru3 / VPCE ID : vpce-029c03d6091cea68b

→ https://xg1evwxru3-vpce-029c03d6091cea68b.execute-api.ap-northeast-2.amazonaws.com

결론. Route53 별칭 활용



Route53 별칭에 등록되려면

선택사항이지만 필수!

결론. Route53 별칭 활용

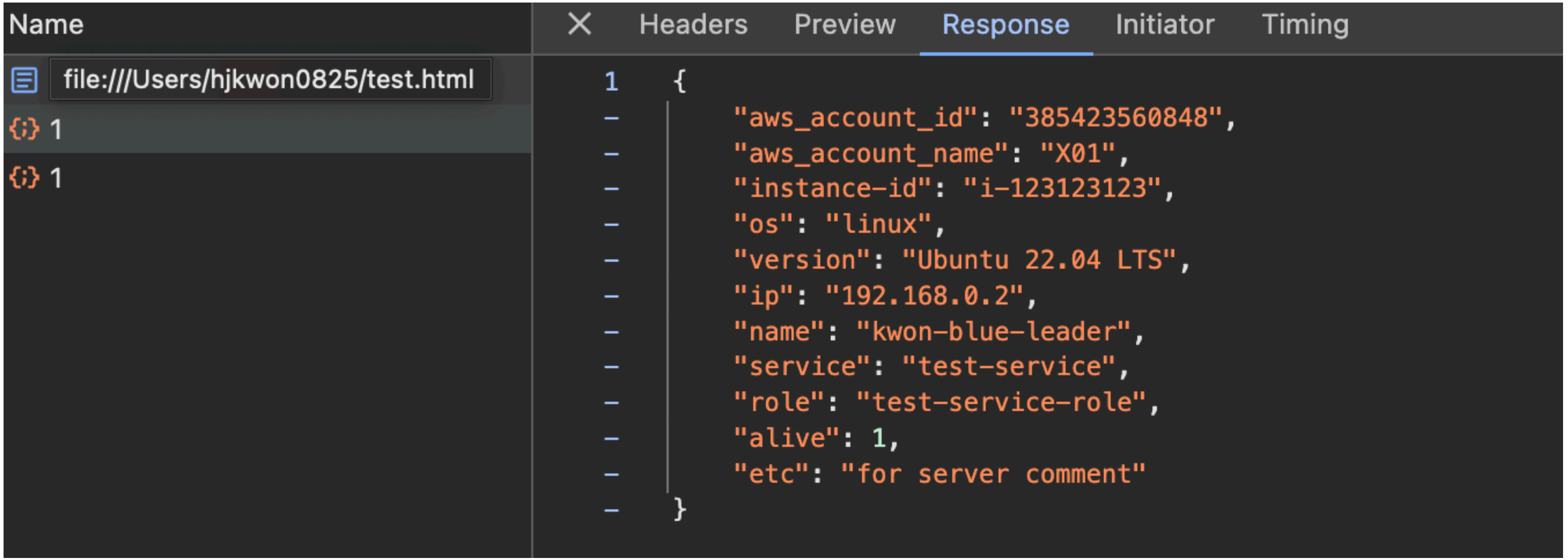
```
hjkwon0825 ~ nslookup
> xg1evwxru3-vpce-029c03d6091cea68b.execute-api.ap-northeast-2.amazonaws.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   xg1evwxru3-vpce-029c03d6091cea68b.execute-api.ap-northeast-2.amazonaws.com
Address: 10.111.0.213
Name:   xg1evwxru3-vpce-029c03d6091cea68b.execute-api.ap-northeast-2.amazonaws.com
Address: 10.111.4.238
>
```

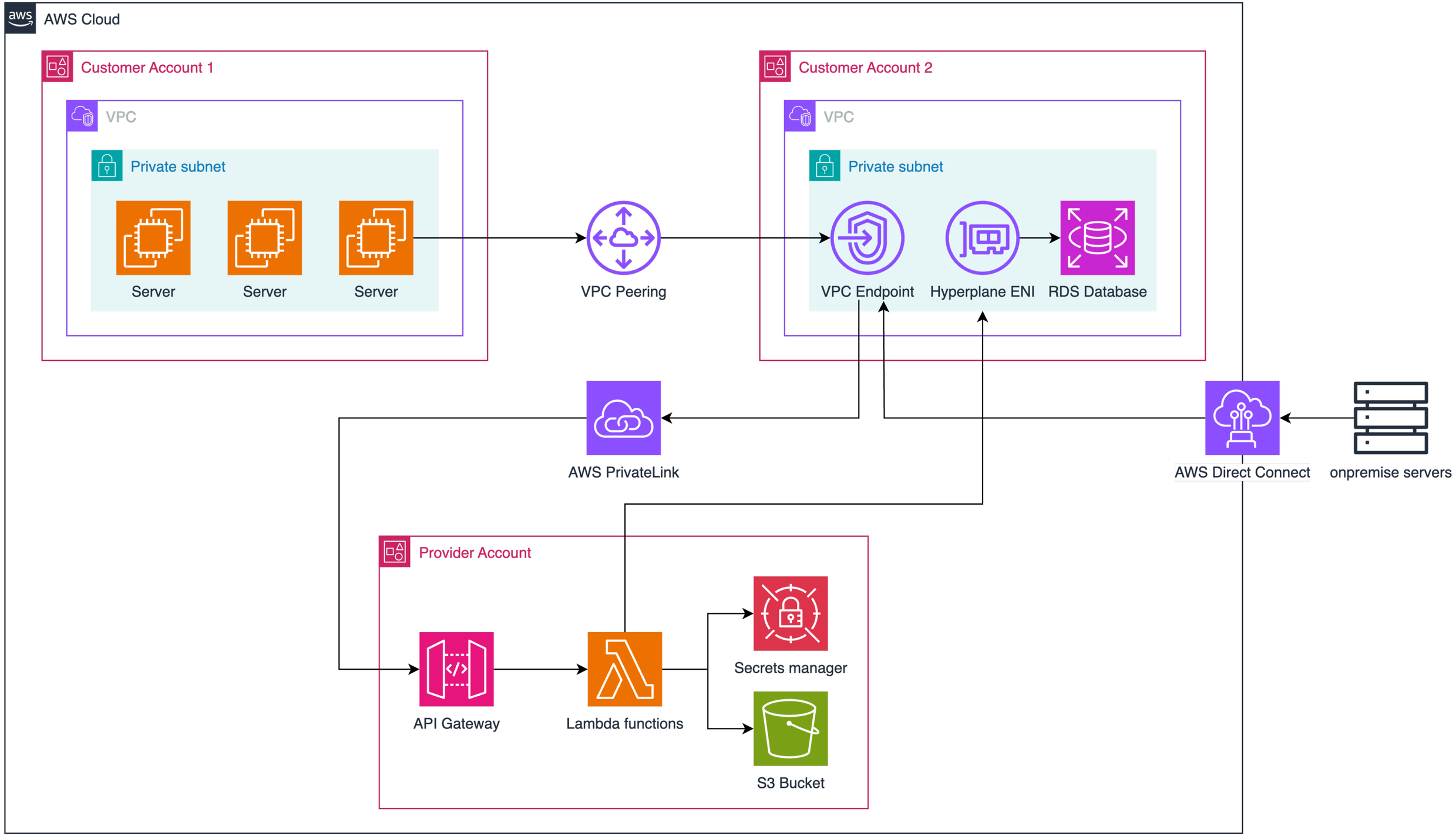
```
hjkwon0825 ~ curl https://xg1evwxru3-vpce-029c03d6091cea68b.execute-api.ap-northeast-2.amazonaws.com/v1/srv/1
-H "X-api-key: 63LS9P3p3b6KKcqQN8Yrc4cPAUQThjx83rHaUglM"
{"aws_account_id": "385423560848", "aws_account_name": "X01", "instance-id": "i-123123123", "os": "linux", "version": "U
buntu 22.04 LTS", "ip": "192.168.0.2", "name": "kwon-blue-leader", "service": "test-service", "role": "test-service-role
", "alive": 1, "etc": "for server comment"}%
hjkwon0825 ~
```

결론. Route53 별칭 활용

Name	Status	Type
test.html	200	document
1	200	fetch
1	200	preflight



최종 정리!


AWS Cloud
Customer Account 1
VPC
Private subnet
Server
Server
Server
VPC Peering
Customer Account 2
VPC
Private subnet
VPC Endpoint
Hyperplane ENI
RDS Database
AWS PrivateLink
AWS Direct Connect
onpremise servers
Provider Account
API Gateway
Lambda functions
Secrets manager
S3 Bucket

참고자료

- https://docs.aws.amazon.com/ko_kr/apigateway/latest/developerguide/apigateway-private-api-test-invoke-url.html#apigateway-private-api-route53-alias

- https://repost.aws/ko/knowledge-center/direct-connect-private-api-gateway

- https://docs.aws.amazon.com/ko_kr/Route53/latest/DeveloperGuide/routing-to-vpc-interface-endpoint.html


Q
A