DNS & BIND

hyuk

DNS

Domain Name System

172.217.175.78

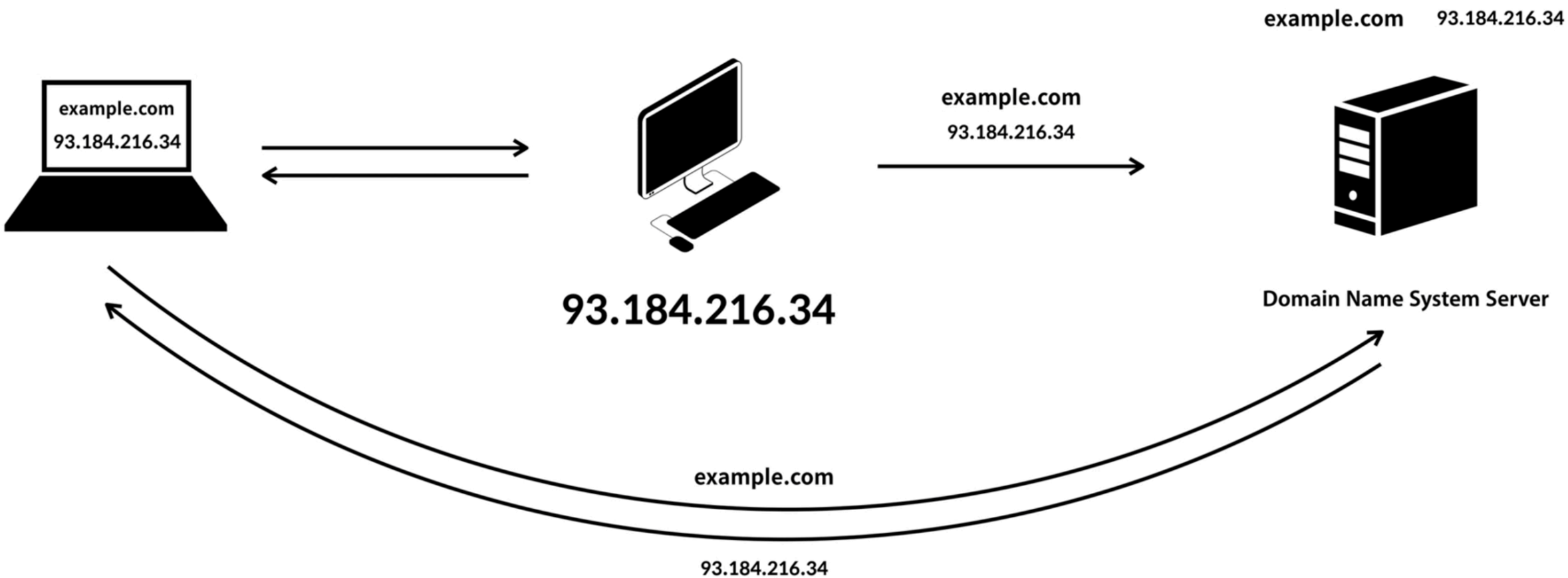
google.com

왜 필요할까?

- 특정 호스트 접근을 위해서 IP 주소가 필요
- IP를 외우기 힘들다
- 그래서 관계(?)를 만들자
- /etc/hosts => local에 여기 저장 되어 있다


example.com
93.184.216.34
93.184.216.34
93.184.216.34 example.com
hosts


example.com
93.184.216.34
93.184.216.34
93.184.216.34
hosts
bank.com

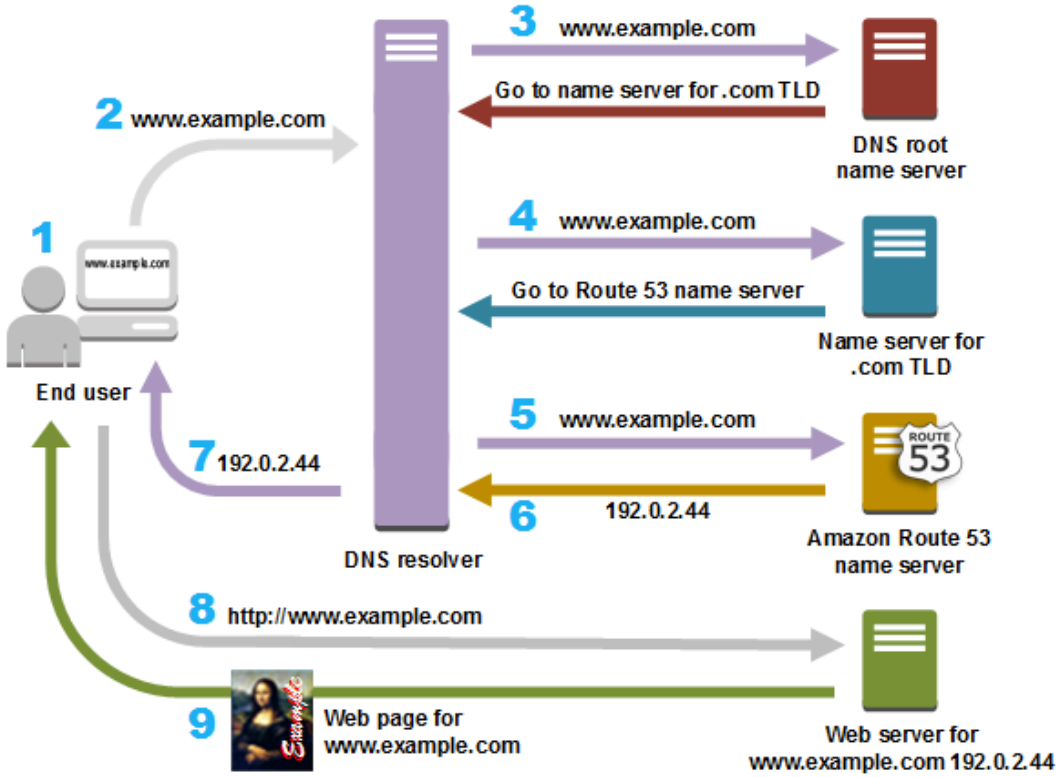

example.com
93.184.216.34
example.com
93.184.216.34
example.com
93.184.216.34
93.184.216.34
Domain Name System Server
example.com
93.184.216.34

DNS

- Domain Name System
- 도메인 이름을 ip 주소로 변환, 대응
- DNS는 분산형 데이터베이스이다.

분산형

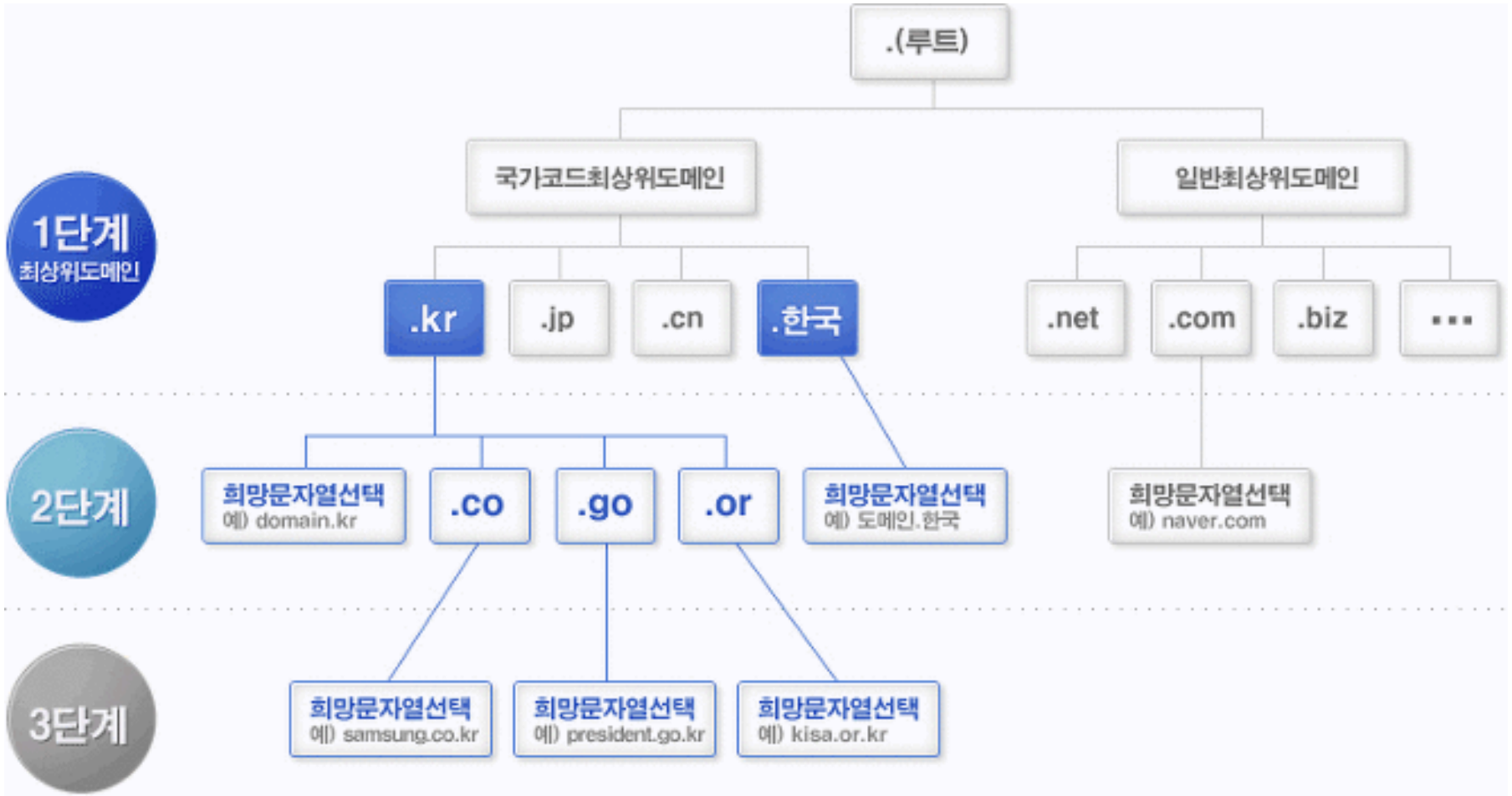
- DNS는 여러개의 Name Server(도메인 ip mapping)으로 이루어져 있다



Domain Name Space

- Domain Name으로 이루어진 트리구조
- 각 노드는 도메인
- 같은 레벨에서 레이블(이름)이 유일
- 계층구조로 이루어져 있음

Domain Name Space



일반최상위도메인은 스폰서 도메인과 언스폰서 도메인으로 나뉜다

Domain Name Space

Root Domain

- 가장 위에 존재하는 계층으로, 모든 도메인 이름은 root부터 시작
- 최상위 도메인으로 전세계13개 뿐이고 다른나라에서 미러 서버를 운영한다

미국에 10개, 네덜란드, 노르웨이, 일본

Domain Name Space

Top Level Domain (TLD, 최상위 도메인 계층)

- Root 바로 아래 해당하는 계층, 1단계 도메인으로도 불림
- 국가에 할당된 도메인과 업체에 할당된 도메인으로 크게 분류됨
- Country Code Top Level Domain (ccTLD)
  - 최상위 도메인 네임은 국가를 나타내며 , 하위 도메인들은 그 국가 조직의 성격을 나타내는 도메인 네임 레이블 상위 노드의 도메인 네임 을 사용
- Generic Top Level Domain (gTLD)
  - 국가 단위가 아닌, 국제적 단위로 사용되는 도메인들을 일반 최상위 도메인
  - 전 세계를 기준으로 비영리, 상업적, 지역별 등의 목적에 따른 분류로 나누어진다

Domain Name Space

Second Level Domain (SLD, 2단계 도메인 계층)

- 도메인을 등록하고자 하는 조직이나 국가에 속하는 기관으로 분류된다
- 상위 도메인이 ccTLD인 경우
  - 호스트와 조직의 성격을 나타내는 도메인이 위치한다(ac.kr, co.kr)
- 상위 도메인이 gTLD인 경우
  - 조직이나 개인을 최종 사용자로 볼 수 있고, 원하는 레이블(이름)을 사용하여 도메인 네임을 할당 받는다(naver.com)

Domain Name Space

Sub Domain

- 상위 도메인이 ccTLD인 경우
  - 3단계 도메인의 특성을 가진 도메인으로 조직이나 개인에서 도메인을 등록, 즉 최종 사용자 도메인이 정의됨
  - google.co.kr, kaist.ac.kr
- 상위 도메인이 gTLD인 경우
  - 서브 도메인으로의 특성을 가진 도메인으로 최종 사용자가 필요에 따라서 만든 하위 도메인
  - 여러 대의 Web Server 를 목적에 따라서 도메인을 구별하는 등의 목적으로 사용된다
  - www.naver.com, sports.naver.com

IP 주소

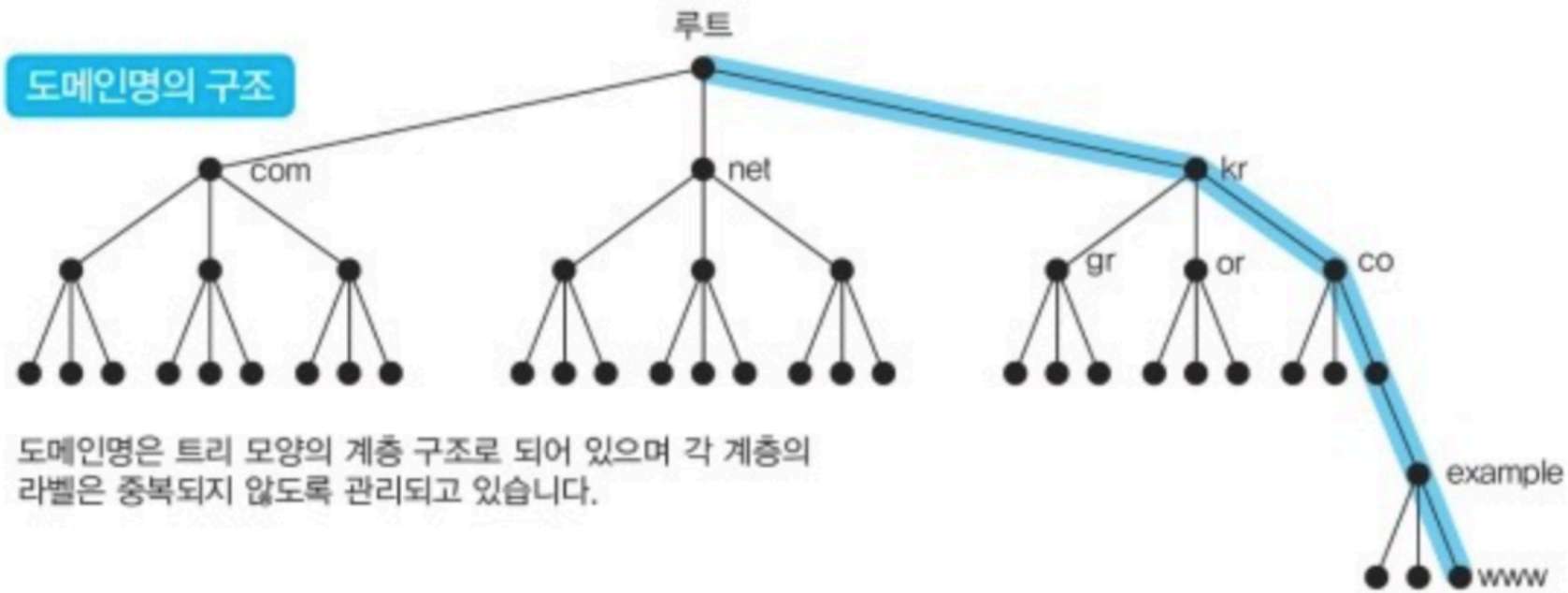
10.1.1.1

도메인명

www.example.co.kr

- www: 호스트명
- example: 제 3레벨 도메인
- co: 제 2레벨 도메인
- kr: 제 1레벨 도메인

도메인명의 구조



도메인명은 트리 모양의 계층 구조로 되어 있으며 각 계층의 라벨은 중복되지 않도록 관리되고 있습니다.

Resource Record

- 도메인과 관련된 정보를 가지고 있는 Record(db에서 데이터를 갖고 있는 항목)
- 리소스 레코드로 정의되어지지 않는다면, domain name space에 정의되어 있어도 해당 도메인 네임에 매치되는 IP주소를 알 수 없기 때문에 접속이 불가능하다
- Resource Record의 유형에는 A(Address), NS(Name Server), CNAME(Canonical Name), SOA(Start of Authority) 등 다양하다

RR유형값	RR 문자 코드	RR 유형	설명
1	A	주소	32비트 IP 주소를 포함합니다. 이 유형은 네임 변환을 위한 노트의 주소가 지정되는 곳이기 때문에 DNS의 "본질"이라고 할 수 있습니다.
2	NS	네임 서버	DNS 구역을 위한 권한 DNS 네임 서버의 네임을 나타냅니다. 각 구역은 1차 네임 서버를 가리키는 NS 레코드를 하나 이상 가지고 있어야 하며 네임은 유효한 주소 레코드(A)를 가지고 있어야 합니다.
5	CNAME	정규 네임	노드의 실제 네임을 가리키도록 정의한 별칭(alias)을 위해 사용합니다. CNAME 레코드는 이 별칭과 노드의 정규 네임 사이의 매핑을 제공합니다. CNAME은 기관의 필요에 따라 내부 네임은 수정하면서도 사용자는 변하지 않는 별칭을 사용하게 함으로써 사용자에게 DNS 구조의 내부 변경을 숨기는데 주로 이용합니다.
6	SOA	권한 개시 정보	DNS 구역의 시작을 표시하는 데 사용하며 DNS 구역에 대한 중요한 정보를 제공합니다. 모든 구역은 정확히 하나의 SOA 레코드를 가져야 합니다. 이 레코드는 구역의 네임, 1차(마스터)권한 서버의 네임뿐만 아니라 관리자의 이메일 주소, 슬레이브(2차)네임 서버를 갱신하는 대기 시간등과 같은 기술적 세부 사항까지 포함합니다.
12	PTR	포인터	네임 공간의 다른 위치를 가리키는 포인터를 제공합니다. 이 레코드는 IN-ADDR.ARPA 도메인을 통한 역방향 전환에 주로 이용합니다.
15	MX	메일 교환	도메인으로 오는 이메일을 처리하는 위치를 명시합니다.
16	TXT	문자열	도메인과 관련해 저장해야 할 임의의 문자를 나타냅니다.

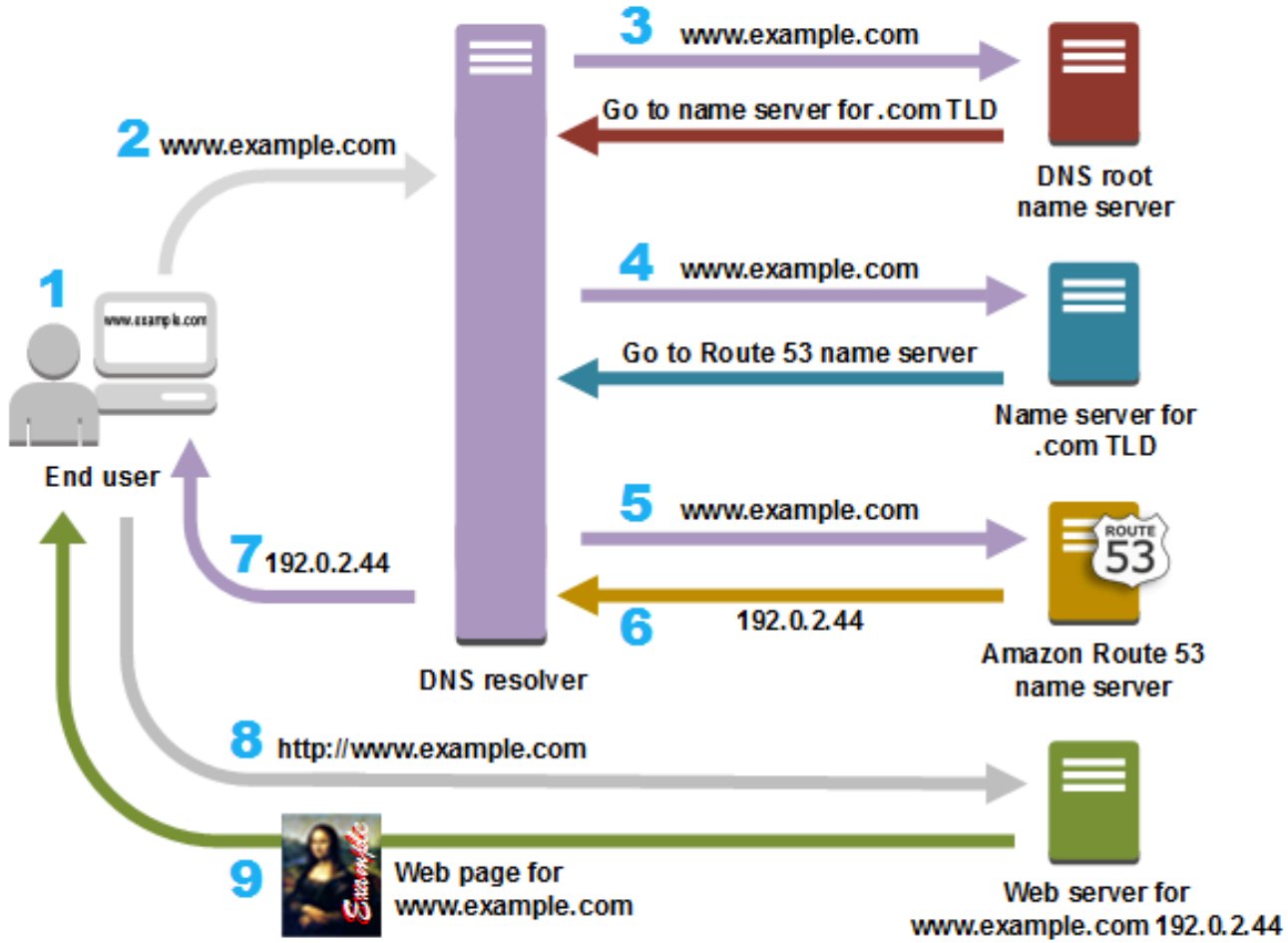
Record Resource

- 구성
- Name : 도메인이름
- Type : 정보유형
- Class : 각 recource record의 유형 집합. TCP/IP 의 class는 IN(텍스트 코드) 혹은 1
- TTL(time to live) : cache 에 저장될 시간
- Resource data: 레코드의 데이터

Name Server/Resolver

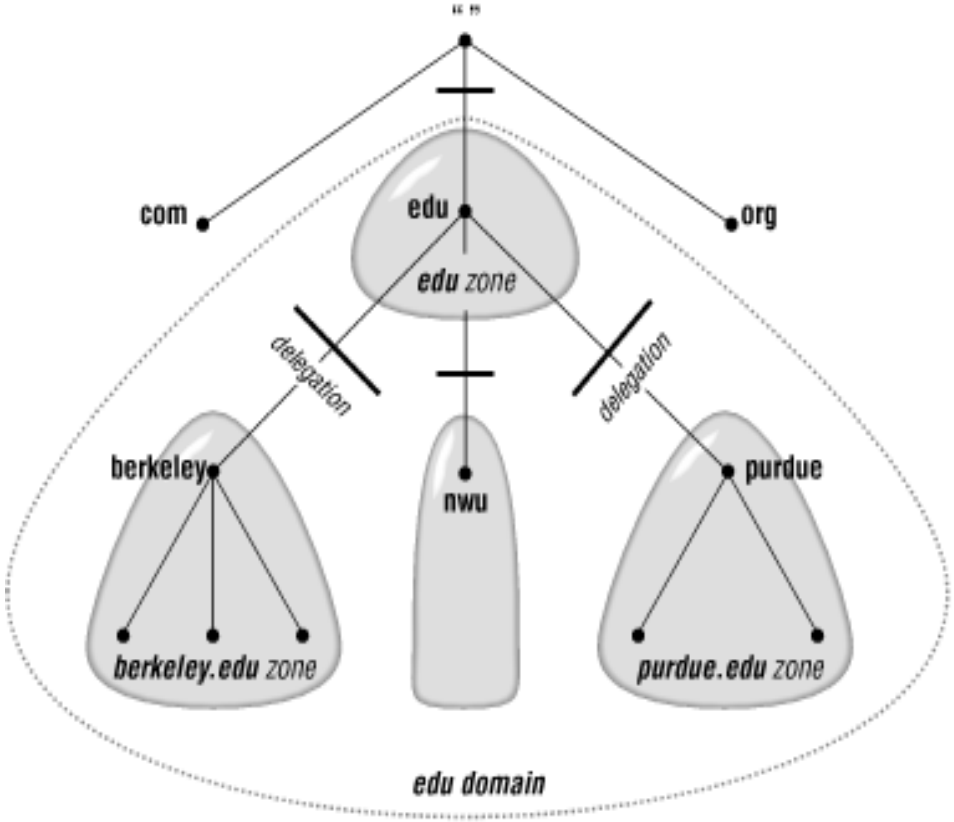
- Name Server
  - 영문 도메인을 ip 주소로 mapping시켜주는 서버

- DNS Resolver
  - DNS 서버에 대한 엑세스를 수행하는 어플리케이션
  - Name server에 원하는 호스트에 대한 정보를 조회하고, 그 응답으로부터 필요한 정보를 추출한다


1
www.example.com
End user
2 www.example.com
DNS resolver
3 www.example.com
Go to name server for .com TLD
DNS root name server
4 www.example.com
Go to Route 53 name server
Name server for .com TLD
5 www.example.com
6 192.0.2.44
ROUTE 53
Amazon Route 53 name server
7 192.0.2.44
8 http://www.example.com
9 Web page for www.example.com
Web server for www.example.com 192.0.2.44

DNS Zone

- Zone
  - Name Server 가 관리하는 영역
- Zone File
  - DNS zone을 나타내는 text file
  - [name] [TTL] [class] [type] [data] 형식으로 구성된다



BIND

Berkely Internet Name Domain

BIND

- BSD (Berkeley Software Distribution) 기반의 UNIX 시스템을 위해 설계된 DNS 소프트웨어이다
- 1980 년대 초 UC Berkeley 대학원생 4 명이 모여서 만든 소프트웨어
- 현재까지 BIND 가 사실상의 standard DNS server
- BIND 9 버전이 사용되고 있다

BIND 서버 명령

설치

sudo apt-get install bind9

실행

sudo service bind9 start

중지

sudo service bind9 stop

재실행

sudo service bind9 restart

BIND 서버 명령

BIND zone file 혹은 config file reload

sudo service bind9 reload

BIND 현 상황

sudo service bind9 status

BIND9 명령어

- DNS 정보 확인
  - nslookup (name server lookup)
  - Domain name을 입력하면 그 주소에 대한 ip 주소와 기타 정보 등을 알려준다
  - 설치 : sudo apt-get install dnsutils
  - 사용법 : nslookup [Domain Name]

  - whois
  - WHOIS 서버에서 domain 정보를 찾아주는 소프트웨어로써 domain에 대한 정보가 아주 자세하게 나오고 등록자에 대한 정보도 나온다
  - 설치 : sudo apt-get install whois
  - 사용법 : whois [Domain Name] ex) whois naver.com

BIND 명령어

- dig (domain information grouper)
- DNS name server 에 질의하기 위한 네트워크 관리 명령 줄 인터페이스 툴
- nslookup 보다 상세한 정보를 여러 option으로 설정 가능
- Option으로 레코드의 type을 지정해줄 수 있다
  - any, soa, a, hinfo, mx, txt 등
- **$** dig example.com any

BIND 설정파일

- /etc/host.conf : ip를 찾을 때 순서를 정해주는 파일
  - order : 붙여진 순서대로 DNS를 찾는다. host, bind, nis 를 사용할 수 있다.
  - multi : on/off. on으로 /etc/hosts에 둘 이상의 ip 주소를 등록하게 허용할 수 있다.
  - alert : on/off. on 으로 spoof 시도가 log되게 할 수 있다.
  - nospoof : on/off. on으로 spoof 시도를 막지만 느려지게 된다.
  - trim : domain name을 인수 취급하게 한다.
- /etc/reslov.conf
  - 네임 서버에 쓸 DNS 저장
- /etc/bind/db.~
  - zone file의 RR type 정보를 기록해둔다
- /etc/bind/named.conf
  - zone file 의 db 위치, 타입에 관한 정보들 설정

```
ubuntu@ip-172-31-45-11:/$ cat /etc/host.conf
# The "order" line is only used by old versions of the C library.
order hosts,bind
multi on
```

실습1

- sudo vim /etc/resolv.conf

```
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "systemd-resolve --status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0
search ap-northeast-2.compute.internal
```

127.0.0.1 자기자신을 의미

실습1

DNS 서버에 zone 생성

sudo vim /etc/bind/named.conf.local

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";


zone "example.com" {
        type master;
        file "/etc/bind/db.example.com";
};
```

실습1

- sudo vim /etc/bind/db.example.com
- 다 치기 힘드니까 db.local복사해서 수정하자

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1
```

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     example.com. root.example.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      example.com.
@       IN      A       100.50.30.1
www     IN      A       100.50.30.2
mail    IN      A       100.50.30.3
ace     IN      CNAME   www
```

실습1

작성한 설정 실행

sudo service bind9 reload

확인

```
ubuntu@ip-172-31-45-11:/$ nslookup
> example.com
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   example.com
Address: 100.50.30.1
> www.example.com
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   www.example.com
Address: 100.50.30.2
> mail.example.com
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   mail.example.com
Address: 100.50.30.3
> ^Cubuntu@ip-172-31-45-11:/$ sudo vim /etc/bind/db.example.com
ubuntu@ip-172-31-45-11:/$ nslookup ace.example.com
Server:         127.0.0.1
Address:        127.0.0.1#53

ace.example.com canonical name = www.example.com.
Name:   www.example.com
Address: 100.50.30.2
```

실습2 – AWS route53

- route 53
- 클라우드 DNS 웹서비스

실습2

- Aws 루트 계정으로 들어가서 지난번에 만들었던 [nickname]에 route53 권한 추가

- 사용자 => nickname 선택 => 권한추가 => 그룹생성 => 이름 아무거나(저는 route53) => AmazonRoute53FullAccess
- 이러면 권한추가 끝

- 사실 그냥 루트 계정으로 들어가도 된다

hyuk에 권한 추가

1 2

권한 부여

IAM 정책을 사용하여 권한을 부여합니다. 기존 정책을 할당하거나 새 정책을 생성할 수 있습니다.

그룹에 사용자 추가 | 기존 사용자에서 권한 복사 | 기존 정책 직접 연결

기존 그룹에 사용자를 추가하거나 새 그룹을 생성합니다. 그룹을 사용하여 직무별로 사용자의 권한을 관리하는 것이 좋습니다. 자세히 알아보기

그룹에 사용자 추가

그룹 생성 | 새로 고침

검색 1 결과 표시

	그룹	연결된 정책
☐	S3Admin	AmazonS3FullAccess

취소 | 다음: 검토

대시보드
호스팅 영역
상태 검사
트래픽 흐름
트래픽 정책
정책 레코드
도메인
등록된 도메인
대기 중인 요청
확인자
VPC
인바운드 엔드포인트
아웃바운드 엔드포인트
규칙

호스팅 영역 생성 | 레코드 세트로 이동 | 호스팅 영역 삭제

Amazon Route 53은 신뢰할 수 있는 Domain Name System(DNS) 서비스입니다. DNS는 사람이 읽을 수 있는 도메인 이름(example.com)을 IP 주소(192.0.2.0)로 변환하는 시스템입니다. Route 53은 전 세계의 데이터 센터에서 신뢰할 수 있는 이름 서버를 사용하여 안정적이고 확장 가능한 고속 시스템입니다.

example.com 같은 도메인 이름이 이미 있는 경우 Route 53은 인터넷에서 도메인의 웹 서버, 메일 서버 및 기타 리소스를 찾을 위치를 Domain Name System(DNS)에 알려줄 수 있습니다.

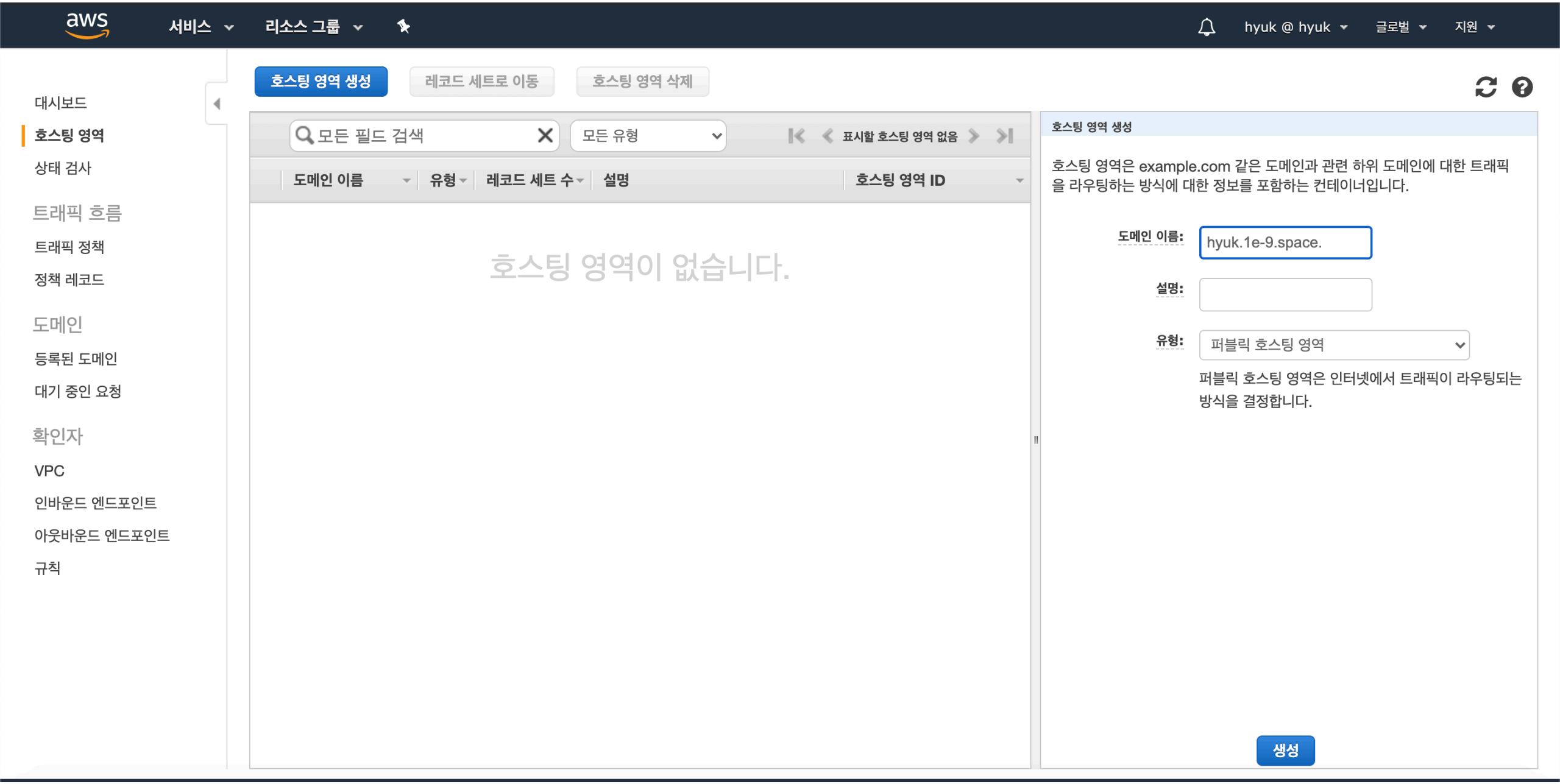
자세히 알아보기

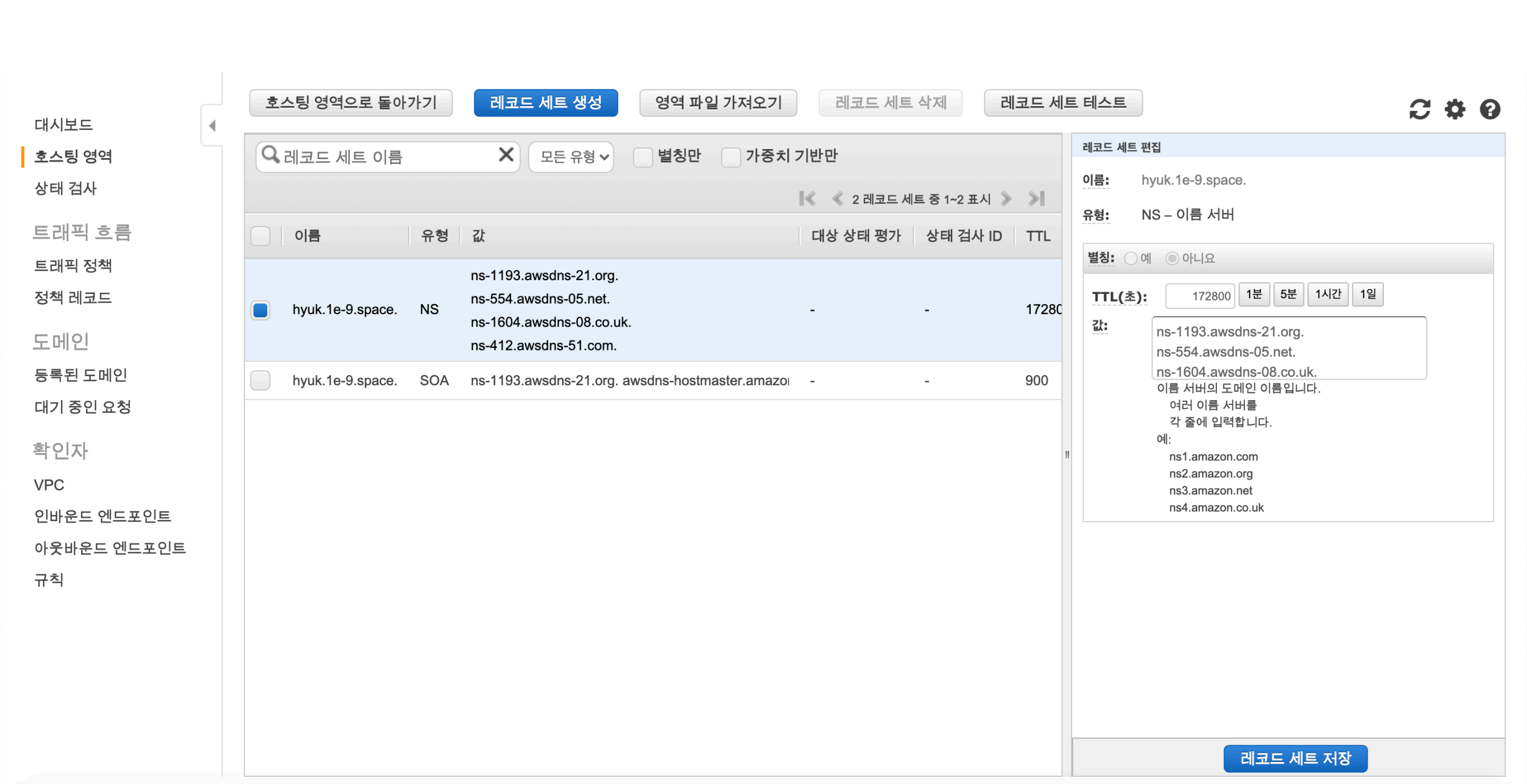
호스팅 영역 생성

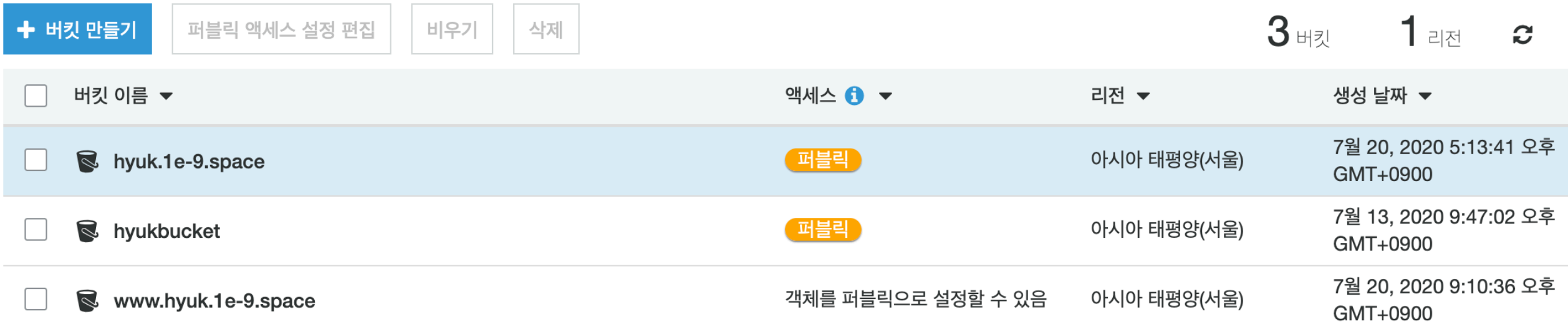
Route 53 설명서 및 지원

시작 안내서 | Amazon Route 53 설명서

DNS는 사람이 읽을 수 있는 도메인 이름(example.com)을 IP 주소(192.0.2.8)로 변환하는 시스템입니다


aws
서비스
리소스 그룹
hyuk @ hyuk
글로벌
지원
대시보드
호스팅 영역
상태 검사
트래픽 흐름
트래픽 정책
정책 레코드
도메인
등록된 도메인
대기 중인 요청
확인자
VPC
인바운드 엔드포인트
아웃바운드 엔드포인트
규칙
호스팅 영역 생성
레코드 세트로 이동
호스팅 영역 삭제
모든 필드 검색
모든 유형
표시할 호스팅 영역 없음
도메인 이름
유형
레코드 세트 수
설명
호스팅 영역 ID
호스팅 영역이 없습니다.
호스팅 영역 생성
호스팅 영역은 example.com 같은 도메인과 관련 하위 도메인에 대한 트래픽을 라우팅하는 방식에 대한 정보를 포함하는 컨테이너입니다.
도메인 이름:
hyuk.1e-9.space.
설명:
유형:
퍼블릭 호스팅 영역
퍼블릭 호스팅 영역은 인터넷에서 트래픽이 라우팅되는 방식을 결정합니다.
생성


대시보드
호스팅 영역
상태 검사
트래픽 흐름
트래픽 정책
정책 레코드
도메인
등록된 도메인
대기 중인 요청
확인자
VPC
인바운드 엔드포인트
아웃바운드 엔드포인트
규칙
호스팅 영역으로 돌아가기
레코드 세트 생성
영역 파일 가져오기
레코드 세트 삭제
레코드 세트 테스트
레코드 세트 이름
모든 유형
별칭만
가중치 기반만
2 레코드 세트 중 1~2 표시
이름
유형
값
대상 상태 평가
상태 검사 ID
TTL
hyuk.1e-9.space.
NS
ns-1193.awsdns-21.org.
ns-554.awsdns-05.net.
ns-1604.awsdns-08.co.uk.
ns-412.awsdns-51.com.
-
-
172800
hyuk.1e-9.space.
SOA
ns-1193.awsdns-21.org. awsdns-hostmaster.amazo
-
-
900
레코드 세트 편집
이름:
hyuk.1e-9.space.
유형:
NS – 이름 서버
별칭:
예
아니요
TTL(초):
172800
1분
5분
1시간
1일
값:
ns-1193.awsdns-21.org.
ns-554.awsdns-05.net.
ns-1604.awsdns-08.co.uk.
이름 서버의 도메인 이름입니다.
여러 이름 서버를
각 줄에 입력합니다.
예:
ns1.amazon.com
ns2.amazon.org
ns3.amazon.net
ns4.amazon.co.uk
레코드 세트 저장



새 버킷을 만들자!!! => 모든 퍼블릭 엑세스 차단 풀기 => 권한 => 버킷 정책=>버킷 정책 생성기

hyuk.1e-9.space

개요 | 속성 | 권한 | 관리 | 액세스 지점

퍼블릭

검색하려면 접두사를 입력하고 Enter 키를 누릅니다. 지우려면 Esc 키를 누릅니다.

업로드 | 폴더 만들기 | 다운로드 | 작업

아시아 태평양(서울)

보기 1 대상 1

이름	마지막 수정	크기	스토리지 클래스
index.html	7월 20, 2020 5:13:55 오후 GMT+0900	143.0 B	스탠다드

보기 1 대상 1

정적 웹 사이트 호스팅

엔드포인트: http://hyuk.1e-9.space.s3-website.ap-northeast-2.amazonaws.com

이 버킷을 사용하여 웹 사이트를 호스팅합니다. 세부 정보

인덱스 문서

index.html

오류 문서

error.html

리디렉션 규칙(선택 사항)

요청 리디렉션 세부 정보

웹 사이트 호스팅 사용 안 함

버킷 호스팅

취소 저장

호스팅 영역으로 돌아가기 | 레코드 세트 생성 | 영역 파일 가져오기 | 레코드 세트 삭제 | 레코드 세트 테스트

레코드 세트 이름 | 모든 유형 | 별칭만 | 가중치 기반만

3 레코드 세트 중 1~3 표시

이름	유형	값	대상 상태 평가	상태 검사 ID	TTL
hyuk.1e-9.space.	A	ALIAS s3-website.ap-northeast-2.amazonaws.com.	아니요	-	
hyuk.1e-9.space.	NS	ns-1193.awsdns-21.org. ns-554.awsdns-05.net. ns-1604.awsdns-08.co.uk. ns-412.awsdns-51.com.	-	-	17280
hyuk.1e-9.space.	SOA	ns-1193.awsdns-21.org. awsdns-hostmaster.amazo	-	-	900

레코드 세트 편집

이름: hyuk.1e-9.space.

유형: A – IPv4 주소

별칭: (●) 예 ( ) 아니요

별칭 대상: s3-website.ap-northeast-2.amazonaws

별칭 호스팅 영역 ID: Z3W03O7B5YMIYP

리소스에 대한 도메인 이름도 입력할 수 있습니다. 예:
- CloudFront 배포 도메인 이름: d111111abcdef8.cloudfront.net
- Elastic Beanstalk 환경 CNAME: example.elasticbeanstalk.com
- ELB Load Balancer DNS 이름: example-1.us-east-2.elb.amazonaws.com
- S3 웹 사이트 엔드포인트: s3-website.us-east-2.amazonaws.com
- 이 호스팅 영역의 리소스 레코드 세트: www.example.com
- VPC 엔드포인트: example.us-east-2.vpce.amazonaws.com
- API Gateway 사용자 지정 지역 API: d-abcde12345.execute-api.us-west-2.amazonaws.com
- Global Accelerator DNS 이름: a012345abc.awsglobalaccelerator.com

자세히 알아보기

라우팅 정책: 심플

Route 53은 이 레코드의 값에 따라서만 쿼리에 응답합니다. 자세히 알아보기

대상 상태 평가: ( ) 예 (●) 아니요

레코드 세트 저장

www.hyuk.1e-9.space

개요 | 속성 | 권한 | 관리 | 액세스 지점

버전 관리

동일 버킷 내에 한 객체의 여러 버전을 보관합니다.

세부 정보

비활성

서버 액세스 로깅

액세스 요청에 대한 세부 정보를 기록하는 액세스 로그를 설정합니다.

세부 정보

비활성

정적 웹 사이트 호스팅

엔드포인트: http://www.hyuk.1e-9.space.s3-website.ap-northeast-2.amazonaws.com

○ 이 버킷을 사용하여 웹 사이트를 호스팅합니다. 세부 정보

● 요청 리디렉션 세부 정보

대상 버킷 또는 도메인

hyuk.1e-9.space

프로토콜

https 또는 http

○ 웹 사이트 호스팅 사용 안 함

✓ 모든 요청 리디렉션

취소 | 저장

호스팅 영역으로 돌아가기 | 레코드 세트 생성 | 영역 파일 가져오기 | 레코드 세트 삭제 | 레코드 세트 테스트

레코드 세트 이름 | 모든 유형 | 별칭만 | 가중치 기반만

4 레코드 세트 중 1~4 표시

이름	유형	값	대상 상태 평가	상태 검사 ID
hyuk.1e-9.space.	A	ALIAS s3-website.ap-northeast-2.amazonaws.com.	아니요	-
hyuk.1e-9.space.	NS	ns-1193.awsdns-21.org. ns-554.awsdns-05.net. ns-1604.awsdns-08.co.uk. ns-412.awsdns-51.com.	-	-
hyuk.1e-9.space.	SOA	ns-1193.awsdns-21.org. awsdns-hostmaster.amazo	-	-
www.hyuk.1e-9.space.	CNAME	www.hyuk.1e-9.space.s3-website.ap-northeast-2.an	-	-

레코드 세트 편집

이름: www .hyuk.1e-9.space.

유형: CNAME – 정식 이름

별칭: ○ 예 ◉ 아니요

TTL(초): 300 | 1분 | 5분 | 1시간 | 1일

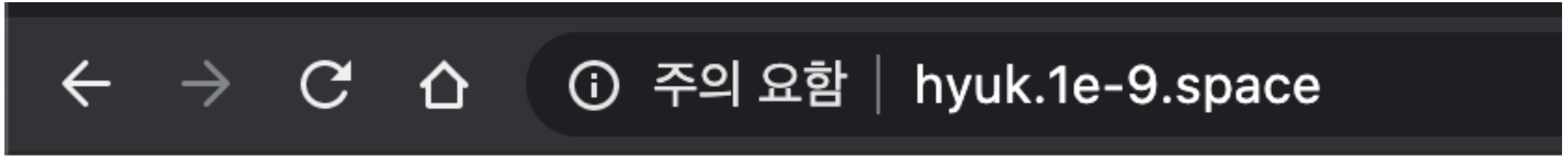
값: www.hyuk.1e-9.space.s3-website.ap-northeast-2.amazonaws.com

이름 필드에서
값 대신 확인할
도메인 이름입니다.
예:
www.example.com

라우팅 정책: 심플

Route 53은 이 레코드의 값에 따라서만 쿼리에 응답합니다. 자세히 알아보기

레코드 세트 저장



2020WheelSeminar

제출

- 아까 한 nslookup사진
- 링크