aws

개발자 가이드

Amazon Route 53

API 버전 2013-04-01

Amazon Route 53: 개발자 가이드

Table of Contents

Amazon Route 53는 무엇인가요?

Amazon Route 53는 가용성과 확장성이 뛰어난 DNS(도메인 이름 시스템) 웹 서비스입니다. Route 53를 사용하여 세 가지 주요 기능, 즉 도메인 등록, DNS 라우팅, 상태 확인을 조합하여 실행할 수 있습니다.

세 기능 모두에 Route 53를 사용하도록 선택한 경우 아래 순서를 따라야 합니다.

1. 도메인 이름 등록

   웹 사이트의 이름(예: example.com)이 필요합니다. Route 53를 통해 웹사이트 또는 웹 애플리케이션의 이름, 즉 도메인 이름을 등록할 수 있습니다.

   - 개요는 도메인 등록 방식 섹션을 참조하세요.
   - 절차는 다음(새 도메인 등록)을 참조하십시오.
   - Amazon S3 버킷에서 도메인을 등록하고 단순한 웹사이트를 만드는 내용의 튜토리얼은 Amazon Route 53 시작하기 섹션을 참조하세요.

2. 인터넷 트래픽을 도메인의 리소스로 라우팅

   사용자가 웹 브라우저를 열어 주소 표시줄에 도메인 이름(example.com) 또는 하위 도메인 이름(acme.example.com)을 입력한 경우 Route 53는 브라우저를 웹 사이트 또는 웹 애플리케이션에 연결하도록 돕습니다.

   - 개요는 웹 사이트 또는 웹 애플리케이션으로 인터넷 트래픽을 라우팅하는 방식 섹션을 참조하세요.
   - 절차는 Amazon Route 53을 DNS 서비스로 구성 단원을 참조하십시오.
   - 이메일을 Amazon WorkMail로 라우팅하는 방법에 대한 절차는 Amazon WorkMail로 트래픽 라우팅 섹션을 참조하세요.

3. 리소스의 상태 확인

   Route 53는 인터넷을 통해 웹 서버 같은 리소스로 자동화된 요청을 보내어 접근 및 사용이 가능하고 정상 작동 중인지 확인합니다. 리소스를 사용할 수 없게 될 때 알림을 수신하고 비정상 리소스가 아닌 다른 곳으로 인터넷 트래픽을 라우팅할 수도 있습니다.

   - 개요는 Amazon Route 53가 리소스의 상태를 확인하는 방법 섹션을 참조하세요.
   - 절차는 Amazon Route 53 상태 확인 생성 단원을 참조하십시오.

기타 Route 53 기능

Route 53는 도메인 이름 시스템(DNS) 웹 서비스일 뿐만 아니라 다음과 같은 기능을 제공합니다.

Route 53 Resolver

의 Amazon VPC AWS 리전, AWS Outposts 랙의 VPCs 또는 기타 온프레미스 네트워크에 대한 재귀 DNS를 가져옵니다. 조건부 전달 규칙 및 Route 53 엔드포인트를 생성하여 Route 53 프라이빗 호스팅 영역 또는 온프레미스 DNS 서버에서 마스터된 사용자 지정 이름을 확인합니다.

자세한 내용은 섹션을 참조하세요Amazon Route 53 Resolver란 무엇인가요?.

Amazon Route 53 Resolver on Outposts

Route 53 Resolver 엔드포인트를 통해 Route 53 Resolver on Outpost 랙을 온프레미스 데이터 센터의 DNS 서버와 연결합니다. 이를 통해 Outposts 랙과 다른 온프레미스 리소스 간의 DNS 쿼리를 해결할 수 있습니다.

자세한 내용은 섹션을 참조하세요Amazon Route 53 on Outposts란 무엇인가요?.

Route 53 Resolver DNS Firewall

Route 53 Resolver 내에서 재귀 DNS 쿼리를 보호합니다. 도메인 목록을 생성하고 이러한 규칙에 대해 아웃바운드 DNS 트래픽을 필터링하는 방화벽 규칙을 구축합니다.

자세한 내용은 DNS 방화벽을 사용하여 아웃바운드 DNS 트래픽 필터링 섹션을 참조하세요.

트래픽 흐름

사용하기 쉽고 비용 효율적인 글로벌 트래픽 관리: 지리 근접성, 지연 시간, 상태 및 기타 고려 사항에 따라 최종 사용자를 애플리케이션에 가장 적합한 엔드포인트로 라우팅합니다.

자세한 내용은 트래픽 흐름을 사용하여 DNS 트래픽 라우팅 섹션을 참조하세요.

Amazon Route 53 프로필

Route 53 Profiles를 사용하면 여러 VPCs하고 관리할 수 있습니다 AWS 계정.

자세한 내용은 섹션을 참조하세요Amazon Route 53 Profiles란?.

주제

- 도메인 등록 방식
- 웹 사이트 또는 웹 애플리케이션으로 인터넷 트래픽을 라우팅하는 방식
- Amazon Route 53가 리소스의 상태를 확인하는 방법

- Amazon Route 53 개념
- Amazon Route 53 시작 방법
- Amazon Route 53 액세스
- AWS 자격 증명 및 액세스 관리
- Amazon Route 53 요금 및 결제
- AWS SDK에서 Route 53 사용

도메인 등록 방식

웹 사이트나 웹 애플리케이션을 만들려면 먼저 domain name이라고 하는 웹 사이트의 이름을 등록합니다. 도메인 이름이란 example.com 같은 이름이고, 사용자가 이를 브라우저에 입력하면 해당 웹 사이트가 표시됩니다.

다음은 Amazon Route 53에 도메인 이름을 등록하는 방법의 개요입니다.

1. 도메인 이름을 선택하고 사용 가능한지, 즉 원하는 도메인 이름을 다른 사람이 이미 등록하지 않았는지 확인합니다.

   원하는 도메인 이름이 이미 사용 중이라면 다른 이름을 시도하거나 .com 등의 최상위 도메인만 .ninja 또는 .hockey 같은 다른 최상위 도메인으로 변경할 수 있습니다. Route 53가 지원하는 최상위 도메인 목록은 Amazon Route 53에 등록할 수 있는 도메인을 참조하세요.
2. Route 53에 도메인 이름을 등록합니다. 도메인을 등록할 때는 도메인 소유자 및 다른 연락처의 이름과 연락처 정보를 제공합니다.

   Route 53에 도메인을 등록하면 Route 53는 다음을 수행함으로써 자동으로 도메인의 DNS 서비스가 됩니다.
   - 도메인과 이름이 같은 hosted zone을 생성합니다.
   - 호스팅 영역에 4개의 이름 서버 세트를 할당합니다. 누군가 브라우저를 사용하여 www.example.com과 같은 웹사이트에 접속하면 이 이름 서버들은 웹 서버 또는 Amazon S3 버킷 같은 리소스를 어디에서 찾아야 하는지 브라우저에게 알려줍니다. (Amazon S3은 웹 어디서나 원하는 양의 데이터를 저장하고 검색하기 위한 객체 스토리지입니다. 버킷은 S3;에 저장하는 객체의 컨테이너입니다.)
   - 호스팅 영역에서 이름 서버를 얻어 도메인에 추가합니다.

   자세한 내용은 웹 사이트 또는 웹 애플리케이션으로 인터넷 트래픽을 라우팅하는 방식 섹션을 참조하세요.

3. 등록 프로세스가 끝나면 도메인 등록 기관에 사용자의 정보를 전송합니다. domain registrar는 Amazon Registrar 또는 등록 대행 협력사 Gandi입니다. 도메인의 등록 대행자가 어디인지 알려면 등록 기관 찾기 단원을 참조하십시오.
4. 등록 대행자는 사용자 정보를 도메인의 등록 기관으로 전송합니다. 등록 기관은 .com과 같은 하나 이상의 최상위 도메인의 도메인 등록을 판매하는 회사입니다.
5. 등록 기관은 자체 데이터베이스에 사용자의 도메인에 관한 정보를 저장하고 일부 정보는 퍼블릭 WHOIS 데이터베이스에도 저장합니다.

도메인 이름을 등록하는 자세한 방법은 새 도메인 등록 단원을 참조하십시오.

다른 등록 기관에 이미 도메인 이름을 등록한 경우, 도메인 등록을 Route 53으로 이전할 수 있습니다. 다른 Route 53 기능을 사용하는 데는 필요하지 않습니다. 자세한 내용은 도메인 등록을 Amazon Route 53으로 이전하기 섹션을 참조하세요.

웹 사이트 또는 웹 애플리케이션으로 인터넷 트래픽을 라우팅하는 방식

스마트폰이나 노트북 연결부터 대규모 소매 웹 사이트의 콘텐츠를 서비스하는 서버에 이르기까지 인터넷상의 모든 컴퓨터는 숫자를 사용하여 서로 통신합니다. IP 주소라고 하는 이 숫자는 다음 형식 중 하나로 되어 있습니다.

- 192.0.2.44와 같은 인터넷 프로토콜 버전 4(IPv4)
- 2001:0db8:85a3:0000:0000:abcd:0001:2345와 같은 인터넷 프로토콜 버전 6(IPv6)

브라우저를 열고 웹 사이트로 이동할 때는 이런 긴 문자열을 기억해 입력할 필요가 없습니다. 그 대신 example.com과 같은 도메인 이름을 입력해도 원하는 웹 사이트로 갈 수 있습니다. Amazon Route 53과 같은 DNS 서비스는 도메인 이름과 IP 주소를 연결하도록 돕습니다.

주제

- 인터넷 트래픽을 도메인으로 라우팅하도록 Amazon Route 53를 구성하는 방법 개요
- Amazon Route 53가 도메인의 트래픽을 라우팅하는 방법

인터넷 트래픽을 도메인으로 라우팅하도록 Amazon Route 53를 구성하는 방법 개요

다음은 Amazon Route 53 콘솔을 사용하여 도메인 이름을 등록하고 인터넷 트래픽을 웹 사이트 또는 웹 애플리케이션으로 라우팅하도록 Route 53를 구성하는 방법의 개요입니다.

1. 사용자들이 콘텐츠에 액세스하는 데 사용될 도메인 이름을 등록해야 합니다. 개요는 도메인 등록 방식 섹션을 참조하세요.
2. 도메인 이름을 등록한 후 Route 53는 도메인과 동일한 이름의 퍼블릭 호스팅 영역을 자동으로 생성합니다. 자세한 내용은 퍼블릭 호스팅 영역 작업 섹션을 참조하세요.
3. 트래픽을 리소스로 라우팅하려면 호스팅 영역에서 리소스 레코드 세트라고도 하는 레코드를 생성합니다. 각각의 레코드에는 도메인의 트래픽을 라우팅할 방법에 관한 다음과 같은 정보가 포함되어 있습니다.

   명칭

   레코드의 이름은 Route 53를 사용하여 트래픽을 라우팅하려는 도메인 이름(예: example.com) 또는 하위 도메인 이름(예: www.example.com)과 일치합니다.

   호스팅 영역에 있는 모든 레코드의 이름은 반드시 호스팅 영역의 이름으로 끝나야 합니다. 예를 들어 호스팅 영역의 이름이 example.com이라면 모든 레코드 이름이 example.com으로 끝나야 합니다. Route 53 콘솔은 자동으로 이 작업을 수행합니다.

   유형

   레코드 유형은 일반적으로 트래픽을 라우팅할 리소스 유형을 결정합니다. 예를 들어 트래픽을 이메일 서버로 라우팅하려면 Type(유형)을 MX로 지정합니다. IPv4 IP 주소를 가진 웹 서버로 트래픽을 라우팅하려면 [Type]을 [A]로 지정합니다.

   값

   [Value]는 [Type]과 밀접한 관련이 있습니다. [Type]을 [MX]로 지정하는 경우, [Value]에 하나 이상의 이메일 서버의 이름을 지정해야 합니다. [Type]을 [A]로 지정하는 경우, 192.0.2.136과 같은 IPv4 형식의 IP 주소를 지정해야 합니다.

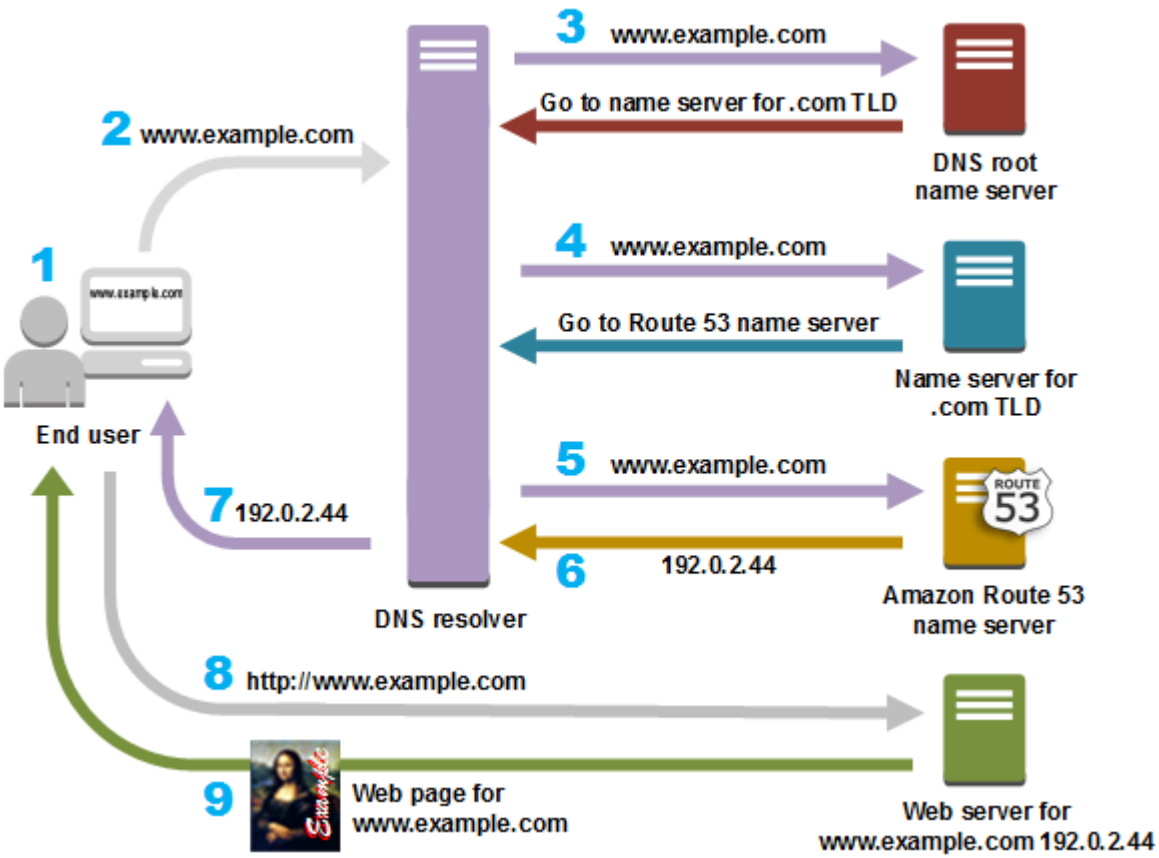
레코드에 대한 자세한 내용은 레코드 작업 단원을 참조하십시오.

트래픽을 Amazon S3 버킷, Amazon CloudFront 배포 및 다른 AWS 리소스로 라우팅하는, 별칭 레코드라고 하는 특별한 Route 53 레코드도 생성할 수 있습니다. 자세한 내용은 별칭 또는 비 별칭 레코드 선택 및 AWS 리소스로 인터넷 트래픽 라우팅 단원을 참조하세요.

리소스로의 인터넷 트래픽 라우팅에 대한 자세한 내용은 Amazon Route 53을 DNS 서비스로 구성 단원을 참조하십시오.

Amazon Route 53가 도메인의 트래픽을 라우팅하는 방법

웹 서버나 Amazon S3 버킷 같은 리소스로 인터넷 트래픽을 라우팅하도록 Amazon Route 53를 구성한 후에는 누군가 www.example.com의 콘텐츠를 요청하면 몇 밀리초 안에 다음과 같은 일이 이루어집니다.



1. 사용자가 웹 브라우저를 열어 주소 표시줄에 www.example.com을 입력하고 Enter 키를 누릅니다.
2. www.example.com에 대한 요청은 일반적으로 케이블 인터넷 공급업체, DSL 광대역 공급업체 또는 기업 네트워크 같은 인터넷 서비스 제공업체(ISP)가 관리하는 DNS 해석기로 라우팅됩니다.
3. ISP의 DNS 해석기는 www.example.com에 대한 요청을 DNS 루트 이름 서버에 전달합니다.
4. DNS 해석기는 www.example.com에 대한 요청을 이번에는 .com 도메인의 TLD 이름 서버 중 하나에 다시 전달합니다. .com 도메인의 이름 서버는 example.com 도메인과 연관된 4개의 Route 53 이름 서버의 이름을 사용하여 요청에 응답합니다.

DNS 해석기는 4개의 Route 53 이름 서버를 캐싱(저장)합니다. 다음에 누군가 example.com을 찾아볼 때 example.com의 이름 서버가 이미 있으므로 해석기는 3단계와 4단계를 건너뜁니다. 이름 서버는 일반적으로 2일 동안 캐시에 저장됩니다.

5. DNS 해석기는 Route 53 이름 서버 하나를 선택하여 www.example.com에 대한 요청을 해당 이름 서버에 전달합니다.
6. Route 53 이름 서버는 example.com 호스팅 영역에서 www.example.com 레코드를 찾아 웹 서버의 IP 주소 192.0.2.44 등 연관된 값을 받아 이 IP 주소를 DNS 해석 프로그램에 반환합니다.
7. DNS 해석기가 마침내 사용자에게 필요한 IP 주소를 해석해 냅니다. 해석기는 이 값을 웹 브라우저로 반환합니다.

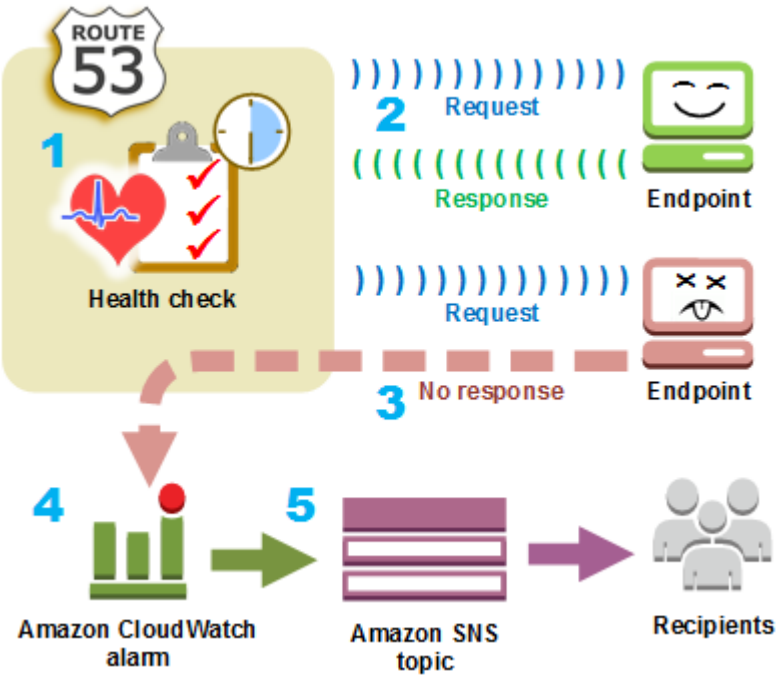
> **Note**
>
> 또한 DNS 해석기는 다음에 누군가가 example.com을 탐색할 때 보다 빠르게 응답할 수 있도록 사용자가 지정하는 일정 기간 동안 example.com의 IP 주소를 캐시에 저장합니다. 자세한 내용은 time to live (TTL) 섹션을 참조하세요.

8. 웹 브라우저는 DNS 해석기로부터 얻은 IP 주소로 www.example.com에 대한 요청을 전송합니다. 여기가 콘텐츠가 있는 곳, 예컨대 Amazon EC2 인스턴스 또는 웹 사이트 엔드포인트로 구성된 Amazon S3 버킷에서 실행되는 웹 서버입니다.
9. 192.0.2.44에 있는 웹 서버 또는 그 밖의 리소스는 www.example.com의 웹 페이지를 웹 브라우저에게 반환하고, 웹 브라우저는 이 페이지를 표시합니다.

Amazon Route 53가 리소스의 상태를 확인하는 방법

Amazon Route 53 상태 확인은 웹 서버 및 이메일 서버 같은 리소스의 상태를 모니터링합니다. 필요할 경우, 상태 확인이 가능하도록 Amazon CloudWatch 경보를 구성하여 리소스를 사용할 수 없게 될 때 알림을 수신할 수 있습니다.

다음은 리소스를 사용할 수 없게 될 때 알림을 수신하고자 하는 경우, 상태 확인이 작동하는 방식의 개요입니다.



1. 상태 확인을 생성하고 원하는 상태 확인 작동 방식을 정의하는 값을 지정하는 방법은 다음과 같습니다.
   - Route 53으로 모니터링하려는 웹 서버 등 엔드포인트의 IP 주소나 도메인 이름입니다. (다른 상태 확인의 상태 또는 CloudWatch 경보의 상태도 모니터링할 수 있습니다.)
   - Amazon Route 53가 상태 확인에 사용할 프로토콜: HTTP, HTTPS 또는 TCP.
   - Route 53가 엔드포인트에 요청을 전송하는 주기입니다. 이것을 요청 간격이라고 합니다.
   - Route 53가 비정상으로 판단하기 전에 엔드포인트가 요청에 대한 응답을 연속해 실패하는 횟수입니다. 이것을 장애 임계치라고 합니다.
   - 필요할 경우, 엔드포인트가 비정상임을 Route 53가 탐지할 때 원하는 알림 방식입니다. 알림을 구성하면 Route 53에서 자동으로 CloudWatch 경보를 설정합니다. CloudWatch는 Amazon SNS 사용하여 엔드포인트가 비정상임을 사용자에게 알립니다.
2. Route 53는 사용자가 상태 확인에서 지정한 시간 간격으로 엔드포인트에 요청을 전송하기 시작합니다.

   엔드포인트가 요청에 응답하면 Route 53는 엔드포인트가 정상이라고 판단하고 아무런 조치도 취하지 않습니다.
3. 엔드포인트가 요청에 응답하지 않으면 Route 53는 엔드포인트가 응답하지 않는 연속적 요청 횟수를 세기 시작합니다.
   - 횟수가 장애 임계치로 지정된 값에 도달하면 Route 53는 엔드포인트가 비정상이라고 판단합니다.

- 횟수가 장애 임계치에 도달하기 전에 엔드포인트가 다시 응답하기 시작하면 Route 53는 횟수를 0으로 리셋하고, CloudWatch는 사용자에게 연락하지 않습니다.

4. Route 53가 엔드포인트가 비정상이라고 판단하고 사용자가 상태 확인 알림을 구성한 경우, Route 53는 CloudWatch에 알립니다.

   알림을 구성하지 않은 경우에도 Route 53 콘솔에서 Route 53 상태 확인의 상태를 확인할 수 있습니다. 자세한 내용은 상태 확인의 상태 모니터링 및 알림 수신 섹션을 참조하세요.
5. 상태 확인 알림을 구성한 경우, CloudWatch는 경보를 트리거하고 Amazon SNS를 사용하여 지정된 수신자에게 알림을 전송합니다.

지정된 엔드포인트의 상태 확인 외에도 하나 이상의 다른 상태 확인을 검사하도록 상태 확인을 구성하면 지정된 수의 리소스(예컨대 5대의 웹 서버 중 2대)를 사용할 수 없을 때 알림을 수신할 수 있습니다. 또 CloudWatch 경보의 상태를 확인하도록 상태 확인을 구성하면 리소스가 요청에 응답하는 경우뿐 아니라 다양한 기준에 따라 알림을 수신할 수 있습니다.

웹 서버 또는 데이터베이스 서버와 같이 동일한 기능을 수행하는 다수의 리소스를 보유한 상황에서 Route 53가 트래픽을 정상적인 리소스에만 라우팅하도록 만들고 싶다면 상태 확인을 해당 리소스의 각 레코드에 연결하여 DNS 장애 조치를 구성할 수 있습니다. 상태 확인이 기본 리소스가 비정상이라고 판정하면, Route 53는 연결된 레코드에서 벗어나도록 트래픽을 라우팅합니다.

Route 53를 사용하여 리소스 상태를 모니터링하는 방법에 대한 자세한 내용은 Amazon Route 53 상태 확인 생성 섹션을 참조하세요.

Amazon Route 53 개념

다음은 Amazon Route 53 개발자 안내서에서 논의되는 개념의 개요입니다.

주제

- 도메인 등록 개념
- Domain Name System(DNS) 개념
- 제어 및 데이터 영역 개념
- 상태 확인 개념

도메인 등록 개념

다음은 도메인 등록과 관련된 개념의 개요입니다.

- domain name
- domain registrar
- domain registry
- domain reseller
- top-level domain (TLD)

도메인 이름

사용자가 웹 사이트 또는 웹 애플리케이션에 액세스하기 위해 웹 브라우저의 주소 표시줄에 입력하는 example.com과 같은 이름. 인터넷에서 웹 사이트 또는 웹 애플리케이션을 사용할 수 있도록 하려면 먼저 도메인 이름을 등록해야 합니다. 자세한 내용은 도메인 등록 방식 섹션을 참조하세요.

도메인 등록 기관

국제인터넷주소관리기구(ICANN)가 인증한, 특정 최상위 도메인(TLD) 등록을 처리하는 회사. 도메인의 등록 기관을 확인하는 방법은 등록 기관 찾기 단원을 참조하세요.

도메인 등록처

특정 최상위 도메인을 가진 도메인을 판매할 권리를 소유한 회사. 예를 들어 VeriSign은 .com TLD를 가진 도메인을 판매할 권리를 소유한 등록 기관입니다. 도메인 등록 기관은 지리적 TLD를 위한 거주 요건 등 도메인 등록 규칙을 정의합니다. 도메인 등록 기관은 동일한 TLD를 갖는 모든 도메인 이름의 권한 데이터베이스도 유지하고 있습니다. 등록 기관의 데이터베이스에는 각 도메인의 연락처 정보와 이름 서버 등의 정보가 포함되어 있습니다.

도메인 리셀러

Amazon Registrar 같은 등록 기관을 위해 도메인 이름을 판매하는 회사입니다. Amazon Route 53는 Amazon Registrar 및 Amazon 등록 기관 협력사인 Gandi의 도메인 리셀러입니다.

상위 수준 도메인(TLD)

.com, .org 또는 .ninja 등 도메인 이름의 마지막 부분. 최상위 도메인에는 다음의 두 가지 유형이 있습니다.

일반적인 최상위 도메인

이런 TLD는 일반적으로 사용자에게 웹 사이트에서 무엇을 보게 될지 알려 줍니다. 예를 들어 .bike라는 TLD를 가진 도메인 이름은 모터사이클 또는 자전거 업체나 조직의 웹 사이트와 연관되는 경우가 많습니다. 몇 가지 예외는 있지만 원하는 어떤 TLD건 사용할 수 있으므로 자전거 클럽의 도메인 이름에 .hockey TLD가 사용될 수도 있습니다.

지리적 최상위 도메인

이 TLD는 국가나 도시 같은 지리적 영역과 연관됩니다. 일부 지리적 TLD의 등록 기관에는 거주 요건이 있는 반면 the section called ".io(영국령 인도양 식민지)" 같은 등록 기관은 일반 TLD 사용을 허용하거나 심지어 권장합니다.

Route 53에 도메인 이름을 등록할 때 사용할 수 있는 TLD 목록은 Amazon Route 53에 등록할 수 있는 도메인 섹션을 참조하세요.

Domain Name System(DNS) 개념

다음은 Domain Name System(DNS)과 관련된 개념의 개요입니다.

- alias record
- authoritative name server
- CIDR block
- DNS query
- DNS resolver
- Domain Name System (DNS)
- hosted zone
- IP address
- name servers
- private DNS
- recursive name server
- record (DNS record)
- reusable delegation set
- routing policy
- subdomain
- time to live (TTL)

별칭 레코드

Amazon Route 53을 사용하여 Amazon CloudFront 배포 및 Amazon S3 버킷과 같은 AWS 리소스로 트래픽을 라우팅하기 위해 생성할 수 있는 레코드 유형입니다. 자세한 내용은 별칭 또는 비 별칭 레코드 선택 단원을 참조하십시오.

권한 이름 서버

Domain Name System(DNS)의 한 부분에 관한 확정적 정보가 있고 DNS 해석기의 요청에 대해 해당되는 정보를 반환하여 응답하는 이름 서버. 예를 들어 .com 최상위 도메인(TLD)의 권한 이름 서버는 등록된 모든 .com 도메인의 이름 서버의 이름을 알고 있습니다. .com 권한 이름 서버는 DNS 해석기로부터 example.com에 대한 요청을 수신하면 example.com 도메인의 DNS 서비스에 해당하는 이름 서버의 이름으로 응답합니다.

Route 53 이름 서버는 Route 53를 DNS 서비스로 사용하는 모든 도메인의 권한 이름 서버입니다. 이름 서버는 도메인의 호스팅 영역에서 사용자가 생성한 레코드를 기반으로 사용자가 원하는 도메인 및 하위 도메인 트래픽 라우팅 방법을 알고 있습니다. (Route 53 이름 서버는 Route 53를 DNS 서비스로 사용하는 도메인의 호스팅 영역을 저장합니다.)

예를 들어 Route 53 이름 서버는 www.example.com에 대한 요청을 수신하면 해당 레코드를 찾아 레코드에 지정된 192.0.2.33과 같은 IP 주소를 반환합니다.

CIDR 블록

CIDR 블록은 IP 기반 라우팅과 함께 사용되는 IP 범위입니다. Route 53에서는 IPv4의 경우 /0에서 /24까지, IPv6의 경우 /0에서 /48까지 CIDR 블록을 지정할 수 있습니다. 예를 들어 /24 IPv4 CIDR 블록은 256개의 연속적인 IP 주소를 포함합니다. CIDR 블록(또는 IP 범위) 집합을 CIDR 위치로 그룹화할 수 있으며, CIDR 위치는 다시 재사용 가능한 CIDR 컬렉션으로 그룹화됩니다.

DNS 쿼리

일반적으로 컴퓨터나 스마트폰 같은 장치가 도메인 이름과 연결된 리소스를 위해 Domain Name System(DNS)에 제출하는 요청. DNS 쿼리의 가장 일반적인 예는 사용자가 브라우저를 열어 주소 표시줄에 도메인 이름을 입력하는 경우입니다. DNS 쿼리에 대한 일반적 응답은 웹 서버 같은 리소스에 연결된 IP 주소입니다. 요청을 시작하는 장치는 IP 주소를 사용하여 리소스와 통신합니다. 예를 들어 브라우저는 IP 주소를 사용하여 웹 서버로부터 웹 페이지를 불러옵니다.

DNS 해석기

흔히 인터넷 서비스 제공업체(ISP)가 관리하며 사용자 요청과 DNS 이름 서버 사이에서 중개 역할을 하는 DNS 서버. 브라우저를 열어 주소 표시줄에 도메인 이름을 입력하면 쿼리는 먼저 DNS 해석기로 전송됩니다. 해석기는 DNS 이름 서버와 통신하여 웹 서버 등 해당되는 리소스의 IP 주소를 가져옵니다. DNS 해석기는 재귀 이름 서버라고도 하는데, 응답(일반적으로 IP 주소)을 얻을 때까지 일련의 권한 DNS 이름 서버에 요청을 전송하고 사용자의 장치(예: 노트북 컴퓨터의 웹 브라우저)로 이 응답을 반환하기 때문입니다.

도메인 이름 시스템(DNS)

컴퓨터, 스마트폰, 태블릿 및 기타 IP 지원 장치가 서로 통신하도록 도와주는 전 세계 서버 네트워크. Domain Name System(DNS)은 example.com 같이 쉽게 이해할 수 있는 도메인 이름을 컴퓨터가 인터넷에서 서로를 찾을 수 있도록 해 주는 IP 주소라는 숫자로 변환합니다.

또한 IP address 섹션도 참조하세요.

호스팅 영역

도메인(예: example.com)과 그 전체 하위 도메인(예: www.example.com, retail.example.com, seattle.accounting.example.com)의 트래픽을 라우팅하는 방법에 대한 정보를 포함하고 있는 레코드의 컨테이너입니다. 호스팅 영역은 해당 도메인과 이름이 같습니다.

예를 들어 example.com의 호스팅 영역에는 www.example.com의 트래픽을 192.0.2.243이라는 IP 주소의 웹 서버로 라우팅하는 것에 관한 정보가 있는 레코드와 example.com의 이메일을 mail1.example.com과 mail2.example.com이라는 2개의 이메일 서버로 라우팅하는 것에 관한 정보가 있는 레코드가 포함될 수 있습니다. 각각의 이메일 서버에는 자체 레코드도 필요합니다.

또한 record (DNS record) 섹션도 참조하세요.

IP 주소

노트북, 스마트폰 또는 웹 서버 같은 장치가 인터넷 상에서 다른 장치와 통신할 수 있도록 인터넷 상에서 장치에 할당되는 번호입니다. IP 주소는 다음 형식 중 하나로 되어 있습니다.

- 192.0.2.44와 같은 인터넷 프로토콜 버전 4(IPv4)
- 2001:0db8:85a3:0000:0000:abcd:0001:2345와 같은 인터넷 프로토콜 버전 6(IPv6)

Route 53는 다음과 같은 목적으로 IPv4 및 IPv6 주소를 모두 지원합니다.

- IPv4 주소의 경우 A 타입, IPv6 주소의 경우 AAAA 타입이 있는 레코드를 생성할 수 있습니다.
- IPv4 주소나 IPv6 주소로 요청을 전송하는 상태 확인을 만들 수 있습니다.
- DNS 해석기는 IPv6 네트워크 상에 있는 경우, IPv4 또는 IPv6를 사용하여 요청을 Route 53에 제출할 수 있습니다.

이름 서버

도메인 이름을 컴퓨터 간 통신에 사용되는 IP 주소로 변환하는 Domain Name System(DNS) 내 서버. 네임서브는 재귀 네임서버(DNS resolver이라고도 함)이거나 authoritative name server입니다.

DNS가 리소스로 트래픽을 라우팅하는 방법과 그 과정에서의 Route 53의 역할의 개요는 Amazon Route 53가 도메인의 트래픽을 라우팅하는 방법 섹션을 참조하세요.

프라이빗 DNS

도메인과 그 하위 도메인의 트래픽을 하나 이상의 Amazon Virtual Private Cloud(VPC) 내의 Amazon EC2 인스턴스로 라우팅하도록 해 주는 Domain Name System(DNS)의 로컬 버전입니다. 자세한 내용은 프라이빗 호스팅 영역 사용 섹션을 참조하세요.

레코드(DNS 레코드)

도메인 또는 하위 도메인의 트래픽을 라우팅할 방법을 정의하는 데 사용되는 호스팅 영역 내 객체. 예를 들어 IP 주소가 192.0.2.234인 웹 서버로 트래픽을 라우팅하는 example.com과 www.example.com의 레코드를 생성할 수 있습니다.

Route 53 전용 레코드가 제공하는 기능에 관한 정보를 비롯하여 레코드에 대한 자세한 내용은 Amazon Route 53을 DNS 서비스로 구성 섹션을 참조하세요.

재귀 이름 서버

DNS resolver 섹션을 참조하세요.

재사용 가능한 위임 세트

2개 이상의 호스팅 영역에 사용할 수 있는 4개의 권한 이름 서버 세트. 기본적으로 Route 53는 각각의 새 호스팅 영역에 무작위로 선택된 이름 서버를 할당합니다. 도메인의 수가 많은 경우, DNS 서비스를 Route 53으로 보다 쉽게 마이그레이션하려면 재사용 가능한 위임 세트를 만든 다음 새 호스팅 영역에 재사용 가능한 위임 세트를 연결할 수 있습니다. (기존 호스팅 영역과 연결된 이름 서버는 변경할 수 없습니다.)

프로그래밍 방식으로 재사용 가능한 위임 세트를 만들어 호스팅 영역에 연결할 수 있습니다. Route 53 콘솔 사용은 지원되지 않습니다. 자세한 내용은 Amazon Route 53 API 참조의 CreateHostedZone 및 CreateReusableDelegationSet를 참조하세요. AWS SDK, AWS Command Line Interface 및 AWS Tools for Windows PowerShell에서도 같은 기능을 사용할 수 있습니다.

라우팅 정책

Route 53가 DNS 쿼리에 응답하는 방식을 결정하는 레코드에 대한 설정입니다. Route 53는 다음의 라우팅 정책을 지원합니다.

- 단순 라우팅 정책(Simple routing policy) - 도메인에 대해 특정 기능을 수행하는 하나의 리소스로 인터넷 트래픽을 라우팅하는 데 사용합니다(예: example.com 웹 사이트의 콘텐츠를 제공하는 하나의 웹 서버).
- 장애 조치 라우팅 정책(Failover routing policy) - 액티브-패시브 장애 조치를 구성하려는 경우에 사용합니다.

- 지리 위치 라우팅 정책(Geolocation routing policy) - 사용자의 위치에 기반하여 인터넷 트래픽을 리소스로 라우팅하려는 경우에 사용합니다.
- 지리 근접 라우팅 정책(Geoproximity routing policy) - 리소스의 위치를 기반으로 트래픽을 라우팅하고 필요에 따라 한 위치의 리소스에서 다른 위치의 리소스로 트래픽을 보내려는 경우에 사용합니다.
- 지연 시간 라우팅 정책(Latency routing policy) – 여러 위치에 리소스가 있고 최상의 지연 시간을 제공하는 리소스로 트래픽을 라우팅하려는 경우에 사용합니다.
- IP 기반 라우팅 정책 - 사용자의 위치에 기반하여 트래픽을 라우팅하고 트래픽이 시작되는 IP 주소가 있는 경우에 사용합니다.
- 다중 응답 라우팅 정책(Multivalue answer routing policy) - Route 53가 DNS 쿼리에 무작위로 선택된 최대 8개의 정상 레코드로 응답하게 하려는 경우에 사용합니다.
- 가중치 기반 라우팅 정책(Weighted routing policy) - 사용자가 지정하는 비율에 따라 여러 리소스로 트래픽을 라우팅하려는 경우에 사용합니다.

자세한 내용은 라우팅 정책 선택 섹션을 참조하세요.

하위 도메인

등록된 도메인 이름 앞에 하나 이상의 레이블이 붙은 도메인 이름. 예를 들어 도메인 이름 example.com을 등록하면 www.example.com은 하위 도메인이 됩니다. example.com 도메인의 호스팅 영역 accounting.example.com을 만들면 seattle.accounting.example.com은 하위 도메인이 됩니다.

하위 도메인의 트래픽을 라우팅하려면 www.example.com 같이 원하는 이름을 가진 레코드를 생성하고 웹 서버의 IP 주소 등 해당 값을 지정하십시오.

유지 시간(TTL)

레코드의 현재 값을 얻기 위해 Route 53에 또 다른 요청을 제출하기 전에 DNS 해석기가 해당 레코드의 값을 캐싱(저장)할 시간(초). DNS 해석기가 TTL 만료 전에 동일한 도메인에 대한 또 다른 요청을 수신하는 경우, 해석기는 캐싱된 값을 반환합니다.

TTL이 길수록 Route 53 요금이 줄어드는데, 요금은 Route 53가 응답하는 DNS 쿼리 수에 부분적으로 기반하기 때문입니다. TTL이 짧으면 www.example.com 웹 서버의 IP 주소 변경 등을 통해 레코드에서 값을 변경한 후 DNS 해석기가 예전의 리소스로 트래픽을 라우팅하는 시간이 줄어듭니다.

제어 및 데이터 영역 개념

다음은 Amazon Route 53가 기능을 제어 및 데이터 영역으로 나누는 방법과 관련된 개념의 개요입니다. Route 53 서비스는 대부분의 AWS 서비스와 같이 리소스 생성, 업데이트 및 삭제와 같은 관리 작업을 수행할 수 있는 컨트롤 플레인과 서비스의 핵심 기능을 제공하는 데이터 영역을 포함합니다. 두 기능 모두 신뢰할 수 있도록 구축되었지만 제어 영역은 데이터 일관성을 위해 최적화되는 반면 데이터 영역은 가용성을 위해 최적화됩니다. 데이터 영역의 복원력 있는 설계로 드물게 중단되는 이벤트에서도 가용성을 유지할 수 있으며 그 동안에는 제어 영역을 사용하지 못할 수 있습니다. 따라서 가용성이 중요한 곳에서는 데이터 영역 기능을 사용하는 것이 좋습니다.

Route 53 퍼블릭 및 프라이빗 DNS 및 상태 확인의 경우 컨트롤 플레인은 us-east-1에 위치 AWS 리전하고 데이터 플레인은 전역적으로 분산됩니다.

Amazon Route 53는 다음과 같이 제어 및 데이터 영역으로 나뉩니다.

- Route 53 퍼블릭 및 프라이빗 DNS의 경우 제어 영역은 Route 53 APIs로 구성되며, 이를 통해 Route 53 및 트래픽 흐름 APIs. Route 53 콘솔은 us-east-1에 있지만 AWS 리전에서 해당 리전에 장애가 있다고 AWS 판단하면 us-west-2에서 Route 53 콘솔을 제공합니다 AWS 리전. 데이터 영역은 200개 이상의 상호 접속 위치(PoP) 위치에서 실행되는 신뢰할 수 있는 DNS 서비스로서 호스팅 영역 및 상태 확인 데이터를 기반으로 DNS 쿼리에 응답합니다.
- Route 53 상태 확인의 경우 컨트롤 플레인은 상태 확인을 생성, 업데이트 및 삭제하는 데 사용할 수 있는 Route 53 APIs 구성됩니다. Route 53 상태 확인 콘솔은 us-east-1에 있지만 AWS 리전,에서 해당 리전에 장애가 있다고 AWS 판단하면 us-west-2에서 Route 53 상태 확인 콘솔을 제공합니다 AWS 리전. 데이터 영역은 상태 확인을 수행하고 결과를 집계하여 Route 53 퍼블릭 및 프라이빗 DNS와 AWS Global Accelerator의 데이터 영역에 전달하는 전 세계에 분산된 서비스입니다.
- 의 경우 제어 영역은 Amazon VPC 설정Amazon Route 53 Resolver, 해석기 규칙, 쿼리 로깅 정책 및 DNS 방화벽 정책을 관리할 수 있는 Route 53 Resolver APIs로 구성됩니다. 데이터 영역은 VPC에서 DNS 쿼리에 응답하는 DNS 해석기 서비스, 쿼리를 다른 해석기로 전달하는 엔드포인트, DNS 쿼리를 필터링하는 정책을 적용하는 DNS 방화벽 데이터 영역입니다. Resolver는 리전 서비스이며 제어 및 데이터 영역은 각각 독립적으로 실행됩니다 AWS 리전.
- Route 53 도메인 등록은 us-east-1 AWS 리전의 제어 영역에서만 관리됩니다.

데이터 영역, 제어 영역 및가 고가용성 목표를 충족하기 위해 서비스를 AWS 빌드하는 방법에 대한 자세한 내용은 Amazon Builders' Library의 가용 영역을 사용한 정적 안정성 문서를 참조하세요.

상태 확인 개념

다음은 Amazon Route 53 상태 확인과 관련된 개념의 개요입니다.

- DNS failover
- endpoint
- health check

DNS 장애 조치

비정상인 리소스로부터 정상인 리소스로 트래픽을 라우팅하는 방법. 동일한 기능을 수행하는 리소스가 두 개 이상(예: 두 개 이상의 웹 서버 또는 메일 서버) 있는 경우 리소스의 상태를 확인하도록 Route 53 상태 확인을 구성하고 정상인 리소스로만 트래픽을 라우팅하도록 호스팅 영역의 레코드를 구성할 수 있습니다.

자세한 내용은 DNS 장애 조치 구성 섹션을 참조하세요.

엔드포인트

상태를 모니터링하도록 상태 확인을 구성하는 웹 서버 또는 이메일 서버 등의 리소스. IPv4 주소(192.0.2.243), IPv6 주소(2001:0db8:85a3:0000:0000:abcd:0001:2345), 또는 도메인 이름(example.com)으로 엔드포인트를 지정할 수 있습니다.

> **Note**
>
> 다른 상태 확인의 상태를 모니터링하거나 CloudWatch 경보의 경보 상태를 모니터링하는 상태 확인도 만들 수 있습니다.

상태 확인

다음을 수행할 수 있도록 해 주는 Route 53 구성 요소.

- 웹 서버 등 지정된 엔드포인트가 정상인지 모니터링
- 필요할 경우, 엔드포인트가 비정상이 될 때 알림 수신
- 필요할 경우, DNS 장애 조치를 구성해 비정상인 리소스로부터 정상인 리소스로 인터넷 트래픽을 다시 라우팅 가능

상태 확인을 만들고 사용하는 자세한 방법은 Amazon Route 53 상태 확인 생성 를 참조하십시오.

Amazon Route 53 시작 방법

Amazon Route 53 시작하기에 대한 자세한 내용은 이 안내서의 다음 주제를 참조하십시오.

- Amazon Route 53 설정: 가입 방법 AWS, AWS 계정에 대한 액세스 보호 방법, Route 53에 대한 프로그래밍 방식 액세스를 설정하는 방법을 설명합니다.
- Amazon Route 53 시작하기에서는 도메인 이름 등록 방법, Amazon S3 버킷을 생성하고 정적 웹 사이트를 호스팅하도록 구성하는 방법, 인터넷 트래픽을 해당 웹 사이트로 라우팅하는 방법을 설명합니다.

Amazon Route 53 액세스

Amazon Route 53에 액세스하는 방법은 다음과 같습니다.

- AWS Management Console -이 가이드의 절차에서는를 사용하여 작업을 AWS Management Console 수행하는 방법을 설명합니다.
- AWS SDKs- SDK를 제공하는 AWS 프로그래밍 언어를 사용하는 경우 SDK를 사용하여 Route 53에 액세스할 수 있습니다. SDK는 인증을 간편하게 만들고, 개발 환경에 쉽게 통합되며, Route 53 명령에 쉽게 액세스할 수 있게 해줍니다. 자세한 내용은 Amazon Web Services용 도구를 참조하세요.
- Route 53 API – SDK를 사용할 수 없는 프로그래밍 언어를 사용하는 경우 API 작업 및 API 요청 방법에 대한 자세한 내용은 Amazon Route 53 API 참조에서 확인하세요.
- AWS Command Line Interface— 자세한 정보는 AWS Command Line Interface사용 설명서에서 AWS Command Line Interface 설정하기를 참조하세요.
- AWS Tools for Windows PowerShell— 자세한 정보는 AWS Tools for Windows PowerShell 사용 설명서에서 AWS Tools for Windows PowerShell설정하기를 참조하세요.

AWS 자격 증명 및 액세스 관리

Amazon Route 53는 조직에서 다음을 수행할 수 있는 서비스인 AWS Identity and Access Management (IAM)과 통합됩니다.

- 조직 AWS 계정에서 사용자 및 그룹 생성
- AWS 계정 내 사용자 간에 계정 리소스를 쉽게 공유
- 각 사용자에게 고유한 보안 자격 증명을 할당합니다.
- 서비스 및 리소스에 대한 사용자 액세스 상세 제어

예를 들어 Route 53에서 IAM을 사용하여 AWS 계정에서 새 호스팅 영역을 생성하거나 레코드를 변경할 수 있는 사용자를 제어할 수 있습니다.

IAM에 대한 전반적인 정보는 다음을 참조하십시오.

- Amazon Route 53의 Identity and Access Management
- Identity and Access Management(IAM)
- IAM 사용 설명서

Amazon Route 53 요금 및 결제

다른 AWS 제품과 마찬가지로 Amazon Route 53 사용에 대한 계약이나 최소 약정은 없습니다. 구성한 호스팅 영역과 Route 53에서 응답하는 DNS 쿼리 수에 대해서만 비용을 지불합니다. 자세한 내용은 Amazon Route 53 요금을 참조하십시오.

청구서를 보고 계정 및 결제를 관리하는 방법을 포함하여 AWS 서비스에 대한 결제에 대한 자세한 내용은 AWS Billing 사용 설명서를 참조하세요.

AWS SDK에서 Route 53 사용

AWS 소프트웨어 개발 키트(SDKs)는 널리 사용되는 많은 프로그래밍 언어에 사용할 수 있습니다. 각 SDK는 개발자가 선호하는 언어로 애플리케이션을 쉽게 구축할 수 있도록 하는 API, 코드 예시 및 설명서를 제공합니다.

SDK 설명서	코드 예제
AWS SDK for C++	AWS SDK for C++ 코드 예제
AWS CLI	AWS CLI 코드 예제
AWS SDK for Go	AWS SDK for Go 코드 예제
AWS SDK for Java	AWS SDK for Java 코드 예제
AWS SDK for JavaScript	AWS SDK for JavaScript 코드 예제
AWS SDK for Kotlin	AWS SDK for Kotlin 코드 예제
AWS SDK for .NET	AWS SDK for .NET 코드 예제
AWS SDK for PHP	AWS SDK for PHP 코드 예제

SDK 설명서	코드 예제
AWS Tools for PowerShell	Tools for PowerShell 코드 예시
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) 코드 예제
AWS SDK for Ruby	AWS SDK for Ruby 코드 예제
AWS SDK for Rust	AWS SDK for Rust 코드 예제
AWS SDK for SAP ABAP	AWS SDK for SAP ABAP 코드 예제
AWS SDK for Swift	AWS SDK for Swift 코드 예제

Route 53에 대한 구체적인 예는 AWS SDKs를 사용하는 Route 53의 코드 예제 섹션을 참조하세요.

> **가용성 예제**
>
> 필요한 예제를 찾을 수 없습니까? 이 페이지 하단의 피드백 제공 링크를 사용하여 코드 예시를 요청하세요.

Amazon Route 53 시작하기

Amazon Route 53로 도메인을 등록하고 정적 웹 사이트로 확인하는 DNS 쿼리에 응답하도록 Route 53를 구성하여 기본 단계를 시작합니다. 첫 번째 자습서에서는 오픈 Amazon S3 버킷에서 정적 웹 사이트를 호스팅하고, 두 번째 자습서에서는 Amazon CloudFront 배포를 사용하여 SSL/TLS를 웹 사이트에 제공합니다.

추정 비용

- 도메인을 등록 연간 요금은 9달러부터 시작하여 .com 등의 최상위 도메인의 경우에는 수백 달러까지 다양합니다. 자세한 내용은 Route 53 도메인 등록 요금을 참조하세요. 이 요금은 환불되지 않습니다.
- 도메인을 등록하면 도메인과 동일한 이름의 호스팅 영역이 자동으로 생성됩니다. 호스팅 영역을 사용하여 Route 53가 도메인의 트래픽을 라우팅할 장소를 지정할 수 있습니다.
- 이 자습서에서는 Amazon S3 버킷을 생성하고 샘플 웹 페이지를 업로드합니다. 신규 AWS 고객인 경우 Amazon S3를 무료로 시작할 수 있습니다. 기존 AWS 고객인 경우 요금은 저장하는 데이터의 양, 데이터에 대한 요청 수, 전송된 데이터의 양에 따라 달라집니다. 자세한 내용은 Amazon S3 요금을 참조하세요.
- CloudFront 요금은 데이터 요청 횟수, 사용하는 엣지 로케이션 수, 전송되는 데이터 양에 따라 청구됩니다. 자세한 내용은 CloudFront 요금을 참조하십시오.

주제

- Amazon Route 53 설정
- Amazon S3 버킷의 정적 웹 사이트에 대한 도메인 사용
- Amazon CloudFront 배포를 사용하여 정적 웹 사이트 제공

Amazon Route 53 설정

이 섹션의 개요와 절차는 시작하는 데 도움이 됩니다 AWS.

주제

- 에 가입 AWS 계정
- 관리자 액세스 권한이 있는 사용자 생성
- 도구 다운로드

에 가입 AWS 계정

가 없는 경우 다음 단계를 AWS 계정완료하여 생성합니다.

에 가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. 온라인 지시 사항을 따릅니다.

   등록 절차 중 전화를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   에 가입하면 AWS 계정AWS 계정 루트 사용자이 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

AWS 는 가입 프로세스가 완료된 후 확인 이메일을 보냅니다. 언제든지 https://aws.amazon.com/으로 이동하고 내 계정을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

에 가입한 후 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 AWS 계정보호 AWS IAM Identity Center, AWS 계정 루트 사용자활성화 및 생성합니다.

보안 AWS 계정 루트 사용자

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자AWS Management Console로에 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 User Guide의 루트 사용자로 로그인을 참조하세요.
2. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자(콘솔)에 대한 가상 MFA 디바이스 활성화를 참조하세요.

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

지침은 AWS IAM Identity Center 사용 설명서의 AWS IAM Identity Center설정을 참조하세요.

2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

   를 자격 증명 소스 IAM Identity Center 디렉터리 로 사용하는 방법에 대한 자습서는 AWS IAM Identity Center 사용 설명서의 기본값으로 사용자 액세스 구성을 IAM Identity Center 디렉터리 참조하세요.

관리 액세스 권한이 있는 사용자로 로그인

- IAM IDentity Center 사용자로 로그인하려면 IAM Identity Center 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

  IAM Identity Center 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 사용 설명서의 AWS 액세스 포털에 로그인을 참조하세요.

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Create a permission set를 참조하세요.

2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 Add groups를 참조하세요.

도구 다운로드

에는 Amazon Route 53용 콘솔이 AWS Management Console 포함되어 있지만 프로그래밍 방식으로 서비스에 액세스하려면 다음을 참조하세요.

- API 가이드는 서비스가 지원하는 작업을 문서화하고 관련 SDK 및 CLI 설명서에 대한 링크를 제공합니다.
  - Amazon Route 53 API 참조
- 원시 HTTP 요청 수집과 같은 하위 수준의 세부 정보를 처리할 필요 없이 API를 호출하려면 AWS SDK를 사용할 수 있습니다. AWS SDKs는 AWS 서비스의 기능을 캡슐화하는 함수와 데이터 형식을 제공합니다. AWS SDK를 다운로드하고 설치 지침에 액세스하려면 해당 페이지를 참조하세요.
  - Java

- JavaScript
- .NET
- Node.js
- PHP
- Python
- Ruby

AWS SDKs. https://aws.amazon.com/tools/

- AWS Command Line Interface (AWS CLI)를 사용하여 명령줄에서 여러 AWS 서비스를 제어할 수 있습니다. 또한, 스크립트를 사용하여 명령을 자동화할 수 있습니다. 자세한 내용은 AWS Command Line Interface 단원을 참조하십시오.
- AWS Tools for Windows PowerShell 는 이러한 AWS 서비스를 지원합니다. 자세한 내용은 AWS Tools for PowerShell Cmdlet 참조를 참조하세요.

Amazon S3 버킷의 정적 웹 사이트에 대한 도메인 사용

이 시작하기 자습서는 다음 작업의 수행 방법을 보여줍니다.

- example.com 등의 도메인 이름 등록
- Amazon S3 버킷을 만들고 웹 사이트를 호스팅하도록 버킷 구성
- 샘플 웹 사이트를 만들고 S3 버킷에 해당 파일을 저장
- 트래픽을 새 웹 사이트로 라우팅하도록 Amazon Route 53 구성

완료되면 브라우저를 열고 도메인 이름을 입력하여 웹 사이트를 볼 수 있습니다.

> **Note**
>
> 기존 도메인을 Route 53로 이전할 수도 있지만 새 도메인을 등록하는 것보다 본 프로세스가 복잡하고 시간이 더 많이 걸립니다. 자세한 내용은 도메인 등록을 Amazon Route 53으로 이전하기 단원을 참조하십시오.

주제

- 사전 조건

사전 조건

시작하기 전에 먼저 Amazon Route 53 설정의 단계를 완료해야 합니다.

1단계: 도메인 등록

example.com과 같은 도메인 이름을 사용하려면 사용되고 있지 않은 도메인 이름을 찾아 등록해야 합니다. 도메인 이름을 등록하면 일반적으로 1년 동안 인터넷 어디서나 도메인 이름을 독점적으로 사용할 수 있습니다. 기본적으로 매년 말에 도메인 이름이 자동으로 갱신되지만 자동 갱신은 꺼둘 수 있습니다. 자세한 내용은 새 도메인 등록 단원을 참조하십시오.

2단계: 루트 도메인에 대한 S3 버킷 생성

Amazon S3를 사용하면 어디서든 인터넷에 데이터를 저장하고 조회할 수 있습니다. 데이터를 체계화하려면 버킷을 만들고 AWS Management Console을 사용하여 버킷에 데이터를 업로드합니다. Amazon S3를 사용하여 버킷에 정적 웹 사이트를 호스팅할 수 있습니다. 다음 절차에서는 버킷 생성 방법을 설명합니다.

루트 도메인에 대한 S3 버킷을 생성하려면

1. https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 만들기를 선택합니다.

3. 다음 값을 입력합니다.

   버킷 이름

   example.com 같은 도메인 이름을 입력합니다.

   리전

   대부분의 사용자와 가장 가까운 리전을 선택합니다.

   선택한 리전을 적어 둡니다. 이 프로세스의 뒷부분에서 이 정보가 필요합니다.

4. 기본 설정을 적용하고 버킷을 생성하려면 버킷 생성을 선택합니다.

3단계: 선택 사항: 하위 도메인에 대한 다른 S3 버킷 생성

앞의 절차에서 example.com 같은 도메인 이름의 버킷을 만들었습니다. 이로써 사용자들이 example.com 같은 도메인 이름을 사용하여 웹 사이트에 액세스할 수 있습니다.

사용자들이 www.example.com 같은 www.*your-domain-name*을 사용하여 샘플 웹 사이트에 액세스할 수 있도록 하려면 두 번째 S3 버킷을 생성합니다. 첫 번째 버킷으로 트래픽을 라우팅하도록 두 번째 버킷을 구성합니다.

www.your-domain-name에 대한 S3 버킷을 생성하려면

1. 버킷 생성을 선택합니다.
2. 다음 값을 입력합니다.

   버킷 이름

   www.***your-domain-name***을 입력합니다. 예를 들어 도메인 이름 example.com을 등록한 경우, www.example.com을 입력합니다.

   리전

   첫 번째 버킷을 생성한 리전과 동일한 리전을 선택합니다.

3. 기본 설정을 적용하고 버킷을 생성하려면 [Create]를 선택합니다.

4단계: 웹 사이트 호스팅용 루트 도메인 버킷 설정

이제 S3 버킷이 생겼으므로 웹 사이트 호스팅에 대한 버킷을 구성할 수 있습니다.

S3 버킷에서 웹 사이트 호스팅을 허용하려면

1. https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷(Buckets) 목록에서 정적 웹 사이트 호스팅을 활성화하려는 버킷의 이름을 선택합니다.
3. 속성을 선택합니다.
4. 정적 웹 사이트 호스팅에서 사용을 선택합니다.
5. 이 버킷을 사용하여 웹 사이트를 호스팅합니다.를 선택합니다.
6. 정적 웹 사이트 호스팅에서 사용을 선택합니다.
7. 인덱스 문서(Index document)에 인덱스 문서 이름을 입력합니다(일반적으로 `index.html`).

   인덱스 문서 이름은 대소문자를 구분하며 S3 버킷에 업로드하려는 HTML 인덱스 문서의 파일 이름과 정확히 일치해야 합니다. 웹 사이트 호스팅용 버킷을 구성하는 경우 인덱스 문서를 지정해야 합니다. 루트 도메인이나 임의의 하위 폴더로 요청이 전송되면 Amazon S3가 이 인덱스 문서를 반환합니다.
8. (선택 사항) 4XX 클래스 오류에 대한 사용자 정의 오류 문서를 제공하려면 오류 문서(Error document)에 사용자 정의 오류 문서 파일 이름을 입력합니다.

   사용자 지정 오류 문서를 지정하지 않았는데 오류가 발생하면 Amazon S3에서 기본 HTML 오류 문서를 반환합니다.
9. (선택 사항) 고급 리디렉션 규칙을 지정하려면 리디렉션 규칙(Redirection rules)에 XML을 입력하여 규칙을 설명합니다.

   자세한 내용은 Amazon Simple Storage Service 사용 설명서의 고급 조건부 리디렉션 구성을 참조하십시오.
10. Save changes(변경 사항 저장)를 선택합니다.
11. 정적 웹 사이트 호스팅에서 엔드포인트를 기록합니다.

    엔드포인트는 버킷의 Amazon S3 웹 사이트 엔드포인트입니다. 버킷을 정적 웹 사이트로 구성한 후 이 엔드포인트를 사용하여 9단계: 도메인 엔드포인트 테스트에 표시된 대로 웹 사이트를 테스트할 수 있습니다.

    퍼블릭 액세스의 설정을 편집하고 퍼블릭 읽기 액세스를 허용하는 버킷 정책을 추가한 후 웹 사이트 엔드포인트를 사용하여 웹 사이트에 액세스할 수 있습니다.

5단계: (선택 사항): 웹 사이트 리디렉션에 대한 하위 도메인 버킷 설정

웹 사이트 호스팅용 루트 도메인 버킷을 구성하면 루트 도메인에 대한 모든 요청을 리디렉션하도록 하위 도메인 버킷을 선택적으로 구성할 수 있습니다. 예를 들어, 모든 요청을 구성하여 `www.example.com`이 `example.com`으로 리디렉션되게 할 수 있습니다.

리디렉션을 구성하려면

1. Amazon S3 콘솔의 버킷(Buckets) 목록에서 하위 도메인 버킷 이름(예: `www.example.com`)을 선택합니다.
2. [속성(Properties)]을 선택합니다.
3. 정적 웹 사이트 호스팅(Static website hosting)에서 편집(Edit)을 선택합니다.
4. 객체에 대한 요청 리디렉션(Redirect requests for an object)을 선택합니다.
5. 대상 버킷(Target bucket) 상자에 루트 도메인(예: **`example.com`**)을 입력합니다.
6. 프로토콜(Protocol)에서 http를 선택합니다.
7. Save changes(변경 사항 저장)를 선택합니다.

6단계: 인덱스를 업로드하여 웹 사이트 콘텐츠 생성

버킷용 정적 웹 사이트 호스팅을 허용할 때 인덱스 문서의 이름(예: **`index.html`**)을 입력합니다. 버킷용 정적 웹 사이트 호스팅을 허용한 후 인덱스 문서 이름이 있는 HTML 파일을 버킷에 업로드합니다.

인덱스 파일을 업로드하려면

1. 이 자습서의 간단한 한 페이지 웹 사이트로 사용할 수 있는 다음 예제 텍스트를 복사한 다음 텍스트 편집기에 붙여넣고 index.html로 저장합니다.

```
<html>
<head>
<title>Amazon Route 53 Getting Started</title>
</head>

<body>

<h1>Routing Internet Traffic to an Amazon S3 Bucket for Your Website</h1>

<p>For more information, see
```

```
<a href="https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/getting-
started.html">Getting Started with Amazon Route 53</a>
in the <emphasis>Amazon Route 53 Developer Guide</emphasis>.</p>

</body>

</html>
```

2. 버킷 목록에서 정적 웹 사이트 호스팅을 사용 설정하려는 버킷의 이름을 선택합니다.
3. Amazon S3 콘솔에서 S3 버킷에서 웹 사이트 호스팅을 허용하려면 절차를 통해 생성한 버킷의 이름을 선택합니다(링크된 버킷 이름 클릭).
4. 업로드 및 파일 추가를 선택하고 저장한 위치에서 index.html을 선택한 다음 업로드를 선택합니다.
5. 문서를 생성했는데 오류가 발생한 경우(예: **`404.html`**) 3단계에서 5단계를 따라 해당 오류를 업로드합니다.

7단계: S3 퍼블릭 액세스 차단 설정 편집

기본적으로 Amazon S3은 계정 및 버킷에 대한 퍼블릭 액세스를 차단합니다. 버킷을 사용하여 정적 웹 사이트를 호스팅하려는 경우 이러한 단계를 사용하여 퍼블릭 액세스 설정을 편집합니다.

> **Warning**
>
> 이 단계를 완료하기 전에 Amazon S3 스토리지에 대한 퍼블릭 액세스 차단을 검토하여 퍼블릭 액세스 허용과 관련된 위험을 이해하고 이에 동의하는지 확인하세요. 퍼블릭 액세스 차단 설정을 해제하여 버킷을 퍼블릭으로 만들면 인터넷상의 모든 사용자가 버킷에 액세스할 수 있습니다. 버킷에 대한 모든 퍼블릭 액세스를 차단하는 것이 좋습니다.

트래픽을 웹 사이트로 라우팅하려면

1. https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 정적 웹 사이트로 구성한 버킷의 이름을 선택합니다.
3. Permissions를 선택합니다.
4. 퍼블릭 액세스 차단(버킷 설정)(Block public access (bucket settings))에서 편집(Edit)을 선택합니다.
5. 모든 퍼블릭 액세스 차단을 선택 취소하고 변경 사항 저장을 선택합니다.

Amazon S3은 버킷에 대한 퍼블릭 액세스 차단 설정을 해제합니다. 정적 퍼블릭 웹 사이트를 생성하려면 버킷 정책을 추가하기 전에 계정에 대한 퍼블릭 액세스 차단 설정을 편집해야 할 수도 있습니다. 퍼블릭 액세스 차단에 대한 계정 설정이 현재 설정되어 있는 경우 퍼블릭 액세스 차단(버킷 설정)(Block public access (bucket settings)) 아래에 메모가 표시됩니다.

8단계: 버킷 정책 연결

Amazon S3 Block Public Access 설정을 편집한 후에는 버킷 정책을 추가하여 버킷 객체에 퍼블릭 읽기 액세스 권한을 부여할 수 있습니다. 퍼블릭 읽기 액세스 권한을 부여하면 인터넷의 모든 사용자가 버킷에 액세스할 수 있습니다.

> **Warning**
>
> 이 단계를 완료하기 전에 Amazon S3 스토리지에 대한 퍼블릭 액세스 차단을 검토하여 퍼블릭 액세스 허용과 관련된 위험을 이해하고 이에 동의하는지 확인하세요. 퍼블릭 액세스 차단 설정을 해제하여 버킷을 퍼블릭으로 만들면 인터넷상의 모든 사용자가 버킷에 액세스할 수 있습니다. 버킷에 대한 모든 퍼블릭 액세스를 차단하는 것이 좋습니다.

트래픽을 웹 사이트로 라우팅하려면

1. https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷에서 버킷의 이름을 선택합니다.
3. Permissions를 선택합니다.
4. 버킷 정책(Bucket Policy)에서 편집(Edit)을 선택합니다.
5. 다음 버킷 정책을 복사하여 텍스트 편집기에 붙여 넣습니다. 이 정책은 인터넷 상의 모든 사람에게 도메인 이름("arn:aws:s3:::*your-domain-name*/*")과 연결된 S3 버킷의 파일("Action": ["s3:GetObject"])을 가져올 수 있는 ("Principal":"*") 권한을 부여합니다.

```
{
   "Version":"2012-10-17",
   "Statement":[{
      "Sid":"AddPerm",
      "Effect":"Allow",
      "Principal":"*",
      "Action":[
         "s3:GetObject"
      ],
```

```
      "Resource":[
         "arn:aws:s3:::your-domain-name/*"
      ]
    }]
}
```

6. Resource의 값을 *your-domain-name*으로 업데이트합니다(예: **example.com**).
7. Save changes(변경 사항 저장)를 선택합니다.

9단계: 도메인 엔드포인트 테스트

퍼블릭 웹 사이트를 호스팅하도록 도메인 버킷을 구성한 후 엔드포인트를 테스트할 수 있습니다. 하위 도메인 버킷은 정적 웹 사이트 호스팅이 아닌 웹 사이트 리디렉션에 대해 설정되어 있으므로 도메인 버킷의 엔드포인트만 테스트할 수 있습니다.

> **Note**
>
> Amazon S3에서는 웹 사이트에 대한 HTTPS 액세스를 지원하지 않습니다. HTTPS를 사용하려는 경우 Amazon CloudFront를 사용하여 Amazon S3에서 호스팅되는 정적 웹 사이트를 제공할 수 있습니다.
> 자세한 내용은 뷰어와 CloudFront 간의 통신에 HTTPS 요구를 참조하세요.

1. 버킷에서 버킷의 이름을 선택합니다.
2. [속성(Properties)]을 선택합니다.
3. 페이지 하단의 정적 웹 사이트 호스팅(Static website hosting)에서 버킷 웹 사이트 엔드포인트(Bucket website endpoint)를 선택합니다.

   인덱스 문서가 별도의 브라우저 창에서 열립니다.

10단계: 도메인의 DNS 트래픽을 웹 사이트 버킷으로 라우팅

이제 S3 버킷에 1페이지짜리 웹 사이트가 생겼습니다. 도메인의 인터넷 트래픽을 S3 버킷으로 라우팅하려면 다음 절차를 수행합니다.

트래픽을 웹 사이트로 라우팅하려면

1. https://console.aws.amazon.com/route53/에서 Route 53 콘솔을 엽니다.

2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.

> **Note**
>
> 도메인을 등록할 때 Amazon Route 53가 같은 이름의 호스팅 영역을 자동으로 생성했습니다. 호스팅 영역에는 Route 53로 도메인의 트래픽을 라우팅하는 방법에 관한 정보가 포함되어 있습니다.

3. 호스팅 영역 목록에서 도메인의 이름을 선택합니다.
4. 레코드 세트 생성을 선택합니다.

> **Note**
>
> 각각의 레코드에는 하나의 도메인(예: example.com) 또는 하위 도메인(예: www.example.com)의 트래픽을 라우팅하려는 방법에 관한 정보가 포함되어 있습니다. 레코드는 도메인의 호스팅 영역에 저장됩니다.

5. 마법사로 전환을 선택합니다.
6. 단순 라우팅을 선택하고 다음을 선택합니다.
7. Define simple record(단순 레코드 정의)를 선택합니다.
8. [레코드 이름(Record name)]에서 기본값(호스팅 영역과 도메인의 이름)을 그대로 사용합니다.
9. 레코드 유형에서 A - 트래픽을 IPv4 주소 및 일부 AWS 리소스로 라우팅을 선택합니다.
10. 값/트래픽 라우팅 대상에서 Alias to S3 website endpoint(S3 웹 사이트 엔드포인트에 대한 별칭)를 선택합니다.
11. 리전을 선택합니다.
12. S3 버킷을 선택합니다.

    버킷 이름은 이름 상자에 나타나는 이름과 일치해야 합니다. S3 버킷 선택 목록에서 버킷 이름은 버킷이 생성된 리전의 Amazon S3 웹 사이트 엔드포인트와 함께 나타납니다(예: `s3-website-us-west-1.amazonaws.com (example.com)`).

    S3 버킷 선택에서는 다음 중 하나에 해당하는 경우 버킷을 나열합니다.

    - 버킷을 정적 웹 사이트로 구성한 경우
    - 버킷 이름이 생성 중인 레코드의 이름과 동일한 경우
    - 현재 AWS 계정이 버킷을 생성했습니다.

버킷이 S3 버킷 선택 목록에 나타나지 않으면 버킷이 생성된 리전의 Amazon S3 웹 사이트 엔드포인트를 입력합니다(예: **s3-website-us-west-2.amazonaws.com**). Amazon S3 웹 사이트 엔드포인트의 전체 목록은 Amazon S3 웹 사이트 엔드포인트를 참조하세요. 별칭 대상에 대한 자세한 내용은 단순 별칭 레코드에 특정한 값의 "값/트래픽 라우팅 대상" 섹션을 참조하세요.

13. 대상 상태 평가에서 아니요를 선택합니다.
14. Define simple record(단순 레코드 정의)를 선택합니다.

(선택 사항) 하위 도메인(**www.example.com**)에 대한 별칭 레코드를 추가하려면

하위 도메인에 대한 버킷을 생성한 경우 해당 버킷에 대한 별칭 레코드도 추가합니다.

1. 레코드 구성에서 단순 레코드 정의를 선택합니다.
2. 하위 도메인의 레코드 이름에 www를 입력합니다.
3. 레코드 유형에서 A - 트래픽을 IPv4 주소 및 일부 AWS 리소스로 라우팅을 선택합니다.
4. 값/트래픽 라우팅 대상에서 Alias to S3 website endpoint(S3 웹 사이트 엔드포인트에 대한 별칭)를 선택합니다.
5. 리전을 선택합니다.
6. S3 버킷을 선택합니다(예: `s3-website-us-west-2.amazonaws.com (example.com)`).

   버킷이 S3 버킷 선택 목록에 나타나지 않으면 버킷이 생성된 리전의 Amazon S3 웹 사이트 엔드포인트를 입력합니다(예: **s3-website-us-west-2.amazonaws.com**).
7. 대상 상태 평가에서 아니요를 선택합니다.
8. Define simple record(단순 레코드 정의)를 선택합니다.
9. 레코드 구성 페이지에서 레코드 생성을 선택합니다.

11단계: 웹 사이트 테스트

웹 사이트가 올바로 작동하는지 확인하려면 웹 브라우저를 열어 다음 URL로 이동합니다.

- http://*your-domain-name*(예: `example.com`) - *your-domain-name* 버킷의 인덱스 문서를 표시합니다.
- http://www.*your-domain-name*(예: `www.example.com`) - 요청을 *your-domain-name* 버킷으로 리디렉션합니다.

예상 동작을 확인하기 위해 캐시를 지워야 하는 경우도 있습니다.

인터넷 트래픽 라우팅에 대한 자세한 내용은 Amazon Route 53을 DNS 서비스로 구성 단원을 참조하십시오. 인터넷 트래픽을 AWS 리소스로 라우팅하는 방법에 대한 자세한 내용은 섹션을 참조하세요AWS 리소스로 인터넷 트래픽 라우팅.

12단계(선택 사항): Amazon CloudFront를 사용하여 콘텐츠 배포 속도 높이기

CloudFront는 .html, .css, .js 및 이미지 파일과 같은 정적 및 동적 웹 콘텐츠를 사용자에게 더 빨리 배포하도록 지원하는 웹 서비스입니다. CloudFront는 엣지 로케이션이라고 하는 데이터 센터의 전 세계 네트워크를 통해 콘텐츠를 제공합니다. CloudFront를 통해 서비스하는 콘텐츠를 사용자가 요청하면 지연 시간이 가장 낮은 엣지 로케이션으로 라우팅되므로 콘텐츠 전송 성능이 뛰어납니다.

- 콘텐츠가 이미 지연 시간이 가장 낮은 엣지 로케이션에 있는 경우 CloudFront가 콘텐츠를 즉시 제공합니다.
- 콘텐츠가 해당 엣지 로케이션에 없는 경우 CloudFront에서는 콘텐츠의 최종 버전의 출처로 식별한 Amazon S3 버킷 또는 HTTP 서버(예: 웹 서버)에서 콘텐츠를 검색합니다.

CloudFront를 사용하여 Amazon S3 버킷의 콘텐츠를 배포하는 방법에 대한 자세한 내용은 Amazon CloudFront 개발자 안내서의 Amazon S3에서 콘텐츠를 배포할 때 CloudFront 추가 섹션을 참조하세요.

Amazon CloudFront 배포를 사용하여 정적 웹 사이트 제공

이 시작하기 자습서는 다음 작업의 수행 방법을 보여줍니다.

- example.com 등의 도메인 이름 등록
- 도메인에 대한 인증서를 생성합니다.
- 2개의 Amazon S3 버킷을 만들고 하나는 웹 사이트를 호스팅하고 다른 하나는 하위 도메인으로 리디렉션하도록 구성합니다.
- 샘플 웹 사이트를 만들고 S3 버킷에 해당 파일을 저장합니다.
- 두 S3 버킷 모두에 대해 CloudFront 배포를 생성합니다.
- Amazon Route 53가 CloudFront 배포로 트래픽을 라우팅하도록 구성합니다.

완료되면 브라우저를 열고 도메인 이름을 입력하여 안전하게 웹 사이트를 볼 수 있습니다.

주제

사전 조건

시작하기 전에 먼저 Amazon Route 53 설정의 단계를 완료해야 합니다.

1단계: 도메인 등록

example.com과 같은 도메인 이름을 사용하려면 사용되고 있지 않은 도메인 이름을 찾아 등록해야 합니다. 도메인 이름을 등록하면 일반적으로 1년 동안 인터넷 어디서나 도메인 이름을 독점적으로 사용할 수 있습니다. 기본적으로 매년 말에 도메인 이름이 자동으로 갱신되지만 자동 갱신은 꺼둘 수 있습니다. 자세한 내용은 새 도메인 등록 섹션을 참조하세요.

2단계: 공인 인증서 요청

뷰어가 HTTPS를 사용할 것을 요청하도록 CloudFront를 구성하려면 Amazon CloudFront 배포에서 공인 인증서를 요구하므로 CloudFront가 뷰어와 통신할 때 연결이 암호화됩니다.

AWS Certificate Manager(ACM) 퍼블릭 인증서를 요청하려면(콘솔)

1. AWS Management Console에 로그인하고 https://console.aws.amazon.com/acm/home ACM 콘솔을 엽니다.

> **Note**
>
> 미국 동부(버지니아 북부) 리전에서 인증서를 생성하는지 확인합니다 Amazon CloudFront에서 이 정보가 필요합니다.

왼쪽 탐색 창에서 인증서 요청을 선택하고 인증서 요청 페이지에서 공인 인증서 요청, 다음을 차례로 선택합니다.

2. 도메인 이름 섹션에 도메인(예:**example.com**)을 입력합니다.

   이 인증서에 다른 이름 추가를 선택하고 도메인 이름 앞에 별표를 입력하여 모든 하위 도메인(예: ***.example.com**)에 대한 와일드카드 인증서를 요청합니다.

3. 검증 방법 선택 섹션에서 DNS 검증을 선택합니다.
4. 키 알고리즘 섹션에서 RSA 2048을 선택합니다.
5. 태그 추가 섹션에서 선택 사항으로 인증서에 태그를 지정할 수 있습니다. 태그는 AWS 리소스를 식별하고 구성하기 위한 메타데이터 역할을 하는 키-값 페어입니다.

   요청을 선택하면 인증서 페이지로 이동합니다.

6. 새 인증서가 보류 중 상태로 표시되면 인증서 ID를 선택하고 인증서 세부 정보 페이지에서 Route 53에서 레코드 생성을 선택하여 도메인에 대한 CNAME 레코드를 자동으로 추가한 다음 레코드 생성을 선택합니다.

   인증서 상태(Certificate status) 페이지가 DNS 레코드가 생성됨(Successfully created DNS records)이라고 표시되는 상태 배너와 함께 열립니다.

   새 인증서의 상태가 최대 30분 동안 계속 검증 보류 중(Pending validation)으로 표시될 수 있습니다.

3단계: S3 버킷 생성하여 하위 도메인 호스팅

www.your-domain-name에 대한 S3 버킷을 생성하려면

Amazon S3를 사용하면 어디서든 인터넷에 데이터를 저장하고 조회할 수 있습니다. 이 단계에서는 S3 버킷을 생성하여 웹 사이트의 모든 파일을 저장합니다.

1. https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.

2. 버킷 만들기를 선택합니다.
3. 다음 값을 입력합니다.

   버킷 이름

   www.***your-domain-name***을 입력합니다. 예를 들어 도메인 이름 example.com을 등록한 경우, www.example.com을 입력합니다.

   리전

   버킷에 대한 리전을 선택합니다.
4. 기본 설정을 적용하고 버킷을 생성하려면 버킷 생성을 선택합니다.

   S3 버킷 설정에 대한 자세한 내용은 Amazon S3 사용 설명서의 버킷 속성 보기 섹션을 참조하세요.

4단계: 루트 도메인에 대한 다른 S3 버킷 생성

사용자들이 example.com 같은 *your-domain-name* 루트 도메인을 사용하여 샘플 웹 사이트에 액세스할 수 있도록 하려면 두 번째 S3 버킷을 생성합니다. 이 자습서에서는 두 번째 버킷(루트 도메인)을 구성하여 첫 번째 버킷으로 트래픽을 라우팅합니다.

your-domain-name에 대한 S3 버킷을 생성하려면

1. https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 만들기를 선택합니다.
3. 다음 값을 입력합니다.

   버킷 이름

   your-domain-name을 입력합니다. 예를 들어 도메인 이름 example.com을 등록한 경우, example.com을 입력합니다.

   리전

   첫 번째 버킷을 생성한 리전과 동일한 리전을 선택합니다.
4. 기본 설정을 적용하고 버킷을 생성하려면 버킷 생성을 선택합니다.

5단계: 하위 도메인 버킷에 웹 사이트 파일 업로드

이제 S3 버킷이 생겼으므로 웹 사이트 파일을 업로드할 수 있습니다. 이 자습서에서는 페이지에 텍스트를 표시하는 간단한 index.html 파일을 업로드합니다.

웹 사이트 호스팅에 대한 S3 버킷을 사용하려면

1. https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 목록에서 웹 사이트 파일(예: **www.example.com**)을 업로드하려는 버킷의 연결된 이름을 선택합니다.
3. 한 페이지의 간단한 웹 사이트를 만드는 예제 텍스트를 복사하여 텍스트 편집기에 붙여넣은 다음 해당 텍스트를 index.html로 저장합니다.

```
<html>
<head>
<title>Amazon Route 53 Getting Started</title>
</head>

<body>

<h1>Routing Internet traffic to Cloudfront distributions for your website stored in
 an S3 bucket</h1>

<p>For more information, see
<a href="https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/getting-
started.html">Getting Started with Amazon Route 53</a>
in the <emphasis>Amazon Route 53 Developer Guide</emphasis>.</p>

</body>

</html>
```

4. 객체(Objects) 탭에서 업로드(Upload)를 선택합니다.
5. 파일 및 폴더(Files and folders)에서 파일 추가(Add files)를 선택하고 웹 사이트 파일을 업로드합니다. 이 자습서에서는 이 절차의 3단계에서 저장한 index.html 파일을 업로드합니다.

6단계: 웹 사이트 호스팅에 대한 루트 도메인 버킷 설정

웹 사이트 호스팅용 루트 도메인 버킷을 구성하면 루트 도메인 버킷을 선택적으로 구성하여 모든 요청을 하위 도메인으로 리디렉션할 수 있습니다. 예를 들어, 모든 요청을 구성하여 `example.com`이 `www.example.com`으로 리디렉션되게 할 수 있습니다.

리디렉션을 구성하려면

1. Amazon S3 콘솔의 버킷(Buckets) 목록에서 버킷 이름(예: `example.com`)을 선택합니다.
2. [속성(Properties)]을 선택합니다.
3. 정적 웹 사이트 호스팅(Static website hosting)에서 편집(Edit)을 선택합니다.
4. 정적 웹 사이트 호스팅(Static website hosting)에서 활성화(Enable)를 선택합니다.
5. 객체에 대한 요청 리디렉션(Redirect requests for an object)을 선택합니다.
6. 호스트 이름(Host name)상자에 하위 도메인(예: **`www.example.com`**)을 입력합니다.
7. 프로토콜에서 HTTPS를 선택합니다.
8. Save changes(변경 사항 저장)를 선택합니다.
9. 정적 웹 사이트 호스팅에서 엔드포인트를 기록합니다.

   엔드포인트는 버킷의 Amazon S3 웹 사이트 엔드포인트입니다. 이 엔드포인트를 사용하여 Amazon CloudFront 배포를 설정합니다.

7단계: 하위 도메인에 대한 Amazon CloudFront 배포 생성

이 단계에서는 사용자가 안전하게 볼 수 있도록 웹 사이트에서 HTTPS를 사용할 수 있도록 www.example.com과 같은 하위 도메인에 대한 CloudFront 배포를 생성합니다.

CloudFront 배포 생성

1. https://console.aws.amazon.com/cloudfront/v4/home에서 CloudFront 콘솔을 엽니다.
2. 배포 생성(Create Distribution)을 선택합니다.
3. 원본 도메인에 대한 원본에서 이전에 생성한 Amazon S3 버킷을 선택합니다. 형식은 **`www.example.com.s3.<Region>.amazonaws.com`**와 비슷합니다.

   원본 액세스에서 레거시 액세스 ID를 선택합니다. 오리진 액세스 ID(Origin access identity)의 경우 목록에서 선택하거나 새 OAI 생성(Create new OAI)을 선택할 수 있습니다(둘 다 작동함).

버킷 정책(Bucket policy)에서 예, 버킷 정책을 업데이트합니다(Yes, update the bucket policy)를 선택합니다.

4. 기본 캐시 동작 설정(Default Cache Behavior Settings)의 경우 뷰어(Viewer)에서 뷰어 프로토콜 정책(Viewer protocol policy)을 HTTP에서 HTTPS로 리디렉션(Redirect HTTP to HTTPS)으로 설정하고 나머지에 대해서는 기본값을 수락합니다.

   캐시 동작 옵션에 대한 자세한 내용은 Amazon CloudFront 개발자 안내서의 캐시 동작 설정을 참조하세요.

5. 웹 애플리케이션 방화벽(WAF) 섹션에서 AWS WAF 보안 보호를 활성화하거나 비활성화하도록 선택할 수 있습니다.

6. 설정(Settings) 아래의 필드에서 다음을 수행합니다.

   - 대체 도메인 이름(CNAME) - 선택 사항에 대해 항목 추가(Add item)를 선택하고 하위 도메인(예: **`www.example.com`**)을 입력합니다.
   - 사용자 정의 SSL 인증서(Custom SSL Certificate)에서 이전에 생성한 인증서를 선택합니다.
   - 기본 루트 객체(Default root object) 텍스트 상자에 **`index.html`**을 입력합니다.
   - 나머지는 기본값을 그대로 사용하고 배포 생성을 선택합니다.

     배포 옵션에 대한 자세한 내용은 배포 설정을 참조하세요.

7. CloudFront에서 배포를 생성하면 배포의 상태(Status) 열 값이 진행 중에(In Progress)서 배포 완료(Deployed)로 변경됩니다. 이 작업은 일반적으로 몇 분 정도 걸립니다.

   CloudFront가 배포에 할당하는 도메인 이름을 기록합니다. 이 도메인 이름은 배포 목록에 나타납니다. 이 도메인 이름을 사용하여 배포를 테스트할 수 있습니다.

8단계: 루트 도메인에 대한 Amazon CloudFront 배포 생성

이 단계에서는 URL이 하위 도메인으로 리디렉션될 때 HTTPS를 사용할 수 있도록 루트 도메인에 대한 CloudFront 배포를 생성합니다.

CloudFront 배포 생성

1. https://console.aws.amazon.com/cloudfront/v4/home에서 CloudFront 콘솔을 엽니다.
2. 배포 생성(Create Distribution)을 선택합니다.

3. 오리진 설정(Origin Settings)에서 오리진 도메인 이름(Origin Domain Name)에 버킷 웹 사이트 엔드포인트를 입력합니다. 이전에 생성한 Amazon S3 버킷에 대한 속성(Properties)의 정적 웹 사이트 호스팅(Static website hosting) 섹션에서 이를 가져올 수 있습니다.

   나머지에 대해서는 기본값을 수락합니다.
4. 웹 애플리케이션 방화벽(WAF) 섹션에서 AWS WAF 보안 보호를 활성화하거나 비활성화하도록 선택할 수 있습니다.
5. 캐시 키 및 오리진 요청 아래의 필드에서 캐시 정책 및 오리진 요청 정책(권장)을 선택하고 캐시 정책 드롭다운에서 CachingDisabled를 선택합니다.

   나머지에 대해서는 기본값을 수락합니다.

   캐시 동작 옵션에 대한 자세한 내용은 Amazon CloudFront 개발자 안내서의 캐시 동작 설정을 참조하세요.
6. 설정(Settings) 아래의 필드에서 다음을 수행합니다.

   - 대체 도메인 이름(CNAME) - 선택 사항에 대해 항목 추가를 선택하고 루트 도메인(예: **`example.com`**)을 입력합니다.
   - 사용자 정의 SSL 인증서(Custom SSL Certificate)에서 이전에 생성한 인증서를 선택합니다.
   - 나머지에 대해서는 기본값을 수락합니다.

   배포 옵션에 대한 자세한 내용은 배포 설정을 참조하세요.
7. 페이지 맨 아래에서 배포 생성(Create Distribution)을 선택합니다.
8. CloudFront에서 배포를 생성하면 배포의 상태(Status) 열 값이 진행 중에(In Progress)서 배포 완료(Deployed)로 변경됩니다. 이 작업은 일반적으로 몇 분 정도 걸립니다.

   CloudFront가 배포에 할당하는 도메인 이름을 기록합니다. 이 도메인 이름은 배포 목록에 나타납니다. 이 도메인 이름을 사용하여 배포를 테스트할 수 있습니다.

9단계: 도메인에 대한 DNS 트래픽을 CloudFront 배포로 라우팅

이제 S3 버킷에 CloudFront 배포를 사용하는 1페이지의 웹 사이트가 생겼습니다. 도메인의 인터넷 트래픽을 CloudFront 배포로 라우팅하려면 다음 절차를 수행합니다.

트래픽을 CloudFront 배포로 라우팅하는 방법에 대한 자세한 내용은 도메인 이름을 사용하여 Amazon CloudFront 배포로 트래픽 라우팅 섹션을 참조하세요.

트래픽을 웹 사이트로 라우팅하려면

1. https://console.aws.amazon.com/route53/에서 Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.

   > **Note**
   >
   > 도메인을 등록할 때 Amazon Route 53가 같은 이름의 호스팅 영역을 자동으로 생성했습니다. 호스팅 영역에는 Route 53로 도메인의 트래픽을 라우팅하는 방법에 관한 정보가 포함되어 있습니다.

3. 호스팅 영역 목록에서 도메인의 이름을 선택합니다.
4. 레코드 세트 생성을 선택합니다.

   빠른 레코드 생성()Quick create record) 보기에 있는 경우 마법사로 전환(Switch to wizard)을 선택합니다.

   > **Note**
   >
   > 각각의 레코드에는 하나의 도메인(예: example.com) 또는 그 하위 도메인(예: www.example.com)의 트래픽을 라우팅하려는 방법에 관한 정보가 포함되어 있습니다. 레코드는 도메인의 호스팅 영역에 저장됩니다.

5. 단순 라우팅(Simple routing)을 선택하고 다음(Next)을 선택합니다.
6. Define simple record(단순 레코드 정의)를 선택합니다.
7. 레코드 이름에 기본값(호스팅 영역과 도메인의 이름) 앞의 **www**를 입력합니다.
8. 레코드 유형에서 A - 트래픽을 IPv4 주소 및 일부 AWS 리소스로 라우팅을 선택합니다.
9. 값/트래픽 라우팅 대상(Value/Route traffic to)에서 CloudFront 배포에 대한 별칭(Alias to CloudFront distribution)을 선택합니다.
10. 배포를 선택합니다.

    배포 이름은 배포(Distributions) 목록의 도메인 이름(Domain name) 상자에 표시되는 이름과 일치해야 합니다(예: `dddjjjkkk.cloudfront.net`).

11. 대상 상태 평가에서 아니요를 선택합니다.
12. Define simple record(단순 레코드 정의)를 선택합니다.

루트 도메인(**example.com**)에 대한 별칭 레코드 추가

루트 도메인에 대한 별칭 레코드도 추가하여 트래픽을 www.example.com으로 리디렉션하는 S3 버킷을 가리킵니다. 트래픽을 CloudFront 배포로 라우팅하는 방법에 대한 자세한 내용은 도메인 이름을 사용하여 Amazon CloudFront 배포로 트래픽 라우팅 섹션을 참조하세요.

1. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
2. 호스팅 영역 목록에서 도메인의 이름을 선택합니다.
3. 레코드 세트 생성을 선택합니다.

   빠른 레코드 생성()Quick create record) 보기에 있는 경우 마법사로 전환(Switch to wizard)을 선택합니다.

   > **Note**
   >
   > 각각의 레코드에는 하나의 도메인(예: example.com) 또는 그 하위 도메인(예: www.example.com)의 트래픽을 라우팅하려는 방법에 관한 정보가 포함되어 있습니다. 레코드는 도메인의 호스팅 영역에 저장됩니다.

4. 단순 라우팅(Simple routing)을 선택하고 다음(Next)을 선택합니다.
5. Define simple record(단순 레코드 정의)를 선택합니다.
6. 레코드 이름(Record name)에서 기본값을 수락합니다.
7. 레코드 유형에서 A - 트래픽을 IPv4 주소 및 일부 AWS 리소스로 라우팅을 선택합니다.
8. 값/트래픽 라우팅 대상(Value/Route traffic to)에서 CloudFront 배포에 대한 별칭(Alias to CloudFront distribution)을 선택합니다.
9. 배포를 선택합니다.

   배포 이름은 배포(Distributions) 목록의 도메인 이름(Domain name) 상자에 표시되는 이름과 일치해야 합니다(예: dddjjjkkk.cloudfront.net).
10. 대상 상태 평가에서 아니요를 선택합니다.
11. Define simple record(단순 레코드 정의)를 선택합니다.
12. 레코드 구성 페이지에서 레코드 생성을 선택합니다.

10단계: 웹 사이트 테스트

웹 사이트가 올바로 작동하는지 확인하려면 웹 브라우저를 열어 다음 URL로 이동합니다.

- http://www.*your-domain-name*(예: `www.example.com`) - *your-domain-name* 버킷의 인덱스 문서를 표시합니다.
- http://*your-domain-name*(예: `example.com`) - 요청을 *www.your-domain-name* 버킷으로 리디렉션합니다.

예상 동작을 확인하기 위해 캐시를 지워야 하는 경우도 있습니다.

인터넷 트래픽 라우팅에 대한 자세한 내용은 Amazon Route 53을 DNS 서비스로 구성 단원을 참조하십시오. 인터넷 트래픽을 AWS 리소스로 라우팅하는 방법에 대한 자세한 내용은 섹션을 참조하세요AWS 리소스로 인터넷 트래픽 라우팅.

다른 서비스와의 통합

Amazon Route 53를 다른 AWS 서비스와 통합하여 Route 53 API로 전송된 요청을 로깅하고, 리소스 상태를 모니터링하고, 리소스에 태그를 할당할 수 있습니다. 또한 Route 53를 사용하여 AWS 리소스로 인터넷 트래픽을 라우팅할 수 있습니다.

주제

로깅, 모니터링, 태그 지정

AWS CloudTrail

Amazon Route 53는 AWS 계정 AWS CloudTrail에서 Route 53 API로 전송되는 모든 요청에 대한 정보를 캡처하는 서비스인와 통합됩니다. CloudTrail 로그 파일의 정보를 사용하여 Route 53에 대해 생성된 요청, 각 요청이 생성된 소스 IP 주소, 요청을 생성한 사람, 요청 생성 시기 등을 확인할 수 있습니다.

자세한 내용은 를 사용하여 Amazon Route 53 API 호출 로깅 AWS CloudTrail 단원을 참조하십시오.

Amazon CloudWatch

Amazon CloudWatch를 사용하여 Route 53 상태 확인의 상태(정상 또는 비정상)를 모니터링할 수 있습니다. 상태 확인은 웹 애플리케이션, 웹 서버, 기타 리소스의 상태와 성능을 모니터링합니다. Route 53는 지정한 간격에 따라 규칙적으로 인터넷을 통해 애플리케이션, 서버 또는 다른 리소스로 자동화된 요청을 제출하여 연결 및 사용이 가능하고 정상적으로 작동되는지 확인합니다.

자세한 내용은 CloudWatch를 이용한 상태 확인 모니터링 단원을 참조하십시오.

태그 편집기

태그는 Route 53 도메인, 호스팅 영역 및 상태 확인을 포함하여 AWS 리소스에 할당하는 레이블입니다. 각 태그는 사용자가 정의하는 키와 값으로 구성됩니다. 예를 들어, "Customer" 키와 "Example Corp." 값이 있는 도메인 등록에 태그를 할당할 수 있습니다. 다양한 용도로 태그를 사용할 수 있습니다. 한 가지 일반적인 용도는 AWS 비용을 분류하고 추적하는 것입니다.

자세한 내용은 Amazon Route 53 리소스 태그 지정 단원을 참조하십시오.

트래픽을 다른 AWS 리소스로 라우팅

Amazon Route 53를 사용하여 트래픽을 다양한 AWS 리소스로 라우팅할 수 있습니다.

Amazon API Gateway

Amazon API Gateway를 사용하면 모든 규모에서 API를 생성, 게시, 유지 관리, 모니터링, 보호할 수 있습니다. 또는 기타 웹 서비스에 액세스하는 AWS APIs와 AWS 클라우드에 저장된 데이터를 생성할 수 있습니다.

Route 53를 사용하여 API 게이트웨이 API로 트래픽을 라우팅할 수 있습니다. 자세한 내용은 도메인 이름을 사용하여 Amazon API Gateway API로 트래픽 라우팅 단원을 참조하십시오.

Amazon CloudFront

웹 콘텐츠 전송 속도를 높이려면 AWS 콘텐츠 전송 네트워크(CDN)인 Amazon CloudFront를 사용하면 됩니다. CloudFront에서는 엣지 로케이션의 글로벌 네트워크를 통해 동적, 정적, 스트리밍 및 대화형 콘텐츠를 포함하는 전체 웹 사이트를 전송할 수 있습니다. CloudFront에서는 콘텐츠에 대한 요청을 지연 시간이 가장 낮은 엣지 로케이션으로 라우팅됩니다. Route 53를 사용하여 도메인의 트래픽을 CloudFront 배포로 라우팅할 수 있습니다. 자세한 내용은 도메인 이름을 사용하여 Amazon CloudFront 배포로 트래픽 라우팅 단원을 참조하십시오.

Amazon EC2

Amazon EC2는 AWS 클라우드에서 확장 가능한 컴퓨팅 용량을 제공합니다. 사전 구성된 템플릿(Amazon Machine Image(AMI))를 사용하여 EC2 가상 컴퓨팅 환경(인스턴스)을 시작할 수 있습니다. EC2 인스턴스를 시작하면 EC2가 운영 체제(Linux 또는 Microsoft Windows) 및 AMI에 포함된 추가 소프트웨어(예: 웹 서버 또는 데이터베이스 소프트웨어)를 자동으로 설치합니다.

웹 사이트를 호스팅하거나 EC2 인스턴스에서 웹 애플리케이션을 실행하는 경우, Route 53를 사용하여 example.com과 같은 도메인에 대한 트래픽을 서버로 라우팅할 수 있습니다. 자세한 내용은 Amazon EC2 인스턴스로 트래픽 라우팅 단원을 참조하십시오.

AWS Elastic Beanstalk

AWS Elastic Beanstalk 를 사용하여 AWS 클라우드에서 애플리케이션을 배포하고 관리하는 경우 Route 53을 사용하여 example.com 같은 도메인의 DNS 트래픽을 Elastic Beanstalk 환경으로 라우팅할 수 있습니다. 자세한 내용은 AWS Elastic Beanstalk 환경으로 트래픽 라우팅 단원을 참조하십시오.

Elastic Load Balancing

여러 Amazon EC2 인스턴스에서 하나의 웹 사이트를 호스팅하는 경우 Elastic Load Balancing(ELB) 로드 밸런서를 사용하여 웹 사이트에 대한 트래픽을 인스턴스 간에 분산할 수 있습니다. 웹 사이트에 대한 트래픽이 시간에 따라 변화하므로 ELB 서비스가 로드 밸런서를 자동으로 확장합니다. 또한 로드 밸런서를 통해 등록된 인스턴스의 상태를 모니터링하고 상태가 양호한 인스턴스로만 도메인 트래픽을 라우팅할 수 있습니다.

Route 53를 사용하여 도메인의 트래픽을 Classic, 애플리케이션 또는 Network Load Balancer로 라우팅할 수 있습니다. 자세한 내용은 ELB 로드 밸런서로 트래픽 라우팅 단원을 참조하십시오.

Amazon Lightsail

Amazon Lightsail은 저렴하고 예측 가능한 월별 요금을 이용할 수 있도록 클라우드에서 웹 사이트, 웹 애플리케이션 및 데이터베이스를 배포하고 관리하는 기능과 컴퓨팅, 스토리지 및 네트워킹 용량을 제공합니다.

Lightsail을 사용하는 경우, Route 53를 사용하여 Lightsail 인스턴스로 트래픽을 라우팅할 수 있습니다. 자세한 내용은 Route 53를 사용하여 도메인을 Amazon Lightsail 인스턴스로 지정을 참조하세요.

Amazon S3

Amazon Simple Storage Service(Amazon S3)는 안전하고 내구성과 확장성이 뛰어난 클라우드 스토리지를 제공합니다. 웹 페이지 및 클라이언트 측 스크립트를 포함할 수 있는 정적 웹 사이트를 호스팅하도록 S3 버킷을 구성할 수 있습니다. S3은 서버 측 스크립팅을 지원하지 않습니다. Route 53를 사용하여 트래픽을 Amazon S3 버킷으로 라우팅할 수 있습니다. 자세한 정보는 다음의 주제를 참조하세요.

- 버킷으로의 트래픽 라우팅에 대한 자세한 내용은 Amazon S3 버킷에서 호스팅하는 웹 사이트로 트래픽 라우팅을 참조하십시오.
- S3 버킷에서 정적 웹 사이트를 호스팅하는 방법에 대한 자세한 설명은 Amazon Route 53 시작하기 단원을 참조하십시오.

Amazon Virtual Private Cloud(VPC)

인터페이스 엔드포인트를 사용하면 AWS PrivateLink로 구동되는 서비스에 연결할 수 있습니다. 이러한 서비스에는 일부 AWS 서비스, 자체 VPCs에서 다른 AWS 고객 및 파트너가 호스팅하는 서비스(엔드포인트 서비스라고 함), 지원되는 AWS Marketplace 파트너 서비스가 포함됩니다.

Route 53를 사용하여 트래픽을 인터페이스 엔드포인트로 라우팅할 수 있습니다. 자세한 내용은 도메인 이름을 사용하여 Amazon Virtual Private Cloud 인터페이스 엔드포인트로 트래픽 라우팅 단원을 참조하십시오.

Amazon WorkMail

기업 이메일로 Amazon WorkMail을 사용하고 DNS 서비스로 Route 53를 사용하는 경우, Route 53를 사용하여 Amazon WorkMail 이메일 도메인으로 트래픽을 라우팅할 수 있습니다. 자세한 내용은 Amazon WorkMail로 트래픽 라우팅 단원을 참조하십시오.

자세한 내용은 AWS 리소스로 인터넷 트래픽 라우팅 섹션을 참조하세요.

DNS 도메인 이름 형식

도메인 이름(도메인, 호스팅 영역 및 레코드 이름 등)은 점으로 구분되는 일련의 레이블로 구성됩니다. 각 레이블의 길이는 최대 63바이트입니다. 도메인 이름의 총 길이는 점을 포함하여 255바이트를 초과할 수 없습니다. Amazon Route 53는 모든 유효한 도메인 이름을 지원합니다.

명명 요구 사항은 도메인 이름 등록 여부나 호스팅 영역 또는 레코드 이름 지정 여부에 따라 다릅니다. 해당 주제를 참조하십시오.

주제

도메인 이름 등록 시 도메인 이름 형식

도메인 이름 등록 시 도메인 이름은 a-z, 0-9 및 -(하이픈)만 사용 가능합니다. 레이블 시작 또는 끝에 하이픈을 지정할 수 없습니다.

다국어 도메인 이름(IDN)을 등록하는 방법에 대한 자세한 내용은 다국어 도메인 이름 형식 단원을 참조하십시오.

호스팅 영역 및 레코드에 대한 도메인 이름 형식

호스팅 영역 및 레코드에 대한 도메인 이름에는 다음과 같은 인쇄 가능한 ASCII 문자(공백 제외)를 사용할 수 있습니다.

- a-z
- 0~9
- - (하이픈)
- ! " # $ % & ' ( ) * + , - / : ; < = > ? @ [\ ] ^ _ ` { | } ~ .

Amazon Route 53는 영문자를 대문자, 소문자 또는 이스케이프 코드의 해당 문자 중 어떻게 지정하는지 관계없이 소문자(a-z)로 저장합니다.

도메인 이름에 다음 문자가 포함되어 있는 경우, *\three-digit octal code* 형식의 이스케이프 코드를 사용하여 문자를 지정해야 합니다.

- 000 - 040 사이의 8진수 문자(0 - 32 사이의 10진수, 0x00 - 0x20 사이의 16진수)
- 177 - 377 사이의 8진수 문자(127 - 255 사이의 10진수, 0x7F - 0xFF 사이의 16진수)
- .(마침표), 056 8진수 문자(46 10진수, 0x2E 16진수), 도메인 이름에서 문자로 사용하는 경우. 구분 기호로 .를 사용하는 경우, 이스케이프 코드를 사용하지 않아도 됩니다.

도메인 이름에 a~z, 0~9, -(하이픈) 또는 _(밑줄) 이외의 문자가 포함되어 있는 경우, Route 53 API 작업에서 이스케이프 코드로 해당 문자를 반환합니다. 엔터티를 생성할 때 해당 문자를 문자로 지정하든 이스케이프 코드로 지정하든 마찬가지입니다. Route 53 콘솔에는 그러한 문자가 이스케이프 코드가 아닌 문자로 표시됩니다.

ASCII 문자 및 해당하는 8진수 코드 목록을 보려면 인터넷에서 "ascii table"을 검색하십시오.

다국어 도메인 이름(IDN)을 지정하려면 해당 이름을 퓨니코드로 변환합니다. 자세한 내용은 다국어 도메인 이름 형식 단원을 참조하십시오.

호스팅 영역 및 레코드의 이름에 별표(*) 사용

이름에 *를 포함하는 호스팅 영역 및 기록을 생성할 수 있습니다.

호스팅 영역

- 도메인 이름의 맨 왼쪽 라벨에 *를 포함할 수 없습니다. 예를 들어 *.example.com은 허용되지 않습니다.
- 다른 위치에 *를 포함시키면 DNS가 이를 와일드카드가 아닌 * 문자(ASCII 42)로 처리합니다.

레코드

DNS는 이름에 표시되는 위치에 따라 * 문자를 와일드카드 또는 * 문자(ASCII 42)로 처리합니다. 레코드의 이름에 *를 와일드카드로 사용할 때의 다음 제한 사항에 유의하십시오.

- * 는 도메인 이름에서 제일 왼쪽 라벨을 바꿔야 합니다(예: *.example.com 또는 *.acme.example.com). 다른 위치에 *를 포함시키면(예: prod.*.example.com) DNS가 이를 와일드카드가 아닌 * 문자(ASCII 42)로 처리합니다.
- *이 전체 라벨을 대신해야 합니다. 예를 들어, *prod.example.com 또는 prod*.example.com을 지정할 수 없습니다.

- 구체적인 도메인 이름이 우선순위입니다. 예를 들어, *.example.com 및 acme.example.com 기록을 생성한다면 Route 53는 acme.example.com 기록 값의 acme.example.com DNS 쿼리에 항상 반응합니다.
- *는 별표 및 해당 하위 도메인의 모든 하위 도메인을 비롯한 하위 도메인 수준의 DNS 쿼리에 적용됩니다. 예를 들어 *.example.com이라는 레코드를 생성하는 경우, Route 53은(호스팅 영역에 어떤 유형의 레코드도 없다면) 이 레코드 값을 사용하여 zenith.example.com, acme.zenith.example.com, 및 pinnacle.acme.zenith.example.com에 대한 DNS 쿼리에 응답합니다.

  *.example.com이라는 레코드를 생성했는데 example.com 레코드가 없는 경우 Route 53는 NXDOMAIN(존재하지 않는 도메인)을 통해 example.com DNS 쿼리에 응답합니다.
- Route 53를 구성하여 동일한 수준의 모든 하위 도메인 및 도메인 이름에 따라 DNS 쿼리에 동일한 응답을 반환할 수 있습니다. 예를 들어, Route 53를 구성하고 example.com 레코드를 사용하여 acme.example.com 및 zenith.example.com과 같은 DNS 쿼리에 응답할 수 있습니다. 다음 단계를 수행합니다.

  1. 도메인의 레코드(예: example.com)를 생성합니다.
  2. 하위 도메인의 별칭 레코드(예: *.example.com)를 생성합니다. 1단계에서 생성한 기록을 별칭 기록 대상으로 지정합니다.
- 유형이 NS인 레코드에 *를 와일드카드로 사용할 수 없습니다.

다국어 도메인 이름 형식

새 도메인 이름을 등록하거나 호스팅 영역 및 레코드를 생성할 때, a-z 이외의 문자(예: 프랑스어의 ç), 기타 알파벳 문자(예: 키릴 자모, 아랍어), 중국어, 일본어 또는 한국어 문자를 지정할 수 있습니다. Amazon Route 53는 이러한 다국어 도메인 이름(IDN)을 퓨니코드로 저장합니다. 그럼 퓨니코드는 유니코드 문자를 ASCII 문자열로 나타냅니다.

도메인 이름을 등록하는 경우 다음 사항에 유의하십시오.

- 최상위 도메인(TLD)이 IDN을 지원하고 사용하려는 언어를 지원하는 경우에만 a-z, 0-9 및 -(하이픈) 이외의 문자를 사용할 수 있습니다. TLD에서 지원하는 언어를 확인하려면 Amazon Route 53에 등록할 수 있는 도메인 단원을 참조하십시오.
- 이름에 a-z 문자만 포함된 경우 지원되지 않는 언어로 이름을 지정할 수 있습니다. 예를 들어 TLD는 프랑스어를 지원하지 않지만 사용하려는 이름에 분음 부호 없이 a-z 문자만 포함되는 경우, 해당 이름을 계속 사용할 수 있습니다. 이 예에서는 “c”를 포함하는 이름은 허용되고 “ç"을 포함하는 이름은 허용되지 않습니다.

- TLD에서 IDN을 지원하지 않거나 도메인 이름에 사용하려는 언어를 지원하지 않는 경우, 퓨니코드에 a-z, 0-9 및 -만 포함되어 있더라도 이름을 퓨니코드로 지정할 수 없습니다.

다음 예는 다국어 도메인 이름 中国.asia를 퓨니코드로 나타낸 것을 보여줍니다.

```
xn--fiqs8s.asia
```

최신 브라우저의 주소 표시줄에 IDN을 입력하면, DNS 쿼리를 제출하거나 HTTP 요청을 수행하기 전에 브라우저에서 이를 퓨니코드로 변환합니다.

IDN을 입력하는 방식은 생성 항목(도메인 이름, 호스팅 영역 또는 레코드)과 해당 항목의 생성 방식(API, SDK 또는 Route 53 콘솔)에 따라 다릅니다.

- Route 53 API 또는 AWS SDKs 중 하나를 사용하는 경우 프로그래밍 방식으로 유니코드 값을 Punycode로 변환할 수 있습니다. 예를 들어, Java를 사용하는 경우 java.net.IDN 라이브러리의 [toASCII] 방식을 사용하여 유니코드 값을 퓨니코드로 변환할 수 있습니다.
- Route 53 콘솔을 사용하여 도메인 이름을 등록하는 경우, 유니코드 문자를 포함한 이름을 이름 필드에 붙여넣을 수 있으며, 콘솔에서 이를 저장하기 전에 퓨니코드로 이 값을 변환합니다.
- Route 53 콘솔을 사용하여 호스팅 영역 또는 레코드를 생성하는 경우, 해당하는 이름 필드에 이름을 입력하기 전에 퓨니코드로 도메인 이름을 변환해야 합니다. 온라인 변환기에 대한 자세한 내용은 인터넷에서 "punycode converter"를 검색하세요.

도메인 이름을 등록하는 경우, 모든 최상위 도메인(TLD)에서 IDN을 지원하지는 않는다는 점을 참고하십시오. Route 53에서 지원하는 TLD 목록은 Amazon Route 53에 등록할 수 있는 도메인 섹션을 참조하세요. IDN을 지원하지 않는 TLD가 나와 있습니다.

Amazon Route 53를 사용하여 도메인 등록 및 관리

http://example.com이라는 URL의 일부인 example.com과 같은 새 도메인 이름을 갖고 싶을 때 Amazon Route 53에 그 이름을 등록할 수 있습니다. 또한 기존 도메인에 대한 등록을 다른 등록 기관으로부터 Route 53으로 이전하거나 Route 53에 등록하는 도메인들에 대한 등록을 다른 등록 기관에게 이전할 수도 있습니다.

이 장의 절차들은 Route 53 콘솔을 이용해 도메인을 등록하고 이전하는 방법, 그리고 도메인 설정을 편집하고 도메인의 상태를 보는 방법을 설명합니다. 도메인을 몇 개만 등록해 관리하고 있다면, 콘솔을 사용하는 것이 가장 손쉬운 방법입니다.

다수의 도메인을 등록하고 관리할 필요가 있다면 프로그래밍 방식으로 변경하는 것이 좋습니다. 자세한 내용은 Amazon Route 53 설정 단원을 참조하십시오.

> **Note**
>
> AWS SDK가 있는 언어를 사용하는 경우 APIs를 통해 작업하려고 하지 말고 SDK를 사용하세요. SDK를 사용하면 인증을 더 간단하게 만들고, 개발 환경에 쉽게 통합할 수 있으며, Route 53 명령에 쉽게 액세스할 수 있습니다.

도메인 이름 등록 서비스는 Amazon의 도메인 이름 등록 계약이 적용됩니다.

주제

- 도메인 등록 문제에 대한 AWS 지원 문의
- 도메인 결제 보고서 다운로드
- Amazon Route 53에 등록할 수 있는 도메인

새 도메인 등록

이 섹션에서는 Amazon Route 53에 새 도메인 등록과 관련된 다음 주제를 다룹니다.

1. 새 도메인 등록:
   - Route 53 콘솔을 사용하여 새 도메인을 등록하는 단계별 절차를 알아봅니다.
   - 문제, 요금, 지원되는 최상위 도메인(TLDs) 및 자동 호스팅 영역 생성에 대해 AWS Support에 문의하는 등 도메인 등록을 위한 고려 사항 및 사전 조건을 이해합니다.
2. 도메인을 등록하거나 이전할 때 지정하는 값:
   - 연락처 정보, 개인 정보 보호 설정, 자동 갱신 옵션을 포함하여 도메인을 등록하거나 전송할 때 제공해야 하는 값을 알아봅니다.
   - 도메인 소유자 또는 등록자 이메일 주소와 같은 특정 값을 변경할 경우의 영향을 이해합니다.
3. 도메인을 등록할 때 Amazon Route 53가 반환하는 값:
   - 등록 날짜, 만료 날짜, 도메인 상태 코드, 전송 잠금 상태, 이름 서버 등 Route 53가 도메인 등록 성공 후 반환하는 값을 알아봅니다.
4. 도메인 등록 상태 보기:
   - ICANN 상태 코드 및 등록자 이메일 주소 확인과 같이 종료 시 필요한 작업을 포함하여 도메인 등록의 현재 상태를 확인하는 방법을 알아봅니다.

새 도메인 등록

새 도메인을 등록하거나 기존 도메인의 이름 서버 업데이트

Route 53에 등록하는 도메인 및 다른 DNS 공급자에 등록한 도메인과 함께 Amazon Route 53를 사용할 수 있습니다. DNS 공급자에 따라 다음 절차 중 하나를 선택하여 Route 53에 새 도메인을 등록하고 사용합니다.

- 새로운 도메인을 등록하려면 Route 53를 사용하여 새 도메인 이름을 등록하려면를 참조하세요.
- 기존 도메인에 대해서는 Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정 섹션을 참조하세요.

- 도메인을 다른 등록자로 옮기는 방법은 update name servers when you want to use another DNS service를 참조하세요.

도메인 등록 고려 사항

시작하기 전에 다음 사항에 유의하세요.

AWS 지원 문의

도메인을 등록하는 동안 문제가 발생하면 무료로 AWS Support에 문의할 수 있습니다. 자세한 내용은 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.

도메인 등록 요금

도메인 등록 요금에 대한 자세한 내용은 Amazon Route 53 도메인 등록 요금을 참조하세요.

지원되는 도메인

지원되는 TLD 목록은 Amazon Route 53에 등록할 수 있는 도메인 단원을 참조하십시오.

도메인 이름을 등록한 후에는 변경할 수 없습니다.

실수로 잘못된 도메인 이름을 등록한 경우 변경할 수 없습니다. 그 대신 다른 도메인 이름을 등록하고 올바른 이름을 지정해야 합니다. 또한 실수로 등록한 도메인 이름에 대해서는 환불을 받을 수 없습니다.

AWS 크레딧

Route 53에 새 도메인을 등록하는 요금은 AWS 크레딧을 사용하여 지불할 수 없습니다.

특별 또는 프리미엄 가격

TLD는 일부 도메인 이름에 특별 또는 프리미엄 가격을 지정하고 있습니다. Route 53를 사용하여 특별 또는 프리미엄 가격이 적용되는 도메인을 등록할 수 없습니다.

호스팅 영역 요금

Route 53에 도메인을 등록하는 경우, Amazon은 자동으로 도메인에 대한 호스팅 영역을 생성하며, 도메인 등록에 대한 연간 요금에 더하여 호스팅 영역에 대한 소액의 월간 요금을 부과합니다. 이 호스팅 영역은 트래픽을 도메인(예: Amazon EC2 인스턴스 또는 CloudFront 배포)으로 라우팅하는 방법에 대한 정보를 저장하는 곳입니다. 도메인을 당장 사용하고 싶지 않다면, 호스팅 영역을 삭제할 수 있습니다. 도메인을 등록한 지 12시간 이내에 삭제하면 AWS 청구서 상에서 호스팅 영역에 대한 요금은 발생하지 않습니다. 도메인에 대해 수신하는 DNS 쿼리에 대한 소액의 요금도 부과됩니다. 자세한 내용은 Amazon Route 53 요금을 참조하십시오.

도메인의 호스팅 영역 바꾸기

도메인에 대해 새 호스팅 영역을 생성하는 경우 도메인의 이름 서버도 업데이트하여 새 호스팅 영역과 동일한 이름 서버를 사용해야 합니다. 세부 정보는 Route 53에 등록된 도메인의 호스팅 영역 바꾸기 단원을 참조하십시오.

Route 53를 사용하여 새 도메인 이름을 등록하려면

Route 53를 사용하여 새 도메인 이름을 등록하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 도메인, 등록된 도메인을 차례로 선택합니다.
3. 등록된 도메인 페이지에서 도메인 등록을 선택합니다.

   a. 도메인 검색 섹션에서 등록하려는 도메인 이름을 입력하고 검색을 선택하여 해당 도메인 이름이 사용 가능한지 알아봅니다.

   등록하려는 도메인 이름에 a-z, A-Z, 0-9 및 -(하이픈) 이외의 문자가 포함된 경우 다음 사항에 유의하십시오.

   - 해당 문자를 사용하여 이름을 입력할 수 있습니다. 이름을 퓨니코드로 변환하지 않아도 됩니다.
   - 언어 목록이 나타납니다. 지정된 이름의 언어를 선택합니다. 예를 들어 příklad(체코어로 “예”)를 입력하면 체코어(CES) 또는 체코어(CZE)를 선택합니다.

   > **Note**
   >
   > 코드가 둘 이상인 언어의 경우 코드 두 개를 모두 시도해야 할 수도 있습니다. CES와 CZE는 동의어이지만 일부 TLD 레지스트리는 둘 중 하나만 지원합니다.

   a-z, 0-9, -(하이픈) 이외의 문자를 지정하는 방법과 국제 도메인 이름을 지정하는 방법은 다음(DNS 도메인 이름 형식)을 참조하십시오.

   입력한 도메인을 사용할 수 있는 경우 해당 도메인이 표시되고, 사용할 수 없는 경우 유사한 도메인이 추천으로 표시됩니다.

등록할 도메인은 최대 5개까지 선택할 수 있습니다. 선택한 도메인이 선택된 도메인 목록에 표시됩니다.

b. 도메인을 더 등록하려면 3a~3b 단계를 반복합니다.

4. 결제 진행을 선택합니다.

5. 요금 페이지에서 도메인을 등록할 연수를 선택하고 만료일 전에 도메인 등록을 자동으로 갱신할지 여부를 선택합니다.

> **Note**
>
> 도메인 이름 등록과 갱신은 환불할 수 없습니다.다. 자동 도메인 갱신을 활성화하고 등록을 갱신한 후 도메인 이름이 필요 없다고 결정하는 경우 갱신 비용에 대한 환불을 받을 수 없습니다.

Next(다음)를 선택합니다.

6. 연락처 정보 페이지에서 도메인 등록자, 관리자, 기술 담당자, 청구 담당자의 연락처 정보를 입력합니다. 이곳에 입력하는 값들은 등록하려는 모든 도메인에 적용됩니다. 자세한 내용은 도메인을 등록하거나 이전할 때 지정하는 값 단원을 참조하십시오.

> **Important**
>
> 도메인 등록 중에 등록자로 나열하는 연락처는 ICANN 전송 정책에 따라 도메인 이름의 등록 이름 보유자로 특정 권한을 갖습니다. 대부분의 도메인은 종료 시 삭제되지만 AWS 계정 (자세한 내용은 참조내 AWS 계정이 닫히거나 영구적으로 닫히고 내 도메인이 Route 53에 등록됨) 도메인이 종료된 계정에 남아 있는 경우 등록자로 등록된 연락처는 외부 등록 기관으로 도메인 이름 이전을 요청할 수 있습니다. 따라서 나열한 등록자 연락처가 자신 또는 책임감 있게 행동할 것으로 신뢰하는 다른 사람이어야 합니다.

다음과 같은 고려 사항에 유의합니다.

이름, 성

[First Name]과 [Last Name]에는 귀하의 공식 ID에 표시된 이름을 지정하는 것이 좋습니다. 도메인 설정에 대한 일부 변경 사항의 경우, 일부 도메인은 신분 증명서를 제공하도록 요구합니

다. ID에 표시된 이름이 해당 도메인의 등록자 연락처에 기재된 이름과 정확히 일치해야 합니다.

다른 연락처

기본값으로 세 사람의 연락처에 대해 같은 정보를 사용합니다. 하나 이상의 연락처에 대해 다른 정보를 입력하려면 등록 연락처와 동일 토글 스위치 값을 비활성으로 변경합니다.

> **Note**
>
> .it 도메인의 경우 등록자 및 관리자 연락처가 동일해야 합니다.

> **Note**
>
> .jp 도메인의 경우 기술 담당자 및 관리 담당자 연락처가 동일해야 합니다.

여러 도메인

1개 이상의 도메인을 등록하는 경우에, 저희는 모든 도메인에 대해 같은 연락처 정보를 사용합니다.

필요한 추가 정보

일부 최상위 도메인(TLD)의 경우에 저희는 추가 정보를 수집할 의무가 있습니다. 이러한 TLD의 경우에는 [Postal/Zip Code] 필드 뒤에 해당 값을 입력합니다.

개인 정보 보호

WHOIS 쿼리로부터 연락처 정보를 숨길지 여부를 선택합니다.

> **Note**
>
> 관리자, 등록자, 기술 담당자, 청구 담당자에 대해 동일한 개인 정보 설정을 지정해야 합니다.

자세한 정보는 다음의 주제를 참조하세요.

- 도메인 연락처 정보의 개인 정보 보호 활성화 또는 비활성화

- Amazon Route 53에 등록할 수 있는 도메인

> **Note**
>
> .uk. .co.uk, .me.uk 및 .org.uk 도메인에 대한 개인 정보 보호를 활성화하려면 지원 사례를 열고 개인 정보 보호를 요청합니다.

Next(다음)를 선택합니다.

7. 검토 페이지에서 입력한 정보를 검토하고 수정할 수도 있습니다. 서비스 계약 조건을 읽은 다음, 확인란을 선택하여 서비스 계약 조건을 읽었음을 확인합니다.

   제출을 선택합니다.

8. 탐색 창에서 도메인을 선택한 다음 요청을 선택합니다.

   이 페이지에서 도메인의 상태를 볼 수 있으며 등록 기관 연락처 확인 이메일에 응답해야 하는지 여부도 확인할 수 있습니다. 확인 이메일을 다시 보내도록 선택할 수도 있습니다.

   Route 53에 도메인을 등록하는 데 사용된 적이 없는 등록 기관 담당자의 이메일 주소를 지정한 경우 일부 TLD 레지스트리는 해당 주소가 유효한지 확인하도록 요청합니다.

   다음 이메일 주소 중 하나에서 확인 이메일을 전송합니다.

   - noreply@registrar.amazon - Amazon Registrar에 등록된 TLDs 경우.
   - noreply@domainnameverification.net - 등록 기관 협력사 Gandi에서 등록한 TLD의 경우. TLD의 등록 기관을 확인하려면 등록 기관 찾기을 참조하세요.

   > **Important**
   >
   > 등록자 연락처는 이메일의 지시 사항에 따라 이메일을 받았다는 사실을 확인해야 합니다. 그렇지 않으면 ICANN에서 요구할 경우 도메인을 일시 중지해야 합니다. 도메인이 일시 중지되면 인터넷에서 접속할 수 없습니다.

   a. 확인 이메일을 받은 경우 이메일 주소가 유효한지 확인하는 이메일의 링크를 선택합니다. 이메일이 즉시 도착하지 않으면 스팸 메일함을 살펴보십시오.

b. 요청 페이지로 돌아갑니다. 상태가 이메일 주소가 확인됨으로 자동으로 업데이트되지 않으면 브라우저를 새로 고칩니다.

9. 도메인 등록이 완료되면, 그 다음 단계는 도메인에 대한 DNS 서비스로 Route 53를 사용할 것인지 아니면 다른 DNS 서비스를 사용할 것인지에 따라 달라집니다.

   - Route 53 - 도메인을 등록할 때 Route 53가 생성한 호스팅 영역에서 레코드를 생성하여 도메인 및 하위 도메인의 트래픽을 라우팅하는 방식을 Route 53에 지시합니다.

     예를 들어, 누군가 브라우저에 도메인 이름을 입력하고 그 쿼리가 Route 53에 전달될 때, Route 53가 데이터 센터의 웹 서버 IP 주소로 그 쿼리에 응답하길 원하십니까, 아니면 ELB 로드 밸런서의 이름으로 응답하길 원하십니까?

     자세한 내용은 레코드 작업 섹션을 참조하세요.

     > **Important**
     >
     > Route 53가 자동으로 생성한 것이 아닌 다른 호스팅 영역에서 레코드를 생성할 경우 도메인의 이름 서버를 업데이트해야 새 호스팅 영역에 대해 이름 서버를 사용할 수 있습니다.

   - 다른 DNS 서비스 - 새 도메인이 DNS 쿼리를 다른 DNS 서비스로 라우팅하도록 구성합니다. 다른 등록자를 사용하도록 이름 서버를 업데이트합니다. 절차를 수행합니다.

도메인을 등록하거나 이전할 때 지정하는 값

> **Note**
>
> Route 53의 도메인 콘솔을 업데이트했습니다. 이전 기간 동안에는 이전 콘솔을 계속 사용하거나 새 콘솔을 사용할 수 있습니다. Route 53에서 반환되는 대부분의 정보는 두 콘솔에서 동일합니다. 차이점은 다음 목록에 나와 있습니다.

도메인을 등록하거나 도메인 등록을 Amazon Route 53으로 이전할 때는 이 주제에서 설명된 값들을 지정합니다.

> **Note**
>
> 1개 이상의 도메인을 등록하는 경우, Route 53는 장바구니에 있는 모든 도메인들에 대해 지정한 값을 사용합니다.

그 밖에 현재 Route 53를 통해 등록된 도메인의 값을 변경할 수도 있습니다. 다음 사항에 유의하세요.

- 도메인에 대한 연락처 정보를 변경하면 그 변경에 관해 등록자 연락처로 이메일 알림이 전송됩니다. 이 이메일은 noreply@registrar.amazon에서 보낸 것입니다. 대부분의 경우, 등록자 연락처가 그 이메일에 응답할 필요는 없습니다.
- 또한 소유권 변경을 구성하는 연락처 정보의 변경에 대해서는 등록자 연락처로 추가 이메일이 전송됩니다. ICANN은 해당 이메일을 받았다는 사실을 등록자 연락처가 확인하도록 요구합니다. 자세한 내용은 이 섹션 뒷부분의 [First Name, Last Name] 및 [Organization] 단원을 참조하십시오.

기존 도메인의 설정 변경 방법에 대한 자세한 내용은 도메인 설정 업데이트 단원을 참조하십시오.

지정하는 값

- My Registrant, Administrative, and Technical contacts are all the same
- Contact Type
- First Name, Last Name
- Organization
- Email
- Phone
- Address 1
- Address 2
- Country
- State
- City
- Postal/Zip Code
- Fields for selected top-level domains
- Privacy Protection
- Auto-renew

등록자 연락처와 동일

도메인 등록자, 관리자, 기술 담당자의 연락처 정보를 모두 같은 것으로 사용하고자 하는지 여부를 지정합니다.

연락처 유형

이 연락처의 범주를 말합니다. 다음 사항에 유의하세요.

- [Person] 이외의 옵션을 선택한 경우 조직 이름을 입력해야 합니다.
- 일부 TLD의 경우 사용 가능한 개인 정보 보호는 [Contact Type]에서 선택한 값에 따라 다릅니다. TLD의 개인 정보 보호 설정은 Amazon Route 53에 등록할 수 있는 도메인 단원을 참조하십시오.
- .es 도메인의 경우 연락처 유형 값은 세 연락처 모두에 대해 개인이어야 합니다.

이름, 성

연락할 사람의 이름과 성.

> **Important**
>
> [First Name]과 [Last Name]에는 귀하의 공식 ID에 표시된 이름을 지정하는 것이 좋습니다. 도메인 설정에 대한 일부 변경 사항의 경우, 신분 증명서를 제공해야 하고 ID의 이름이 해당 도메인의 등록자 연락처 이름과 일치해야 합니다.

도메인을 Route 53으로 이전하는 경우 다음 조건에 해당하면 도메인 소유자를 변경합니다.

- 연락처 유형이 개인인 경우.
- 현재 설정에서 등록자 연락처의 이름 및/또는 성 필드를 변경합니다.

이 경우 ICANN은 등록자 연락처에 이메일을 보내 승인을 얻도록 규정하고 있습니다. 다음 이메일 주소 중 하나에서 이메일을 전송합니다.

TLD	승인 이메일을 발송하는 이메일 주소
Amazon Registrar에서 등록한 TLD	noreply@registrar.amazon
.fr	nic@nic.fr(이메일은 현재 등록자 연락처 및 새 등록자 연락처 모두에 전송됩니다.)

TLD	승인 이메일을 발송하는 이메일 주소
기타 모두	noreply@domainnameverification.net

TLD의 등록 대행자를 확인하려면 Amazon Route 53에 등록할 수 있는 도메인을 참조하십시오.

> **Important**
>
> 등록자 연락처는 이메일의 지시 사항에 따라 이메일을 받았다는 사실을 확인해야 합니다. 그렇지 않으면 ICANN에서 요구할 경우 도메인 이름이 일시 중지해야 합니다. 도메인이 일시 중지되면 인터넷에서 접속할 수 없습니다.

등록자 연락처의 이메일 주소를 변경하면, 이 이메일이 등록자 연락처에 대한 이전의 이메일 주소 및 새 이메일 주소로 전송됩니다.

일부 TLD 등록 대행자들의 경우에는 도메인 소유자 변경에 대해 요금을 부과합니다. 이 값들 중 하나를 변경하면, Route 53 콘솔이 요금이 발생하는지 여부를 알리는 메시지를 표시합니다.

조직

연락처와 관련된 조직. 등록자 및 관리자 연락처의 경우에는 일반적으로 도메인을 등록하는 조직을 말합니다. 기술 담당자 연락처의 경우에는 도메인을 관리하는 조직일 수 있습니다.

연락처 유형이 [Person]을 제외한 다른 값이고 등록자 연락처에 대해 [Organization] 필드를 변경하는 것은 도메인 소유자를 변경하는 것이나 마찬가지입니다. ICANN은 이 경우 등록자 연락처에 이메일을 보내 승인을 얻도록 규정하고 있습니다. 다음 이메일 주소 중 하나에서 이메일을 전송합니다.

TLD	승인 이메일을 발송하는 이메일 주소
Amazon Registrar에서 등록한 TLD	noreply@registrar.amazon
.fr	nic@nic.fr(이메일은 현재 등록자 연락처 및 새 등록자 연락처 모두에 전송됩니다.)

TLD	승인 이메일을 발송하는 이메일 주소
기타 모두	noreply@domainnameverification.net

TLD의 등록 대행자를 확인하려면 Amazon Route 53에 등록할 수 있는 도메인을 참조하십시오.

등록자 연락처의 이메일 주소를 변경하면, 이 이메일이 등록자 연락처에 대한 이전의 이메일 주소 및 새 이메일 주소로 전송됩니다.

일부 TLD 등록 대행자들의 경우에는 도메인 소유자 변경에 대해 요금을 부과합니다. 조직(Organization)의 값을 변경하면, Route 53 콘솔이 요금이 발생하는지 여부를 알리는 메시지를 표시합니다.

이메일

연락 대상의 이메일 주소.

등록자 연락처의 이메일 주소를 변경하면, 알림 이메일이 이전의 이메일 주소 및 새 이메일 주소로 전송됩니다. 이 이메일은 noreply@registrar.amazon에서 보낸 것입니다.

전화번호

연락 대상의 전화번호.

- 미국 또는 캐나다 지역의 전화번호를 입력할 경우에는, 첫 번째 필드에 [1]을, 두 번째 필드에는 열 자리의 지역 번호 및 전화번호를 입력합니다.
- 기타 지역의 전화번호를 입력할 경우에는, 첫 번째 필드에 국가 번호를, 두 번째 필드에는 나머지 전화번호를 입력합니다. 전화 국가 코드 목록은 Wikipedia 기사 List of country calling codes 단원을 참조하십시오.

주소 1

연락 대상의 거리 주소.

주소 2

아파트 번호 또는 우편함과 같은 연락 대상의 추가 주소 정보.

국가

연락 대상의 국가.

시/도

연락 대상의 주 또는 도(해당되는 경우).

구/군/시

연락 대상의 도시.

우편번호

연락 대상의 우편 번호.

선택한 최상위 도메인의 필드

다음 최상위 도메인(TLD)에서는 값을 추가 지정해야 합니다.

- .com.au 및 .net.au
- .ca
- .es
- .fi
- .fr
- .it
- .ru
- .se
- .sg
- .co.uk, .me.uk, .org.uk,.uk

또한 여러 TLD에서는 VAT 식별 번호를 요구합니다.

유효한 값에 대한 자세한 내용은 Amazon Route 53 API 참조의 ExtraParam을 참조하세요.

개인 정보 보호

WHOIS 쿼리로부터 연락처 정보를 감추길 원하는지 여부. 개인 정보 보호 켜기(새 콘솔)를 선택하거나 연락처 정보 숨기기(이전 콘솔)을 선택한 경우 WHOIS('who is') 쿼리는 등록자에 대한 연락처 정보 또는 '정책으로 보호됨' 값을 반환합니다.

> **Note**
>
> 관리자, 등록자, 기술 담당자, 청구 담당자에 대해 동일한 개인 정보 설정을 지정해야 합니다.

[Don't hide contact information]을 선택하면, 지정한 이메일 주소로 더 많은 스팸 메일을 받습니다.

누구나 도메인에 대한 WHOIS 쿼리를 전송하여 그 도메인에 대한 연락처 정보 전체를 받을 수 있습니다. WHOIS 명령은 많은 운영 체제에서 사용할 수 있고, 많은 웹 사이트에서 웹 애플리케이션으로도 사용 가능합니다.

> **Important**
>
> 도메인과 연결된 연락처 정보에 대한 합법적 사용자가 있지만, 가장 흔한 사용자들은 원하지 않는 이메일 및 가짜 제안으로 도메인 연락처를 노리는 스패머들입니다. 일반적으로 저희는 [Privacy Protection]에 대해 [Hide contact information]를 선택하도록 권장합니다.

일부 도메인에 대한 개인 정보 보호를 활성화하거나 비활성화하려면 지원 사례를 열고 개인 정보 보호를 요청합니다.

개인 정보 보호에 대한 자세한 내용은 다음 주제를 참조하십시오.

- 도메인 연락처 정보의 개인 정보 보호 활성화 또는 비활성화
- Amazon Route 53에 등록할 수 있는 도메인

자동 갱신(도메인 설정을 편집할 때만 사용 가능)

Route 53가 도메인 만료 전에 도메인을 자동으로 갱신하길 원하는지 여부. 등록 요금은 AWS 계정에 청구됩니다. 이전 콘솔에서는 도메인 설정을 편집할 때만 이 설정을 사용할 수 있습니다. 자세한 내용은 도메인 등록 갱신 단원을 참조하십시오.

> **Important**
>
> 자동 갱신을 비활성화하면 만료 날짜가 지나도 도메인에 대한 등록이 갱신되지 않아 도메인 이름에 대한 통제권을 상실할 수 있습니다.

도메인 이름을 갱신할 수 있는 기간은 TLD(최상위 도메인) 별로 차이가 있습니다. 도메인 갱신에 대한 개요는 도메인 등록 갱신 단원을 참조하십시오. 지정된 연 수 동안 도메인 등록을 연장하는 방법에 대한 자세한 내용은 도메인의 등록 기간 연장 단원을 참조하십시오.

도메인을 등록할 때 Amazon Route 53가 반환하는 값

Amazon Route 53에 도메인을 등록할 때 Route 53는 지정한 값뿐만 아니라 다음 값들도 반환합니다.

등록 날짜

Route 53에 도메인을 최초로 등록한 날짜.

만료 날짜

현재 등록 기간이 만료되는 날짜 및 시간(그리니치 표준시, GMT).

일부 최상위 도메인(TLD) 등록 기관의 등록 기간은 더 길지만, 등록 기간은 보통 1년입니다. TLD의 등록 및 갱신 기간은 Amazon Route 53에 등록할 수 있는 도메인을 참조하십시오.

대부분의 TLD의 경우 등록 기간을 최대 10년 연장할 수 있습니다. 자세한 내용은 도메인의 등록 기간 연장 섹션을 참조하세요.

도메인 이름 상태 코드

도메인의 현재 상태.

도메인 이름의 중앙 데이터베이스를 유지하는 조직인 ICANN은 도메인 이름의 다양한 작업 상태를 알려주는 일련의 도메인 이름 상태 코드(EPP 상태 코드라고도 함)를 개발했습니다. 예를 들어, 도메인 이름 등록, 도메인 이름을 다른 등록자로 이전, 도메인 이름에 대한 등록 갱신 등이 있습니다. 모든 등록 대행자는 이 상태 코드를 사용합니다.

도메인 이름 상태 코드의 현재 목록과 각 코드의 의미에 대한 설명을 보시려면 ICANN 웹 사이트로 가서 [epp status codes]를 검색하십시오. ICANN 웹 사이트에서 검색하십시오. 웹 검색 시 때로는 지난 버전의 문서가 표시될 수도 있습니다.

이전 잠금

누군가 귀하의 도메인을 허락 없이 다른 등록 대행자에게 이전할 가능성을 줄이기 위해 도메인을 잠글 것인지 여부. 도메인이 잠겨 있으면, 이전 잠금의 값은 활성입니다. 도메인이 잠겨 있지 않으면, 값은 비활성입니다.

자동 갱신

만료 날짜 직전에 이 도메인의 등록을 Route 53가 자동으로 갱신할 것인지 여부.

권한 부여 코드

이 도메인의 등록을 다른 등록 대행자에게 이전하고 싶은 경우에 필요한 코드. 권한 부여 코드는 그것을 요청할 때만 생성됩니다. 도메인을 다른 등록 대행자에게 이전하는 것에 대한 내용은 다음(Amazon Route 53에서 다른 등록 기관으로 도메인 이전하기)을 참조하십시오.

이름 서버

이 도메인에 대한 DNS 쿼리에 응답하는 Route 53 서버. Route 53 이름 서버는 삭제하지 않는 것이 좋습니다.

이름 서버 추가, 변경, 또는 삭제에 대한 내용은 다음(도메인의 글루 레코드 및 이름 서버 추가 또는 변경)을 참조하십시오.

도메인 등록 상태 보기

도메인 이름의 중앙 데이터베이스를 유지하는 조직인 ICANN은 도메인 이름의 다양한 작업 상태, 예를 들어 도메인 이름 등록, 다른 등록 대행자에 대한 도메인 이름 이전, 도메인 이름 등록 갱신 등에 대해 알려주는 일련의 도메인 이름 상태 코드(EPP 상태 코드라고도 함)를 개발했습니다. 모든 등록 대행자는 이 상태 코드를 사용합니다.

도메인의 상태 코드를 보려면, 다음 절차를 수행하십시오.

도메인의 ICANN 상태 코드를 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 도메인을 확장하고 등록된 도메인을 선택합니다.
3. 도메인의 링크된 이름을 선택합니다.
4. 등록자 연락처에 확인 이메일을 다시 보내는 등의 조치를 취해야 하는 경우 페이지 상단의 배너에 수행해야 할 조치가 표시됩니다.
5. 도메인의 현재 상태를 보려면 도메인 상태 코드 필드의 값을 확인합니다.

   도메인 이름 상태 코드의 현재 목록과 각 코드의 의미에 대한 설명을 보시려면 ICANN 웹 사이트로 가서 [epp status codes]를 검색하십시오. ICANN 웹 사이트에서 검색하십시오. 웹 검색 시 때로는 지난 버전의 문서가 표시될 수도 있습니다.

요청 페이지에서 등록 상태를 볼 수도 있습니다.

등록 상태를 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 도메인을 확장하고 요청을 선택합니다.

3. 요청 페이지에서 등록 상태를 볼 수 있으며, 도메인 삭제, 도메인 이전 잠금, DNSSEC 키 추가 또는 삭제 등 도메인에서 수행한 기타 작업의 상태를 볼 수 있습니다.

   이메일 확인과 같은 프로세스를 완료하기 위해 취해야 할 모든 조치도 나열되어 있습니다.

   - 작업 요청에 응답하려면 도메인 이름 옆에 있는 라디오 버튼을 선택한 다음 작업 드롭다운에서 작업을 선택합니다.

도메인 설정 업데이트

이 섹션에서는 Route 53의 도메인 설정 관리와 관련된 다음 주제에 대한 정보를 제공합니다.

1. 도메인 연락처 정보 및 소유권 업데이트:
   - 관리자, 기술 담당자, 등록자, 청구 담당자의 연락처를 포함하여 도메인의 연락처 정보를 업데이트하는 방법을 알아봅니다.
   - 등록 기관에서 도메인 소유권 변경 양식을 요청할 경우의 도메인 소유자 변경 절차를 이해합니다.
2. 도메인 연락처 정보의 개인 정보 보호 활성화 또는 비활성화:
   - WHOIS 쿼리에서 개인 세부 정보를 숨기거나 공개하는 연락처 정보에 대한 개인 정보 보호를 활성화하거나 비활성화하는 방법을 알아봅니다.
3. 도메인 자동 갱신 활성화 또는 비활성화:
   - 도메인의 자동 갱신을 활성화하거나 비활성화하는 방법을 알아봅니다. 그러면 Route 53가 만료 전에 등록을 자동으로 갱신할지 여부를 결정합니다.
4. 다른 등록 대행자로의 무단 이전을 방지하기 위해 도메인 잠그기:
   - 다른 등록 기관으로 무단 전송을 방지하기 위해 도메인을 잠그는 방법과 필요한 경우 잠금을 비활성화하는 방법을 알아봅니다.
5. 도메인의 등록 기간 연장:
   - 도메인의 등록 기간을 1년 단위로 최대 10년까지 연장하는 절차를 이해합니다.
6. 다른 등록자를 사용하도록 이름 서버를 업데이트합니다. 및 도메인의 글루 레코드 및 이름 서버 추가 또는 변경:
   - 이름 서버를 업데이트하여 다른 DNS 서비스를 사용하거나 화이트 레이블(베니티) 이름 서버를 구성하는 방법을 알아봅니다.
   - 이름 서버와 글루 레코드를 변경할 때의 고려 사항과 모범 사례를 알아봅니다.

도메인 연락처 정보 및 소유권 업데이트

도메인에 대한 관리 및 기술 담당 연락처를 변경 승인 없이 모두 변경할 수 있습니다. 자세한 내용은 도메인 연락처 정보 업데이트 단원을 참조하십시오.

등록자 연락처의 경우, 변경 승인 없이 대부분의 값을 변경할 수 있습니다. 하지만 일부 TLD의 경우 도메인 소유자를 변경하려면 승인이 필요합니다. 자세한 내용은 관련 주제를 참조하십시오.

주제

도메인 소유자는 누구입니까?

> **Important**
>
> 등록자로 나열한 연락처는 ICANN 전송 정책에 따라 도메인 이름의 등록 이름 보유자로 특정 권한을 갖습니다. 대부분의 도메인은 종료 시 삭제되지만 AWS 계정 (자세한 내용은 참조내 AWS 계정이 닫히거나 영구적으로 닫히고 내 도메인이 Route 53에 등록됨) 도메인이 종료된 계정에 남아 있는 경우 등록자로 등록된 연락처는 외부 등록 기관으로 도메인 이름 이전을 요청할 수 있습니다. 따라서 나열한 등록자 연락처가 자신 또는 책임감 있게 행동할 것으로 신뢰하는 다른 사람이어야 합니다.

연락처 유형이 [Person]이고 등록자 연락처의 [First Name] 또는 [Last Name] 필드를 변경하는 것은 도메인 소유자를 변경하는 것이나 마찬가지입니다.

연락처 유형이 Person 외의 다른 값일 경우 Organization을 변경하면 도메인 소유자가 변경됩니다.

도메인 소유자 변경에 대한 다음 정보를 확인하십시오.

- 일부 TLD의 경우 도메인 소유자를 변경하려면 수수료가 부과됩니다. 도메인에 대한 TLD 수수료가 있는지 여부를 확인하려면 Amazon Route 53 도메인 등록 요금의 "소유권 변경 요금" 열을 참조하세요.

> **Note**
>
> AWS 크레딧을 사용하여 요금을 지불하고 도메인 소유자를 변경할 수 없습니다.

- 일부 TLD의 경우 도메인 소유자를 변경하면 등록자 연락처의 이메일 주소로 권한 부여 이메일이 발송됩니다. 등록자 연락처는 이메일의 지침에 따라 변경을 승인해야 합니다.
- 일부 TLD의 경우 Amazon Route 53 지원 엔지니어가 정보를 업데이트할 수 있도록 도메인 소유권 변경 양식을 작성하고 자격 증명 사본을 제공해야 합니다. 해당 도메인의 TLD가 도메인 소유권 변경 양식이 필요한 TLD인 경우, 지원 요청 생성을 위한 양식으로 이동하는 링크가 포함된 메시지가 콘솔에 표시됩니다. 자세한 내용은 등록 기관에서 도메인 소유권 변경 양식을 요청할 경우의 도메인 소유자 변경 단원을 참조하십시오.

소유자를 변경하기 위해 특별 처리가 필요한 TLD

도메인 소유자를 변경할 때 일부 TLD의 레지스트리에서는 특별 처리가 필요합니다. 다음 도메인 중 하나에 대한 소유자를 변경하는 경우 해당 절차를 수행합니다. 다른 도메인의 소유자를 변경하는 경우 프로그래밍 방식으로 또는 Route 53 콘솔을 사용하여 소유자를 직접 변경할 수 있습니다. 도메인 연락처 정보 업데이트을 참조하세요.

다음 TLD의 경우 도메인 소유자를 변경하려면 특별한 처리가 필요합니다.

.be, .cl, .com.br, .es, .fi, .ru, .se, .sh

.be

.be 도메인에 대한 레지스트리에서 전송 코드를 가져온 다음 AWS Support에서 사례를 열어야 합니다.

- 이전 코드를 받으려면 https://www.dnsbelgium.be/en/manage-your-domain-name/change-holder#transfer를 참조하고 화면에 나타나는 메시지를 따릅니다.
- 사례를 개설하려면 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.

.cl

양식을 작성하여 AWS Support에 제출해야 합니다. 등록 기관에서 도메인 소유권 변경 양식을 요청할 경우의 도메인 소유자 변경을 참조하세요.

.com.ar

양식을 작성하여 AWS Support에 제출해야 합니다. 등록 기관에서 도메인 소유권 변경 양식을 요청할 경우의 도메인 소유자 변경을 참조하세요.

.com.br

양식을 작성하여 AWS Support에 제출해야 합니다. 등록 기관에서 도메인 소유권 변경 양식을 요청할 경우의 도메인 소유자 변경을 참조하세요.

.es

양식을 작성하여 AWS Support에 제출해야 합니다. 등록 기관에서 도메인 소유권 변경 양식을 요청할 경우의 도메인 소유자 변경을 참조하세요.

.fi

Route 53 콘솔에서 소유자 변경을 시작합니다. 변경을 시작한 후 fi-domain-tech@traficom.fi 이메일 주소로부터 소유자 이전 키(Holder transfer key)를 받습니다. 키를 받은 후 AWS Support에서 지원 사례를 열고 키 코드를 공유하세요. 도메인 등록 문제에 대한 AWS 지원 문의을 참조하세요.

.qa

양식을 작성하여 AWS Support에 제출해야 합니다. 등록 기관에서 도메인 소유권 변경 양식을 요청할 경우의 도메인 소유자 변경을 참조하세요.

.ru

양식을 작성하여 AWS Support에 제출해야 합니다. 등록 기관에서 도메인 소유권 변경 양식을 요청할 경우의 도메인 소유자 변경을 참조하세요.

.se

양식을 작성하여 AWS Support에 제출해야 합니다. 등록 기관에서 도메인 소유권 변경 양식을 요청할 경우의 도메인 소유자 변경을 참조하세요.

sh

양식을 작성하여 AWS Support에 제출해야 합니다. 등록 기관에서 도메인 소유권 변경 양식을 요청할 경우의 도메인 소유자 변경을 참조하세요.

도메인 연락처 정보 업데이트

도메인의 연락처 정보를 업데이트하려면 다음과 같이 하십시오.

도메인 연락처 정보를 업데이트하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.

2. 탐색 창에서 등록된 도메인을 선택합니다.
3. 연락처 정보를 업데이트하고자 하는 도메인의 이름을 선택합니다.
4. 연락처 정보 탭에서 편집을 선택합니다.
5. 등록자 연락처의 이메일 주소에 대한 액세스 권한이 없는 경우 다음 단계를 수행합니다. 등록자 연락처의 이메일 주소에 대한 액세스 권한이 있는 경우 6단계로 건너뜁니다.

   a. 등록자 연락처의 이메일 주소만 변경합니다. 도메인 연락처 중 하나의 다른 값을 변경하지 마십시오. 다른 값도 변경하려는 경우 프로세스의 나중에 변경합니다.

      Save changes(변경 사항 저장)를 선택합니다.

      새 이메일 주소를 확인하려면 새 주소로 확인 이메일을 보냅니다(TLD에 필요한 경우). 새 이메일 주소가 유효한지 확인하려면 이메일의 링크를 선택해야 합니다. 확인이 필요한 경우, 새 이메일 주소를 확인하지 않으면 Route 53는 ICANN의 필요에 따라 도메인을 일시 중단합니다.

      확인 이메일을 다시 보내야 하는 경우 등록된 도메인 페이지로 이동하여 업데이트한 도메인 이름 옆에 있는 라디오 버튼을 선택한 다음 업데이트하려는 도메인의 이름을 선택합니다. 도메인 일시 중지를 방지하기 위해 이메일 확인 알림에서 이메일 다시 보내기를 선택합니다.

   b. 도메인의 등록자, 관리자, 기술 담당자 또는 청구 담당자의 다른 값을 변경하려면 1단계로 돌아가서 절차를 반복합니다.
6. 관련 값들을 업데이트합니다. 등록 연락처 복사를 선택하여 등록 연락처에 입력한 것과 동일한 정보를 자동으로 입력할 수도 있습니다. 자세한 내용은 도메인을 등록하거나 이전할 때 지정하는 값 단원을 참조하십시오.

   도메인의 TLD와 변경하려는 값에 따라 콘솔에 다음 메시지가 표시될 수 있습니다.

   "To change the registrant name or organization, open a case(등록자 이름이나 조직을 변경하려면 지원 요청을 생성하십시오)."

   이 메시지가 표시될 경우 이 절차의 나머지 부분을 건너뛰고 등록 기관에서 도메인 소유권 변경 양식을 요청할 경우의 도메인 소유자 변경에서 자세한 정보를 확인하십시오.
7. 저장(Save)을 선택합니다.
8. 도메인 소유자를 변경한 경우 도메인 소유자는 누구입니까?에서 설명한 대로 도메인 등록자 연락처로 이메일이 발송됩니다. 이메일은 소유자 변경을 위한 승인을 요청합니다.

   최상위 도메인에 따라 다르지만 3~15일 이내에 변경이 승인되지 않으면 ICANN의 요구에 따라 요청을 취소해야 합니다.

이메일은 다음 이메일 주소 중 하나에서 발송합니다.

TLD	권한 부여 이메일을 발송하는 이메일 주소
.fr	nic@nic.fr
.com.au .net.au	noreply@emailverification.info
기타 모두	다음 이메일 주소 중 하나: • noreply@registrar.amazon • noreply@domainnameverification.net

9. 연락처 정보를 업데이트하는 동안 문제가 발생하면 AWS Support에 무료로 문의할 수 있습니다. 자세한 내용은 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.

연락처 정보를 업데이트하는 데 사용할 수 있는 API에 대한 자세한 내용은 UpdateDomainContact를 참조하세요.

등록 기관에서 도메인 소유권 변경 양식을 요청할 경우의 도메인 소유자 변경

도메인의 레지스트리에서 도메인 소유권 변경을 완료하고 AWS Support에 양식을 제출해야 하는 경우 다음 절차를 수행합니다. 이 절차를 수행해야 하는지 여부를 확인하려면 다음 주제를 참조하십시오.

- 변경하려는 값이 소유자 변경으로 간주되는지 여부를 확인하려면 도메인 소유자는 누구입니까? 단원을 참조하십시오.
- 도메인에 도메인 소유권 변경 양식이 필요한지 여부를 확인하려면 소유자를 변경하기 위해 특별 처리가 필요한 TLD 단원을 참조하십시오.

등록 기관에서 도메인 소유권 변경 양식을 요청할 경우 도메인 소유자를 변경하려면

1. 도메인의 소유자를 변경할 때 도메인의 등록 기관에서 특별 처리가 필요한지 여부를 확인하려면 이 주제의 소개 단원을 참조하십시오. 특별 처리가 필요하고 도메인 소유권 변경 양식이 필요한 경우 이 절차를 계속합니다.

   도메인 소유권 변경 양식이 필요하지 않은 경우 그 대신 적용되는 주제의 절차를 수행합니다.
2. 도메인 소유권 변경 양식을 다운로드합니다. 파일은 .zip 파일로 압축됩니다.
3. 양식을 작성합니다.
4. 이전 도메인 소유자 그리고 새 소유자에 대한 등록자 연락처의 경우, 신분증, 운전면허증, 여권 또는 기타 법률상 신분 증명서와 같이, 개인 신원을 증명할 수 있는 증서 복사본을 준비합니다.

   또한 등록자 조직으로 법인이 명시되어 있을 경우 이전 도메인 소유자 그리고 새로운 소유자에 대한 다음 정보를 입수합니다.

   - 도메인이 등록된 조직이 존재함을 증명하는 증명서.
   - 이전 소유자 및 새 소유자의 대리인이 조직을 대신해 행동할 권한이 있음을 보여주는 증서. 이 문서는 조직 이름과 계약 중역(CEO, 사장, 전무 등)으로서 대리인의 이름을 모두 포함하는 공인 법률 문서여야 합니다.
5. 도메인 소유권 변경 양식과 필요한 증명서를 스캔합니다. 스캔한 문서를 .pdf 파일이나 .png 파일 같은 일반적인 형식으로 저장합니다.
6. 도메인이 현재 등록된 AWS 계정을 사용하여 AWS 지원 센터에 로그인합니다.

   Important

   다음 방법을 사용하여 루트 계정을 사용하거나 IAM 권한을 부여한 사용자를 이용하여 로그인해야 합니다.

   - 사용자에게 AdministratorAccess 관리형 정책을 할당했습니다.
   - 사용자에게 AmazonRoute53DomainsFullAccess 관리형 정책을 할당했습니다.
   - 사용자에게 AmazonRoute53FullAccess 관리형 정책을 할당했습니다.

   루트 계정을 사용하거나 필수 권한이 있는 사용자를 사용하여 로그인하지 않으면 도메인 소유자를 변경할 수 없습니다. 이는 권한이 없는 사용자가 도메인 소유자를 변경하는 것을 방지하기 위한 조치입니다.
7. 다음 값을 지정하세요.

관련

계정 및 청구의 기본값을 수락합니다.

Service

도메인의 기본값을 수락합니다.

범주

소유권 변경의 기본값을 수락합니다.

심각도

일반 질문의 기본값을 수락합니다.

다음 단계: 추가 정보(Next step: Additional information)를 선택합니다

제목

Change the owner of a domain(도메인 소유자 변경)을 지정합니다.

설명

다음 정보를 제공합니다.

- 소유자를 변경하려는 도메인
- 도메인이 등록된 계정의 12자리 계정 ID AWS

첨부 파일 추가

5단계에서 스캔한 문서를 업로드합니다.

연락 방법

연락 방법을 지정하고 해당 정보를 입력합니다.

8. 제출을 선택합니다.

AWS 지원 엔지니어가 제공한 정보를 검토하고 설정을 업데이트합니다. 업데이트가 완료되거나 추가 정보가 필요할 경우 엔지니어가 연락을 드립니다.

도메인 연락처 정보의 개인 정보 보호 활성화 또는 비활성화

Amazon Route 53를 통해 도메인을 등록하거나 도메인을 Route 53으로 이전하는 경우 도메인의 모든 연락처에 대해 기본적으로 개인 정보 보호가 활성화됩니다. 이렇게 하면 일반적으로 대부분의

연락처 정보가 WHOIS("Who is") 쿼리에서 숨겨지며 수신하는 스팸 메일의 양이 줄어듭니다. 개인 정보 보호를 활성화하면 연락처 정보는 등록 기관의 연락처 정보 또는 "개인 정보 보호를 위해 편집됨(REDACTED FOR PRIVACY)" 또는 "<도메인 이름> 소유자 대신(On behalf of <domain name> owner)"이라는 문구로 대체됩니다.

개인 정보 보호를 비활성화한 경우, 도메인의 모든 연락처에 대해 비활성화해야 합니다. 개인 정보 보호를 비활성화하면 누구나 도메인에 대한 WHOIS 쿼리를 보낼 수 있으며 대부분의 최상위 도메인(TLD)에 대해 이름, 주소, 전화번호, 이메일 주소를 포함해 도메인 등록 시 또는 이전 시 제공한 모든 연락처 정보를 얻을 수 있습니다. WHOIS 명령은 널리 사용되고 있고, 여러 운영 체제에 내장되어 있으며, 또한 여러 웹 사이트에서 웹 애플리케이션으로도 사용 가능합니다.

도메인을 다른 등록기관으로 이전하고 도메인 연락처에 대해 개인 정보 보호가 활성화된 경우, 이전 확인을 위한 이메일이 Amazon Registrar에 등록된 TLD의 identity-protect.org 주소에서 전송됩니다. TLD의 등록 기관을 확인하려면 등록 기관 찾기을 참조하세요.

WHOIS 쿼리로부터 숨길 수 있는 정보는 두 가지 요인에 달려 있습니다.

최상위 도메인 등록

대부분 TLD 등록 기관에서는 자동으로 모든 연락처 정보를 숨기지만, 사용자가 모든 연락처 정보를 숨기도록 선택할 수 있게 허용하거나, 사용자가 일부 정보만 숨길 수 있도록 허용하거나, 정보 숨김을 허용하지 않는 기관도 있습니다.

도메인에서 개인 정보 보호를 활성화하면 연락처 정보가 개인 정보 보호 서비스의 연락처 정보 또는 “개인 정보 보호를 위해 편집됨(REDACTED FOR PRIVACY)”이라는 문구로 대체됩니다. 개인 정보 보호 서비스는 스팸 방지 기능을 적용하며(주소 회전 및 SPF/DKIM/스팸 분석 등) 대부분 이러한 필터를 통과하는 이메일을 자동으로 전달합니다. 그러나 스팸 메커니즘으로 인해 전달되지 않을 수 있으므로 프라이버시가 보호된 이메일 주소로 중요한 이메일을 보내는 것은 좋지 않습니다.

또한, 한 도메인에 어느 개인 정보 보호 방식을 사용할지 선택은 사용자가 구성할 수 없고, 시스템이 자동 선택합니다. 개인 정보 보호 서비스의 연락처 세부 정보를 수동으로 업데이트할 수 없습니다.

> **Note**
>
> 일부 도메인에 대한 개인 정보 보호를 활성화하거나 비활성화하려면 지원 사례를 열고 개인 정보 보호를 요청합니다. 자세한 내용은 Amazon Route 53에 등록할 수 있는 도메인에서 해당 단원을 참조하십시오.
>
> - .co.uk(영국)
> - .me.uk(영국)
> - .org.uk(영국)

- .link

등록 대행자

Route 53를 통해 도메인을 등록하거나 도메인을 Route 53로 이전하는 경우 도메인 등록 기관은 Amazon Registrar 또는 등록 대행 협력사 Gandi입니다. Amazon Registrar와 Gandi는 기본적으로 다른 정보를 숨깁니다.

- Amazon Registrar - 기본적으로 모든 연락처 정보가 숨겨집니다. 하지만 TLD 등록 기관에 대한 규정이 우선적으로 적용됩니다.
- Gandi - 기본적으로 조직 이름(있을 경우)을 제외한 모든 연락처 정보가 숨겨집니다. 하지만 TLD 등록 기관에 대한 규정이 우선적으로 적용됩니다.

  개인 정보 보호를 허용하지 않는 지리적 TLD의 경우, Gandi 웹 사이트의 Whois Directory Search 페이지에서 개인 정보가 "redacted(편집됨)"으로 표시됩니다. 하지만 도메인 등록 기관이나 제3자 WHOIS 웹 사이트에서 해당 개인 정보가 제공될 수도 있습니다.

도메인의 TLD에 대해 어떤 정보가 숨겨지는지 알아보려면 Amazon Route 53에 등록할 수 있는 도메인 단원을 참조하십시오.

Route 53를 사용하여 등록한 도메인의 개인 정보 보호를 활성화 또는 비활성화하려면 다음 절차를 수행하세요.

도메인 연락처 정보의 개인 정보 보호를 활성화 또는 비활성화하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 등록된 도메인을 선택합니다.
3. 개인 정보 보호를 활성화 또는 비활성화하려는 도메인의 이름을 선택합니다.
4. 연락처 정보 섹션에서 편집을 선택합니다.
5. 개인 정보 보호 섹션에서 연락처 정보를 숨길지 여부를 선택합니다. 관리자, 등록자, 기술 담당자, 청구 담당자 4명의 연락처에 대해 모두 동일한 개인 정보 설정을 지정해야 합니다.

> **Note**
>
> TLD에서 개인 정보 보호가 지원되지 않는 경우 개인 정보 보호 섹션이 표시되지 않습니다.

6. Save changes(변경 사항 저장)를 선택합니다.
7. 개인 정보 보호를 활성화하거나 비활성화하는 동안 문제가 발생하면 AWS Support에 무료로 문의할 수 있습니다. 자세한 내용은 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.

도메인 자동 갱신 활성화 또는 비활성화

만료 날짜 직전에 Amazon Route 53가 도메인 등록을 자동으로 갱신할지 여부를 변경하거나 자동 갱신의 현재 설정을 보려면 다음 절차를 수행하세요.

도메인에 대한 등록 갱신 요금은 AWS 크레딧을 사용하여 지불할 수 없습니다.

> **Note**
>
> AWS 계정을 취소하려면 자동 갱신을 꺼야 합니다. 그렇지 않으면에서 갱신 알림을 계속 받게 됩니다 AWS. 하지만 계정을 다시 활성화하지 않는 한 도메인은 갱신되지 않습니다.

도메인 자동 갱신을 활성화 또는 비활성화하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 등록된 도메인을 선택합니다.
3. 업데이트하려는 도메인의 이름을 선택합니다.
4. 세부 정보 섹션의 작업 드롭다운에서 자동 갱신 켜기를 선택합니다.

   <domain name>에 자동 갱신 켜기?에서 연간 요금 지불에 동의하고 켜기를 선택합니다.

   > **Note**
   >
   > 나열된 가격은 현재 등록 기간 기준이며 변경될 수 있습니다. 자세한 내용은 Amazon Route 53 도메인 등록 요금을 참조하세요.

5. 자동 갱신을 끄려면 작업 드롭다운에서 자동 갱신 끄기를 선택합니다.
6. 자동 갱신을 활성화하거나 비활성화하는 동안 문제가 발생하면 AWS Support에 무료로 문의할 수 있습니다. 자세한 내용은 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.

다른 등록 대행자로의 무단 이전을 방지하기 위해 도메인 잠그기

모든 일반 TLD 및 대다수 지리적 TLD의 도메인 등록 기관에서는 다른 사람이 허가 없이 도메인을 다른 등록 대행자로 이전하지 못하도록 도메인을 잠글 수 있습니다. 도메인의 등록 기관에서 도메인을 잠글 수 있는지 여부를 확인하려면 Amazon Route 53에 등록할 수 있는 도메인 단원을 참조하십시오. 잠금이 지원되고 도메인을 잠그려는 경우 다음 절차를 수행합니다. 도메인을 다른 등록 대행자에게 이전하고 싶다면 잠금 비활성화 절차를 사용할 수도 있습니다.

다른 등록 대행자로의 무단 이전을 방지하기 위해 도메인을 잠그려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 [Registered Domains]를 선택합니다.
3. 업데이트하려는 도메인의 이름을 선택합니다.
4. 세부 정보 섹션의 작업 드롭다운에서 이전 잠금을 켜기 또는 끄기 중에서 원하는 바에 따라 이전 잠금 켜기 또는 이전 잠금 끄기를 선택합니다.

   요청 페이지로 이동하여 요청의 진행 상황을 확인할 수 있습니다.
5. 도메인을 잠그는 동안 문제가 발생하면 무료로 AWS Support에 문의할 수 있습니다. 자세한 내용은 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.

WHOIS 검색에서 이 상태는 `clientTransferProhibited`로 표시됩니다. 일부 TLD에는 다음과 같은 상태가 더 있을 수 있습니다.

- `clientUpdateProhibited`
- `clientDeleteProhibited`

도메인의 등록 기간 연장

Amazon Route 53에 도메인을 등록하거나 도메인 등록을 Route 53,으로 이전할 때 도메인이 자동 갱신되도록 구성합니다. 일부 TLD(최상위 도메인) 등록 기관의 갱신 기간은 더 길지만, 자동 갱신 기간은 보통 1년입니다.

다음 사항에 유의하세요.

최대 갱신 기간

모든 일반 TLD와 많은 국가 코드 TLD를 통해 도메인 등록을 장기간(일반적으로 1년씩 연장하여 최대 10년) 연장할 수 있습니다. 도메인의 등록 기간을 연장할 수 있는지 알아보려면 Amazon Route 53에 등록할 수 있는 도메인 단원을 참조하십시오. 등록 기간을 연장할 수 있는 경우 다음 절차를 수행합니다.

도메인 등록을 갱신하거나 연장할 수 있는 시기에 대한 제한

일부 TLD 등록 기관에는 도메인 등록을 갱신하거나 연장할 수 있는 시기에 제한이 있습니다(예: 도메인이 만료되기 2개월 전). 등록 기관에서 도메인 등록 기간 연장을 허용하더라도 도메인이 만료되기 며칠 전에는 허용하지 않을 수 있습니다.

AWS 크레딧

도메인의 등록 기간 연장에 대한 요금을 지불하는 데 AWS 크레딧을 사용할 수 없습니다.

도메인의 등록 기간을 연장하려면

1. https://console.aws.amazon.com/route53/에서 Route 53 콘솔을 엽니다.
2. 탐색 창에서 [Registered Domains]를 선택합니다.
3. 등록 기간을 연장할 도메인의 이름을 선택합니다.
4. 세부 정보 섹션의 작업 드롭다운에서 도메인 등록 갱신을 선택합니다.
5. 도메인 등록 갱신 대화 상자의 갱신 기간 드롭다운에서 등록을 연장할 연수를 선택합니다.

   목록에 이 도메인의 현재 만료 날짜와 등록 기관에서 허용한 최대 등록 기간에 따라 모든 현재 옵션이 표시됩니다. 해당 연수가 적용된 만료일이 기간 아래에 나열됩니다.
6. 도메인 등록 갱신을 선택합니다.

   레지스트리로부터 만료 날짜가 업데이트되었다는 확인을 받으면 만료 날짜를 변경했음을 확인할 수 있도록 사용자에게 이메일을 보냅니다.
7. 도메인의 등록 기간을 연장하는 동안 문제가 발생하면 AWS Support에 무료로 문의할 수 있습니다. 자세한 내용은 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.

다른 등록자를 사용하도록 이름 서버를 업데이트합니다.

DNS 관리를 다른 등록자로 이동하려면 다음을 가리키도록 이름 서버를 업데이트해야 합니다.

다른 DNS 서비스를 이용하고자 할 때 도메인에 대한 이름 서버를 업데이트하려면

1. DNS 서비스가 제공하는 프로세스를 이용해 도메인에 대한 이름 서버를 얻습니다.
2. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
3. 탐색 창에서 등록된 도메인을 선택합니다.
4. 다른 DNS 서비스를 사용하도록 구성하고자 하는 도메인의 이름을 선택합니다.
5. 세부 정보 섹션의 작업 드롭다운 아래에서 이름 서버 편집을 선택합니다.
6. 기존 이름 서버를 삭제하면 이름 서버의 이름을 1단계의 DNS 서비스로부터 얻은 이름 서버에 추가합니다.
7. Save changes(변경 사항 저장)를 선택합니다.
8. (선택 사항) 도메인을 등록할 때 Route 53가 자동으로 생성한 호스팅 영역을 삭제합니다. 이렇게 하면 사용하고 있지 않은 호스팅 영역에 요금이 부과되지 않습니다.

    a. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
    b. 도메인과 이름이 같은 호스팅 영역에 대해 라디오 버튼을 선택합니다.
    c. [Delete Hosted Zone]을 선택합니다.
    d. [Confirm]을 선택해 호스팅 영역을 삭제하고자 한다는 것을 확인합니다.

도메인의 글루 레코드 및 이름 서버 추가 또는 변경

Route 53으로 도메인을 등록하면 도메인의 호스팅 영역을 자동으로 생성하고, 네 개의 이름 서버를 호스팅 영역에 할당한 다음 해당 이름 서버를 사용하도록 도메인 등록을 업데이트합니다. 다른 DNS 서비스를 사용하거나 화이트 레이블 이름 서버를 사용하려는 경우가 아니면 일반적으로 이러한 설정을 변경할 필요가 없습니다.

Route 53의 도메인당 이름 서버의 최대 수는 6개입니다.

> **Warning**
>
> 이름 서버를 잘못된 값으로 변경하거나 글루 레코드에 잘못된 IP 주소를 지정하거나 새 이름 서버를 지정하지 않고 1개 이상의 이름 서버를 삭제한 경우에는 인터넷에서 웹 사이트 또는 애플리케이션에 최대 2일 동안 접속하지 못할 수 있습니다.

주제

이름 서버 및 글루 레코드 변경 시 고려 사항

구성을 변경하기 전에 다음 문제를 고려하십시오.

주제

- You want to make Route 53 the DNS service for your domain
- You want to use another DNS service
- You want to use white-label name servers
- You're changing name servers for a .it domain

Route 53를 도메인의 DNS 서비스로 사용하려는 경우

현재 다른 DNS 서비스를 사용 중이고 Route 53를 도메인의 DNS 서비스로 사용하려는 경우, DNS 서비스를 Route 53으로 마이그레이션하는 방법에 대한 자세한 지침은 Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정 섹션을 참조하세요.

> **Important**
>
> 마이그레이션 프로세스에 철저히 따르지 않을 경우, 최대 2일 동안 인터넷에서 도메인에 접속하지 못할 수 있습니다.

다른 DNS 서비스를 사용하려는 경우

도메인에 Route 53 이외의 DNS 서비스를 사용하려면 다음 절차에 따라 도메인 등록의 이름 서버를 다른 DNS 서비스에서 제공하는 이름 서버로 변경하세요.

> **Note**
>
> 이름 서버를 변경하고 Route 53가 다음 오류 메시지를 반환하면 TLD의 등록처가 유효한 이름 서버로 지정한 이름 서버를 인식하지 못합니다.
> `"We're sorry to report that the operation failed after we forwarded your request to our registrar associate. This is`

```
because: One or more of the specified name servers are not known
to the domain registry."
```

TLD 등록처는 공용 DNS 서비스에서 제공하는 이름 서버를 일반적으로 지원하지만 등록처에 해당 이름 서버의 IP 주소가 없는 경우 Amazon EC2 인스턴스에서 구성한 DNS 서버와 같은 개인 DNS 서버는 지원하지 않습니다. Route 53는 TLD 등록처에서 인식하지 못하는 이름 서버 사용을 지원하지 않습니다. 이 오류가 발생하면 Route 53 또는 다른 퍼블릭 DNS 서비스의 이름 서버로 변경해야 합니다.

화이트 레이블 이름 서버를 사용하려는 경우

이름 서버의 이름을 도메인 이름의 하위 도메인으로 지정하기 위해 화이트 라벨 이름 서버를 만들 수 있습니다. (화이트 레이블 이름 서버는 가상 이름 서버 또는 프라이빗 이름 서버라고도 합니다.) 예를 들어 example.com 도메인에 대해 ns1.example.com에서 ns4.example.com까지 이름 서버를 만들 수 있습니다. 화이트 레이블 이름 서버를 사용하려면 다음 절차에 따라 이름 대신 이름 서버의 IP 주소를 지정하십시오. 이러한 IP 주소를 글루 레코드라고 합니다.

화이트 레이블 이름 서버를 구성하는 방법에 대한 자세한 내용은 화이트 레이블 이름 서버 구성 단원을 참조하십시오.

.it 도메인의 이름 서버를 변경하는 경우

IT 도메인의 이름 서버는 DNS 확인을 통과해야 합니다. 변경 요청을 제출하기 전에 https://dns-check.nic.it/에서 이름 서버를 확인하는 것이 좋습니다. 변경하기 전 이름 서버를 사용하여 등록처가 계속 DNS 쿼리에 응답합니다. 이전 이름 서버를 더 이상 사용할 수 없으면 인터넷에서 해당 도메인을 사용할 수 없게 됩니다.

> **Important**
>
> 도메인의 이름 서버를 변경할 때마다 이전의 DNS 서비스를 취소하거나 이전의 이름 서버가 사용된 Route 53 호스팅 영역을 삭제하기 전에 새 이름 서버를 사용하여 DNS가 쿼리에 응답하는지 확인하세요.

에서 .it 도메인에 대한 레지스트리를 사용하여 이름 서버의 이름을 수정 AWS 하는 방법에 대한 자세한 내용은 섹션을 참조하세요도메인 등록 문제에 대한 AWS 지원 문의.

이름 서버 또는 글루 레코드 추가 또는 변경

이름 서버 또는 글루 레코드를 추가하거나 변경하려면 다음 절차를 수행하십시오.

> **Note**
>
> 기본적으로 DNS 해석기는 보통 2일 동안 이름 서버의 이름을 캐시합니다. 따라서 변경 사항이 적용되기까지 2일이 걸릴 수 있습니다. 자세한 내용은 Amazon Route 53가 도메인의 트래픽을 라우팅하는 방법 단원을 참조하십시오.

도메인의 이름 서버 또는 글루 레코드를 추가하거나 변경하려면

1. 이름 서버 및 글루 레코드 변경 시 고려 사항을 검토하여 해당되는 문제가 있다면 처리합니다.
2. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
3. 탐색 창에서 등록된 도메인을 선택합니다.
4. 설정을 편집하고자 하는 도메인의 이름을 선택합니다.
5. 세부 정보 섹션의 작업 드롭다운에서 이름 서버 편집을 선택합니다.
6. 이름 서버 편집 대화 상자에서 다음 작업을 수행할 수 있습니다.

   - 다음 중 하나를 수행하여 도메인의 DNS 서비스 변경
     - 다른 DNS 서비스의 이름 서버를 Route 53 호스팅 영역의 이름 서버로 바꾸기
     - Route 53 호스팅 영역의 이름 서버를 다른 DNS 서비스의 이름 서버로 바꾸기
     - Route 53 호스팅 영역 하나의 이름 서버를 다른 Route 53 호스팅 영역의 이름 서버로 바꾸기

     도메인의 DNS 서비스 변경에 대해서는 Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정을 참조하십시오. 도메인의 DNS 서비스로 사용하려는 Route 53 호스팅 영역의 이름 서버를 얻는 방법에 대해서는 퍼블릭 호스팅 영역에 대한 이름 서버 가져오기 섹션을 참조하세요.
   - 1개 이상의 이름 서버 추가.
   - 기본 이름 서버 이름 교체.
   - 화이트 레이블 이름 서버를 지정하는 경우, 글루 레코드에서 IP 주소를 추가하거나 변경합니다. 주소를 IPv4 또는 IPv6 형식으로 입력할 수 있습니다. 한 이름 서버에 여러 IP 주소가 있는 경우 각 주소를 별도의 줄에 입력합니다.

     화이트 레이블 이름 서버에는 ns1.example.com과 같은 이름 서버의 이름에 example.com과 같은 도메인 이름이 포함됩니다. 화이트 레이블 이름 서버를 지정하면 Route 53는 이름 서버의 IP

주소를 하나 이상 지정하라는 메시지를 표시합니다. 이 IP 주소를 글루 레코드라고 합니다. 자세한 내용은 화이트 레이블 이름 서버 구성 단원을 참조하십시오.

- 이름 서버 삭제. 해당 이름 서버에 대한 필드 오른쪽에 있는 x 아이콘을 선택합니다.

> **Warning**
>
> 이름 서버를 잘못된 값으로 변경하거나 글루 레코드에 잘못된 IP 주소를 지정하거나 새 이름 서버를 지정하지 않고 1개 이상의 이름 서버를 삭제한 경우에는 인터넷에서 웹 사이트 또는 애플리케이션에 최대 2일 동안 접속하지 못할 수 있습니다.

7. 업데이트를 선택합니다.
8. 이름 서버 또는 글루 레코드를 추가하거나 변경하는 동안 문제가 발생하면 AWS Support에 무료로 문의할 수 있습니다. 자세한 내용은 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.

도메인 등록 갱신

Amazon Route 53에 도메인을 등록하거나 도메인 등록을 Route 53,으로 이전할 때 도메인이 자동 갱신되도록 구성합니다. 일부 TLD(최상위 도메인) 등록 기관의 갱신 기간은 더 길지만, 자동 갱신 기간은 보통 1년입니다. TLD의 등록 및 갱신 기간은 Amazon Route 53에 등록할 수 있는 도메인을 참조하십시오.

> **Note**
>
> 도메인 등록 갱신에 대한 요금을 지불하기 위해 AWS 크레딧을 사용할 수 없습니다.

대부분의 최상위 도메인(TLD)의 경우 도메인의 만료 날짜를 변경할 수 있습니다. 자세한 내용은 도메인의 등록 기간 연장 섹션을 참조하세요.

> **Important**
>
> 자동 갱신을 해제하는 경우 도메인에 미치는 다음 효과를 고려하십시오.
>
> - 일부 TLD 등록 기관은 사용자가 충분히 일찍 갱신하지 않을 경우 만료 날짜 이전에도 도메인을 삭제합니다. 도메인 이름을 유지하려면 반드시 자동 갱신을 활성화한 상태로 두는 것이 좋습니다.

- 또한, 도메인이 만료된 후 도메인을 다시 등록하지 마십시오. 어떤 등록 기관에서는 도메인 만료 직후에 다른 사람이 도메인을 등록하도록 허용하므로, 다른 사람이 해당 도메인을 점유하기 전에 다시 등록하지 못할 수도 있습니다.
- 어떤 등록 기관에서는 만료된 도메인을 복원하는 데 비싼 할증료를 청구합니다.
- 만료 날짜 또는 그에 가까운 날짜에 인터넷에서 도메인을 사용할 수 없게 됩니다.

자신의 도메인에 대해 자동 갱신이 활성화되어 있는지 확인하려면 다음(도메인 자동 갱신 활성화 또는 비활성화)을 참조하십시오.

자동 갱신이 활성화되어 있는 경우에는 다음과 같이 적용됩니다.

만료 45일 전

등록자 연락처로 이메일을 보내어 현재 자동 갱신이 활성화되어 있음을 알려주고 이를 비활성화하는 방법을 제공합니다. 이 이메일을 놓치지 않도록 등록자 연락 이메일 주소를 최신 상태로 유지하십시오.

만료 35일 또는 30일 전

.com.ar, .com.br 및 .jp 도메인을 제외한 모든 도메인에 대해, 도메인 이름이 만료되기 전에 갱신 관련 문제를 해결할 시간을 확보하도록 만료 날짜 35일 전에 도메인 등록을 갱신합니다.

.com.ar, .com.br 및 .jp 도메인에 대한 등록의 경우 만료 전 30일 이내에 도메인을 갱신해야 합니다. 당사의 등록 대행 협력사인 Gandi로부터 만료 30일 전에 갱신 이메일을 받게 되고, 사용자 도메인의 자동 갱신이 활성화되어 있는 경우 같은 날에 도메인을 갱신합니다.

> **Note**
>
> 도메인을 갱신할 때 이를 알리는 이메일을 보내 드립니다. 갱신에 실패한 경우 그 이유를 설명하는 이메일을 보내 드립니다.

자동 갱신이 비활성화되어 있는 경우 도메인 이름 만료 날짜가 다가옴에 따라 다음과 같이 적용됩니다.

만료 45일 전

도메인 등록자 연락처로 이메일을 보내어 현재 자동 갱신이 비활성화되어 있음을 알려주고 이를 활성화하는 방법을 제공합니다. 이 이메일을 놓치지 않도록 등록자 연락 이메일 주소를 최신 상태로 유지하십시오.

만료 30일 및 7일 전

도메인에 대한 자동 갱신을 비활성화한 경우 도메인 등록 관리 기관인 ICANN에서 등록 대행자에게 이메일을 보내도록 요구합니다. 이메일은 다음 이메일 주소 중 하나에서 발송합니다.

- noreply@registrar.amazon - 등록 기관이 Amazon Registrar인 도메인의 경우.
- noreply@domainnameverification.net - 등록 기관이 당사의 등록 기관 협력사 Gandi인 도메인의 경우.

TLD의 등록 기관을 확인하려면 Amazon Route 53에 등록할 수 있는 도메인을 참조하세요.

만료까지 30일 미만으로 남은 시점에 자동 갱신을 활성화하고 갱신 기간이 지나지 않았다면, 해당 도메인을 24시간 내에 갱신합니다.

> **Important**
>
> 일부 TLD 레지스트리는 도메인을 갱신할 수 있는 시기에 제한이 있습니다. 해당 도메인에 대한 자세한 내용은 Amazon Route 53에 등록할 수 있는 도메인 섹션을 참조하세요. 그 밖에도, 갱신을 처리하는 데 최장 하루가 걸릴 수 있습니다. 자동 갱신을 활성화하기 전에 지연이 너무 길어질 경우 갱신 처리를 할 수 있기 전에 도메인이 만료되어 해당 도메인을 잃을 수도 있습니다. 만료 날짜가 다가오는 경우 도메인의 만료 날짜를 수동으로 연장하는 것이 좋습니다. 자세한 내용은 도메인의 등록 기간 연장 단원을 참조하십시오.

갱신 기간에 대한 자세한 내용은 Amazon Route 53에 등록할 수 있는 도메인의 TLD에 대한 Deadlines for renewing and restoring domains 섹션을 참조하세요.

만료 날짜 후

대부분의 도메인은 만료 후 짧은 시간 동안 등록자가 보유하므로 만료 날짜 후에는 만료된 도메인을 갱신하지 못할 수도 있습니다. 따라서 도메인을 유지하려면 자동 갱신을 활성화한 상태로 유지하는 것이 좋습니다. 만료 날짜 후의 도메인 갱신에 대한 자세한 내용은 다음(만료되거나 삭제된 도메인 복원)을 참조하십시오.

도메인이 만료되었지만 추가 기간에 갱신이 가능한 경우 표준 갱신 요금으로 도메인을 갱신할 수 있습니다. 도메인이 추가 갱신 기간에 포함되는지 확인하려면 도메인의 등록 기간 연장 단원의 절차를 수행하십시오. 도메인이 목록에 아직 있으면 아직 추가 갱신 기간이 지나지 않은 것입니다.

갱신 기간에 대한 자세한 내용은 Amazon Route 53에 등록할 수 있는 도메인의 TLD에 대한 Deadlines for renewing and restoring domains 섹션을 참조하세요.

만료되거나 삭제된 도메인 복원

추가 갱신 기간 내에 도메인을 갱신하지 않거나 도메인을 부주의로 삭제한 경우, 다른 사용자가 해당 도메인을 등록하기 전에 상위 도메인(TLD)의 일부 레지스트리를 사용하여 도메인을 복원할 수 있습니다.

도메인이 삭제되거나 도메인 추가 갱신 기간이 끝나면 Amazon Route 53 콘솔에 나타나지 않습니다.

> **Important**
>
> 도메인을 복원하는 요금은 일반적으로 비싸며, 경우에 따라 도메인을 등록하거나 갱신하는 요금보다 훨씬 비쌉니다. 현재 도메인 복원 요금을 확인하려면 Amazon Route 53 도메인 등록 요금에서 복원 요금 열을 참조하세요.

만료된 도메인 복원에 대한 요금을 지불하는 데 AWS 크레딧을 사용할 수 없습니다.

도메인이 삭제되거나 추가 갱신 기간이 만료된 후 도메인 등록 복원을 시도하려면

1. 도메인의 TLD 레지스트리가 도메인 복원을 지원하는지 확인한 후, 지원하면 복원이 가능한 기간을 확인합니다.

   a. Amazon Route 53에 등록할 수 있는 도메인로 이동합니다.
   b. 도메인에 대한 TLD를 찾고 도메인 갱신 및 복원 기한 섹션의 값을 검토합니다.

   > **Important**
   >
   > 복원 요청은 Gandi로 전달되며, Gandi는 월요일에서 금요일까지 영업 시간 중에 접수된 요청을 처리합니다. Gandi는 파리를 소재지로 하며, UTC/GMT +1시간의 표준 시간대가 적용됩니다. 따라서 요청을 제출하는 시간에 따라 드물긴 해도 요청이 처리되기까지 1주일 이상 걸릴 수도 있습니다.

2. 도메인 복원 요금을 검토합니다. 이 요금은 종종 비싸며, 경우에 따라 도메인을 등록하거나 갱신하는 요금보다 훨씬 비쌉니다. Amazon Route 53 도메인 등록 요금에서 도메인의 TLD(예: .com)를 찾고 복원 요금 열에서 요금을 확인합니다. 그래도 도메인을 복원하고 싶으면 요금을 기록해 두십시오. 이후의 단계에서 필요합니다.
3. 도메인이 등록된 AWS 계정을 사용하여 AWS 지원 센터에 로그인합니다.
4. 다음 값을 지정하세요.

관련

계정 및 청구의 기본값을 수락합니다.

Service

도메인의 기본값을 수락합니다.

범주

복원의 기본값을 수락합니다.

심각도

일반 질문의 기본값을 수락합니다.

다음 단계: 추가 정보(Next step: Additional information)를 선택합니다

제목

Restore an expired domain(만료된 도메인 복원하기) 또는 Restore a deleted domain(삭제된 도메인 복원하기)을 입력합니다.

설명

다음 정보를 제공합니다.

- 복원하려는 도메인
- 도메인이 등록된 계정의 12자리 계정 ID입니다. AWS
- 도메인 복원 요금에 동의한다는 확인. 다음 텍스트를 사용합니다.

  "I agree to the price of $____ for restoring my domain."("도메인 등록 요금 $____에 동의합니다.")

  2단계에서 확인한 요금을 빈 칸에 기입합니다.

연락 방법

연락 방법을 지정하고 해당 정보를 입력합니다.

5. 제출을 선택합니다.
6. 도메인을 복원할 수 있는지 여부를 알게 되면 AWS Support 담당자가 연락을 드릴 것입니다. 또한 복원 가능한 도메인은 콘솔에 다시 나타납니다. 만료 날짜는 도메인이 만료되었거나 실수로 삭제되었는지 여부에 따라 달라집니다.

도메인 만료

새 만료 날짜는 일반적으로 이전 만료 날짜로부터 1년 또는 2년(TLD에 따라 다름)입니다.

> **Note**
>
> 새 만료 날짜는 도메인이 복구된 날짜로부터 계산되지 않습니다.

도메인이 실수로 삭제됨

만료 날짜는 일반적으로 변경되지 않습니다.

Route 53에 등록된 도메인의 호스팅 영역 바꾸기

도메인의 호스팅 영역을 삭제한 경우, 인터넷에서 도메인을 사용 가능하도록 설정하려면 다른 호스팅 영역을 만들어야 합니다. 다음 절차를 수행합니다.

도메인의 호스팅 영역을 바꾸려면

1. 퍼블릭 호스팅 영역을 만듭니다. 자세한 내용은 퍼블릭 호스팅 영역 생성 섹션을 참조하세요.
2. 호스팅 영역에 레코드를 생성합니다. 레코드는 도메인(example.com)과 하위 도메인(acme.example.com, zenith.example.com)에 대한 트래픽을 라우팅하는 방법을 정의합니다. 자세한 내용은 레코드 작업 섹션을 참조하세요.
3. 새로운 호스팅 영역의 네임 서버를 사용하도록 도메인 구성을 업데이트합니다. 자세한 내용은 도메인의 글루 레코드 및 이름 서버 추가 또는 변경 섹션을 참조하세요.

   > **Important**
   >
   > 호스팅 영역을 생성할 때 Route 53는 호스팅 영역에 4개의 이름 서버를 할당합니다. 호스팅 영역을 삭제한 후 만들면 Route 53에서 다른 4개의 이름 서버를 할당합니다. 일반적으로 새 호스팅 영역의 이름 서버는 이전 호스팅 영역의 이름 서버와 일치하는 것이 없습니다. 새 호스팅 영역의 이름 서버를 사용하도록 도메인 구성을 업데이트하지 않으면 도메인은 인터넷에서 사용할 수 없는 상태로 유지됩니다.

4. 도메인의 호스팅 영역을 교체하는 동안 문제가 발생하면 AWS Support에 무료로 문의할 수 있습니다. 자세한 내용은 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.

도메인 이전

도메인 등록을 다른 등록 기관에서 Amazon Route 53으로, 한 AWS 계정에서 다른 으로 또는 Route 53에서 다른 등록 기관으로 이전할 수 있습니다. 한 계정에서 다른 AWS 계정으로 도메인을 이전하는 데 드는 비용은 없습니다.

이 섹션의 이 주제에서는 도메인 이전과 관련된 다음 주제를 다룹니다.

1. 도메인 등록을 Amazon Route 53으로 이전하기
   - 사전 조건, 권한 부여 코드, DNS 설정 업데이트를 포함하여 도메인을 다른 등록 기관에서 Route 53으로 이전하는 단계별 절차를 알아봅니다.
   - 도메인 이전이 만료 날짜와 다양한 최상위 도메인(TLD)에 대한 고려 사항에 미치는 영향을 이해합니다.
2. 도메인 이전 상태 보기
   - 도메인 이전 요청의 상태와 이전 프로세스 중에 서로 다른 상태 코드의 의미를 확인하는 방법을 알아봅니다.
3. Amazon Route 53으로 도메인을 이전할 때 도메인 등록에 대한 만료 날짜에 미치는 영향
   - 도메인을 Route 53으로 이전하는 것이 도메인의 만료 날짜에 어떤 영향을 미칠 수 있는지 알아봅니다.
4. 도메인을 다른 AWS 계정으로 이전
   - 이전을 시작하고 수락하는 데 필요한 역할 및 권한을 포함하여 한 계정에서 다른 AWS 계정으로 도메인을 이전하는 방법을 알아봅니다.
   - 도메인 이전 후 호스팅 영역을 새 계정으로 마이그레이션하는 선택적 단계에 대해 알아봅니다.
5. Amazon Route 53에서 다른 등록 기관으로 도메인 이전하기
   - 권한 부여 코드 가져오기, DNS 설정 업데이트, 확인 이메일 응답 등 Route 53에서 다른 등록 기관으로 도메인을 이전하는 프로세스를 이해합니다.
   - DNS 서비스를 다른 제공업체로 이전할 때 고려해야 할 사항과 별칭 레코드 및 라우팅 정책과 같은 Route 53 관련 기능에 미칠 수 있는 잠재적 영향에 유의합니다.

위에 나열된 항목의 정보를 따르면 Route 53에서 도메인을 효과적으로 이전하고, 이전 프로세스를 관리하고, 적절한 DNS 구성 및 라우팅을 유지하면서 원활한 전환을 보장할 수 있습니다.

도메인 등록을 Amazon Route 53으로 이전하기

> **Important**
>
> .cc 및 .tv를 제외한 모든 국가 코드 최상위 도메인(ccTLD)을 Route 53으로 이전하는 동안 소유자 연락처에 대한 업데이트는 사용되지 않고 레지스트리의 소유자 연락처 데이터가 사용됩니다. 이전이 완료된 후 소유자 연락처 정보를 업데이트할 수 있습니다. 자세한 내용은 도메인 연락처 정보 및 소유권 업데이트 단원을 참조하십시오.

도메인 등록을 Amazon Route 53으로 이전하려면 이 주제의 절차를 따릅니다.

> **Important**
>
> 한 단계라도 건너뛰면 인터넷에서 도메인을 사용하지 못할 수 있습니다.

다음 사항에 유의하세요.

AWS 지원 문의

도메인을 전송하는 동안 문제가 발생하면 AWS Support에 무료로 문의할 수 있습니다. 자세한 내용은 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.

만료 날짜

도메인 이전이 현재 만료 날짜에 미치는 영향에 대한 자세한 내용은 다음(Amazon Route 53으로 도메인을 이전할 때 도메인 등록에 대한 만료 날짜에 미치는 영향)을 참조하십시오.

이전 요금

도메인을 Route 53으로 이전할 때 AWS 계정에 적용되는 이전 요금은 .com 또는 .org와 같은 최상위 도메인에 따라 달라집니다. 자세한 내용은 Route 53 요금을 참조하세요.

Route 53으로 도메인을 이전하는 경우 AWS 크레딧을 사용하여 요금을 지불할 수 없습니다.

> **Note**
>
> Route 53에서는 이전 프로세스를 시작하기 전에 도메인 이전에 대한 요금이 부과됩니다. 어떤 이유로든 이전이 실패하면 그 즉시 이전 비용을 크레딧으로 환불해드립니다.

특별 및 프리미엄 도메인 이름

TLD는 일부 도메인 이름에 특별 또는 프리미엄 가격을 지정하고 있습니다. 특별 또는 프리미엄 가격이 적용되는 도메인은 Route 53로 이전할 수 없습니다.

도메인 할당량

AWS 계정당 기본 최대 도메인 수는 20개입니다. 더 높은 할당량을 요청할 수 있습니다. 자세한 내용은 도메인에 대한 할당량 단원을 참조하십시오.

이름 서버 제한

Route 53의 도메인당 이름 서버의 최대 수는 6개입니다.

주제

최상위 도메인에 따른 이전 요건

대부분의 도메인 등록 대행자는 도메인을 다른 등록 대행자로 이전할 때 요구 사항을 적용합니다. 이러한 요구 사항의 주요 목적은 사기 도메인의 소유자가 도메인을 다른 등록 대행자로 반복해서 이전하지 못하도록 하는 것입니다. 요구 사항은 다양하지만, 일반적인 요구 사항은 다음과 같습니다.

- 적어도 60일 전에 현재 등록 대행자에 도메인을 등록하거나 현재 등록 대행자에 도메인 등록을 이전해야 합니다.
- 도메인 이름에 대한 등록이 만료되어 복원해야 하는 경우에는 최소 60일 전에 복원해야 합니다.
- 그 도메인은 다음 도메인 이름 상태 코드 중 어떤 것도 가질 수 없습니다.
  - clientTransferProhibited
  - pendingDelete
  - pendingTransfer

  - redemptionPeriod
  - serverTransferProhibited
- 일부 최상위 도메인 등록 기관은 도메인 소유자 변경과 같은 변경이 완료될 때까지 이전을 허용하지 않습니다.

도메인 이름 상태 코드의 현재 목록과 각 코드의 의미에 대한 설명을 보려면 ICANN 웹 사이트로 가서 EPP status codes를 검색합니다. ICANN 웹 사이트에서 검색하십시오. 웹 검색 시 때로는 지난 버전의 문서가 표시될 수도 있습니다.

> **Note**
>
> ICANN은 도메인 이름 등록 및 이전 관련 정책을 수립하는 조직입니다.

Whois용 웹 사이트에서 도메인 이름을 검색하여 도메인에 대한 상태 코드 및 기타 정보를 확인할 수도 있습니다.

1단계: Amazon Route 53가 최상위 도메인을 지원하는지 확인

Amazon Route 53에 등록할 수 있는 도메인을 참조하세요. 이전하려는 도메인의 최상위 도메인이 목록에 있다면 도메인을 Amazon Route 53으로 이전할 수 있습니다.

TLD가 목록에 없다면 현재는 도메인 등록을 Route 53으로 이전할 수 없습니다. 수시로 목록에 TLD가 추가되므로 이후에라도 도메인에 대한 지원이 추가됐는지 확인하십시오.

2단계(선택 사항): DNS 서비스를 Amazon Route 53 또는 다른 DNS 서비스 공급자로 이전

DNS를 먼저 이전해야 하는 이유

일부 등록 기관은 Route 53로부터 도메인 등록 이전을 요청을 수신하는 즉시 사용 중지될 수 있는 무료 DNS 서비스를 제공합니다. Route 53에서 도메인에 대한 DNS 서비스를 제공하도록 하려면 Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정 섹션을 참조하세요.

3단계: 현재 등록 대행자에 대한 설정 변경

현재 등록 기관에서 제공하는 방법을 사용해 이전하고자 하는 각 도메인마다 다음 작업을 각각 수행하세요.

- Confirm that the email for the registrant contact for your domain is up to date
- Unlock the domain so it can be transferred
- Confirm that the domain status allows you to transfer the domain
- Disable DNSSEC for the domain
- Get an authorization code
- Renew your domain registration before you transfer the domain (selected geographic TLDs)

도메인의 등록자 연락처 이메일이 최신인지 확인합니다

이전 승인을 요청하기 위해 해당 이메일 주소로 이메일을 보내드리겠습니다. 이전 권한을 부여하려면 이메일에 포함된 링크를 클릭해야 합니다. 링크를 클릭하지 않으면 이전을 취소합니다.

> **Important**
>
> 등록자로 나열하는 연락처는 ICANN 전송 정책에 따라 도메인 이름의 등록 이름 보유자로 특정 권한을 갖습니다. 대부분의 도메인은 종료 시 삭제되지만 AWS 계정 (자세한 내용은 참조내 AWS 계정이 닫히거나 영구적으로 닫히고 내 도메인이 Route 53에 등록됨) 도메인이 종료된 계정에 남아 있는 경우 등록자로 등록된 연락처는 외부 등록 기관으로 도메인 이름 이전을 요청할 수 있습니다. 따라서 나열한 등록자 연락처가 자신 또는 책임감 있게 행동할 것으로 신뢰하는 다른 사람이어야 합니다.

도메인의 잠금을 해제하여 이전할 수 있게 합니다

도메인 등록 관리 기관인 ICANN은 도메인 이전에 앞서 도메인 잠금을 해제할 것을 요구합니다.

도메인 상태가 도메인 이전을 허용한다는 것을 확인합니다

자세한 내용은 최상위 도메인에 따른 이전 요건 섹션을 참조하세요.

도메인의 DNSSEC를 비활성화합니다

도메인과 함께 DNSSEC를 사용하고 도메인 등록을 Route 53으로 이전하는 경우 먼저 이전 등록 기관에서 DNSSEC를 비활성화해야 합니다. 그런 다음 도메인 등록을 이전한 후 Route 53에서 도메인에 대한 DNSSEC를 설정하는 단계를 수행합니다. Route 53는 도메인 등록 및 DNSSEC 서명을 위해 DNSSEC를 지원합니다. 자세한 내용은 Amazon Route 53에서 DNSSEC 서명 구성 섹션을 참조하세요.

> **Important**
>
> DNSSEC가 구성된 동안 도메인 등록을 Route 53으로 이전하면 DNSSEC 퍼블릭 키도 이전됩니다. DNS 서비스를 DNSSEC를 지원하지 않는 다른 공급자에게 전송하는 경우, 도메인에서 DNSSEC 키를 삭제할 때까지 DNS 해석이 간헐적으로 실패합니다. 자세한 내용은 도메인의 퍼블릭 키 삭제 섹션을 참조하세요.

권한 부여 코드를 얻습니다

현재 등록 기관의 인증 코드로 해당 도메인에 대한 등록을 Route 53으로 이전하도록 요청할 수 있습니다. 절차 후반에 Route 53 콘솔에 이 코드를 입력할 것입니다.

일부 최상위 도메인에는 추가 요건이 있습니다.

.co.za 도메인

.co.za 도메인을 Route 53로 이전하는 데는 권한 부여 코드가 필요하지 않습니다.

.uk, .co.uk, .me.uk 및 .org.uk 도메인

.uk, .co.uk, .me.uk 또는 .org.uk 도메인을 Route 53으로 이전할 경우, 권한 부여 코드를 얻지 않아도 됩니다. 대신에 현재 도메인 등록 대행자가 제공하는 방법을 사용해 도메인에 대한 IPS 태그의 값을 [GANDI](모두 대문자)로 업데이트합니다. (IPS 태그는 .uk 도메인 이름 등록부인 Nominet에 필요한 것입니다). 등록 대행사가 IPS 태그의 값을 변경하지 않으려 하면 Nominet에 연락하십시오.

IPS 태그 변경에 대한 다음 정보를 확인하십시오.

5일 이내에 이전을 요청해야 합니다.

IPS 태그를 변경한 후 5일 이내에 전송을 요청하지 않으면 태그가 이전 값으로 다시 변경됩니다. IPS 태그의 값을 다시 변경해야 합니다. 그렇지 않으면 전송 요청이 실패합니다.

WHOIS 쿼리에서 IPS 태그 보기

IPS 태그에 대한 변경 사항은 Route 53로의 이전이 완료되기 전에는 WHOIS 쿼리에 나타나지 않습니다.

Gandi의 이메일

등록 대행사인 Gandi로부터 이전 프로세스에 대한 이메일을 수신하시게 될 것입니다. Gandi(transfer-auth@gandi.net)로부터 도메인 이전에 대한 이메일을 수신하는 경우에는 이

메일의 지침을 무시하세요. Route 53과 관련성이 없기 때문입니다. 대신에 이 항목의 지침을 따르십시오.

도메인(선택한 지리적 TLD)을 이전하기 전에 도메인 등록 갱신

대부분의 TLD의 경우, 도메인을 이전하면 등록이 자동으로 1년 연장됩니다. 하지만 일부 지리적 TLD의 경우, 도메인을 이전할 때 등록이 연장되지 않습니다. 이러한 TLD 중 하나가 있는 Route 53으로 도메인을 이전하는 경우, 특히 만료 날짜가 다가오고 있다면 도메인을 이전하기 전에 도메인 등록을 갱신하는 것이 좋습니다.

> **Important**
>
> 도메인을 이전하기 전에 갱신하지 않으면 이전을 완료하기 전에 등록이 만료될 수 있습니다. 이 상황이 발생할 경우 도메인은 인터넷에서 사용할 수 없게 되며 도메인 이름은 다른 사람이 구입 가능하게 될 수 있습니다.

다음 도메인을 다른 등록 대행자로 이전할 때는 등록이 자동으로 연장되지 않습니다.

- .ch(스위스)
- .cl(칠레)
- .co.uk(영국)
- .co.za(남아프리카)
- .com.au(호주)
- .cz(체코 공화국)
- .es(스페인)
- .fi(핀란드)
- .im(맨 섬)
- .jp(일본)
- .me.uk(영국)
- .net.au(호주)
- .org.uk(영국)
- .se(스웨덴)
- .uk(영국)

4단계: 이름 서버의 이름 가져오기

Amazon Route 53를 DNS 서비스로 사용 중이거나 기존 DNS 서비스를 계속 사용할 경우에는 이후의 프로세스에서 자동으로 이름 서버의 이름을 가져옵니다. 5단계: 이전 요청로 이동하세요.

도메인을 Route 53으로 이전하는 동시에 DNS 서비스를 Route 53 이외의 공급자로 변경하고 싶다면 해당 DNS 서비스 공급자가 제공하는 절차를 사용해 이전하려는 각 도메인의 이름 서버의 이름을 얻으세요.

> **Important**
>
> 도메인의 등록 기관이 도메인의 DNS 서비스 공급자인 경우, 도메인 등록을 이전하는 프로세스를 계속 진행하기 전에 DNS 서비스를 Route 53 또는 다른 DNS 서비스 공급자로 이전합니다. 도메인 등록을 이전하는 동시에 DNS 서비스도 이전하는 경우 해당 도메인과 연결된 웹 사이트, 이메일 및 웹 애플리케이션을 사용하지 못할 수 있습니다. 자세한 내용은 2단계(선택 사항): DNS 서비스를 Amazon Route 53 또는 다른 DNS 서비스 공급자로 이전 섹션을 참조하세요.

5단계: 이전 요청

도메인을 현재 등록 기관에서 Amazon Route 53로 이전하려면 Route 53 콘솔을 사용하여 이전 요청을 합니다. Route 53는 도메인의 현재 등록 기관과의 통신을 처리합니다.

콘솔을 사용하여 최대 5개의 도메인을 이전할 수 있습니다.

사용할 절차는 1개의 도메인을 이전하는지 또는 최대 5개의 도메인을 이전하는지에 따라 달라집니다.

- 단일 도메인의 도메인 등록을 Route 53으로 이전하려면
- 최대 5개의 도메인에 대해 Route 53으로 도메인 등록을 이전하려면

도메인을 내 계정으로 이전 프로세스를 사용하여 단일 도메인을 내 계정으로 이전합니다.

단일 도메인의 도메인 등록을 Route 53으로 이전하려면

1. https://console.aws.amazon.com/route53/에서 Route 53 콘솔을 엽니다.
2. 탐색 창에서 등록된 도메인을 선택합니다.
3. 등록된 도메인 페이지에서 내 송신 드롭다운에서 단일 도메인을 선택합니다.
4. 도메인을 내 계정으로 이전 페이지의 도메인 이전 가능성 검사 섹션에서 Route 53으로 등록을 이전하려는 도메인의 이름을 입력하고 확인을 선택합니다.

5. 도메인 등록을 이전할 수 있는 경우 최상위 도메인에 대한 이전 요구 사항을 완료했는지 확인하고 다음을 선택합니다.

   도메인 등록을 이전할 수 없는 경우 Route 53 콘솔에 그 이유가 나열됩니다. 등록 대행자에게 연락해 도메인 등록을 이전하지 못하게 막는 문제점들을 해결하는 방법에 대한 정보를 얻습니다.

6. DNS 서비스 페이지에서 이름 서버에 대한 정보를 검토하고 다음을 선택합니다.

7. 표시되면 3단계: 현재 등록 대행자에 대한 설정 변경에서 현재 등록 기관으로부터 받은 권한 부여 코드 또는 IPS 태그를 입력합니다.

   > **Note**
   >
   > .co.za, .uk, .co.uk, .me.uk 또는 .org.uk 도메인을 Route 53으로 전송하기 위해 권한 부여 코드를 입력할 필요가 없습니다.

   Next(다음)를 선택합니다.

8. 도메인 요금 옵션 페이지에서 이전하려는 도메인을 등록할 연수와 만료일 전에 도메인 등록을 자동으로 갱신할지 여부를 선택합니다.

   > **Note**
   >
   > 도메인 이름 등록과 갱신은 환불할 수 없습니다.다. 자동 도메인 갱신을 활성화하고 등록을 갱신한 후 도메인 이름이 필요 없다고 결정하는 경우 갱신 비용에 대한 환불을 받을 수 없습니다.

   Next(다음)를 선택합니다.

9. 연락처 정보 페이지에서 도메인 등록자, 관리자, 기술 담당자, 청구 담당자의 연락처 정보를 입력합니다. 이곳에 입력하는 값들은 등록하려는 모든 도메인에 적용됩니다. 자세한 내용은 도메인을 등록하거나 이전할 때 지정하는 값 섹션을 참조하세요.

   다음과 같은 고려 사항에 유의합니다.

   이름, 성

   [First Name]과 [Last Name]에는 귀하의 공식 ID에 표시된 이름을 지정하는 것이 좋습니다. 도메인 설정에 대한 일부 변경 사항의 경우, 일부 도메인은 신분 증명서를 제공하도록 요구합니

다. ID에 표시된 이름이 해당 도메인의 등록자 연락처에 기재된 이름과 정확히 일치해야 합니다.

다른 연락처

기본값으로 세 사람의 연락처에 대해 같은 정보를 사용합니다. 하나 이상의 연락처에 대해 다른 정보를 입력하려면, 등록 연락처와 동일 토글 스위치의 값을 비활성 위치로 변경합니다.

> **Note**
>
> .it 도메인의 경우 등록 기관 및 관리자 연락처가 동일해야 합니다.

필요한 추가 정보

일부 최상위 도메인(TLD)의 경우에 저희는 추가 정보를 수집할 의무가 있습니다. 이러한 TLD의 경우에는 [Postal/Zip Code] 필드 뒤에 해당 값을 입력합니다.

개인 정보 보호

WHOIS 쿼리로부터 연락처 정보를 숨길지 여부를 선택합니다.

> **Note**
>
> 관리자, 등록 기관 및 기술 담당자에 대해 동일한 개인 정보 설정을 지정해야 합니다.

자세한 정보는 다음의 주제를 참조하세요.

- 도메인 연락처 정보의 개인 정보 보호 활성화 또는 비활성화
- Amazon Route 53에 등록할 수 있는 도메인

> **Note**
>
> .uk. .co.uk, .me.uk 및 .org.uk 도메인에 대한 개인 정보 보호를 활성화하려면 지원 사례를 열고 개인 정보 보호를 요청합니다.

Next(다음)를 선택합니다.

10. 검토 페이지에서 입력한 정보를 검토하고 필요한 경우 수정합니다. 서비스 계약 조건을 읽은 다음, 확인란을 선택하여 서비스 계약 조건을 읽었음을 확인합니다.

    요청 제출을 선택합니다.

11. 탐색 창에서 도메인을 선택한 다음 요청을 선택합니다.

    이 페이지에서 도메인의 상태를 볼 수 있으며 등록 기관 담당자 확인 이메일에 응답해야 하는지 여부도 확인할 수 있습니다. 확인 이메일을 다시 보내도록 선택할 수도 있습니다.

    Route 53에 도메인을 등록하는 데 사용된 적이 없는 등록 기관 담당자의 이메일 주소를 지정한 경우 일부 TLD 레지스트리는 해당 주소가 유효한지 확인하도록 요청합니다.

    다음 이메일 주소 중 하나에서 확인 이메일을 전송합니다.

    - noreply@registrar.amazon - Amazon Registrar에 등록된 TLDs 경우.
    - noreply@domainnameverification.net - 등록 기관 협력사 Gandi에서 등록한 TLD의 경우. TLD의 등록 기관을 확인하려면 등록 기관 찾기을 참조하세요.

    > **Important**
    >
    > 등록자 연락처는 이메일의 지시 사항에 따라 이메일을 받았다는 사실을 확인해야 합니다. 그렇지 않으면 ICANN에서 요구할 경우 도메인을 일시 중지해야 합니다. 도메인이 일시 중지되면 인터넷에서 접속할 수 없습니다.

    a. 확인 이메일을 받은 경우 이메일 주소가 유효한지 확인하는 이메일의 링크를 선택합니다. 이메일이 즉시 도착하지 않으면 스팸 메일함을 살펴보십시오.

    b. 요청 페이지로 돌아갑니다. 상태가 [email-address is verified]로 자동으로 업데이트되지 않으면 [Refresh status]를 선택합니다.

12. 도메인 이전이 완료되면, 그 다음 단계는 도메인에 대한 DNS 서비스로 Route 53를 사용할 것인지 아니면 다른 DNS 서비스를 사용할 것인지에 따라 달라집니다.

    - Route 53 - 도메인을 등록할 때 Route 53가 생성한 호스팅 영역에서 레코드를 생성하여 도메인 및 하위 도메인의 트래픽을 라우팅하는 방식을 Route 53에 지시합니다.

      예를 들어, 누군가 브라우저에 도메인 이름을 입력하고 그 쿼리가 Route 53에 전달될 때, Route 53가 데이터 센터의 웹 서버 IP 주소로 해당 쿼리에 응답하길 원하십니까, 아니면 Elastic Load Balancing 로드 밸런서의 이름으로 응답하길 원하십니까?

자세한 내용은 레코드 작업 단원을 참조하십시오.

> **Important**
>
> Route 53가 자동으로 생성한 것이 아닌 다른 호스팅 영역에서 레코드를 생성할 경우 도메인의 이름 서버를 업데이트해야 새 호스팅 영역에 대해 이름 서버를 사용할 수 있습니다.

- 다른 DNS 서비스 - 새 도메인이 DNS 쿼리를 다른 DNS 서비스로 라우팅하도록 구성합니다. 다른 등록자를 사용하도록 이름 서버를 업데이트합니다. 절차를 수행합니다.

다음 절차를 사용하여 최대 5개의 도메인을 해당 계정으로 이전할 수 있습니다.

최대 5개의 도메인에 대해 Route 53으로 도메인 등록을 이전하려면

1. https://console.aws.amazon.com/route53/에서 Route 53 콘솔을 엽니다.
2. 탐색 창에서 등록된 도메인을 선택합니다.
3. 등록된 도메인 페이지의 내 송신 드롭다운에서 다중 도메인을 선택합니다.
4. 여러 도메인을 내 계정으로 이전 페이지에서 이전하려는 도메인을 최대 5개까지 입력하고 필요한 경우 줄마다 승인 코드를 입력하고 확인을 선택합니다.
5. 이전할 수 있는 도메인 등록은 도메인 가용성 목록에서 가능한 것으로 나열됩니다. 등록을 이전하려는 각 도메인 옆의 확인란을 선택하고 최상위 도메인에 대한 이전 요구 사항을 완료했는지 확인한 후 다음을 선택합니다.

   도메인 등록을 이전할 수 없는 경우 Route 53 콘솔에 그 이유가 나열됩니다. 등록 대행자에게 연락해 도메인 등록을 이전하지 못하게 막는 문제점들을 해결하는 방법에 대한 정보를 얻습니다.
6. DNS 서비스 페이지에서 이름 서버에 대한 정보를 검토하고 다음을 선택합니다.

   > **Note**
   >
   > 도메인 이름 등록과 갱신은 환불할 수 없습니다. 자동 도메인 갱신을 활성화하고 등록을 갱신한 후 도메인 이름이 필요 없다고 결정하는 경우 갱신 비용에 대한 환불을 받을 수 없습니다.
7. 연락처 정보 페이지에서 도메인 등록 기관, 관리자, 기술 담당자의 연락처 정보를 입력합니다. 여기에 입력하는 값들은 이전하는 모든 도메인에 적용됩니다.

> **Important**
>
> 등록자 연락처(도메인 소유자)에 대해 다음 값을 지정하는 것이 좋습니다.
>
> - 이름 및 성: 귀하의 공식 신분증에 표시된 이름을 지정하는 것이 좋습니다. 도메인 설정에 대한 일부 변경 사항의 경우, 일부 도메인은 신분 증명서를 제공하도록 요구합니다. ID에 표시된 이름이 해당 도메인의 등록자 연락처에 기재된 이름과 정확히 일치해야 합니다.
> - 연락처 세부 정보: 도메인 이전 중에는 현재 등록 대행자에 지정된 것과 동일한 값을 지정하는 것이 좋습니다. 등록자 연락처의 세부 정보를 변경하면 도메인 소유자가 변경되며 일부 TLD 등록기관에서는 도메인 이전 중에 도메인 소유자를 변경할 수 없도록 하고 있습니다. 등록자 연락처의 세부 정보를 변경하면 이전이 실패할 수 있습니다. 도메인을 이전한 후 등록자 연락처의 세부 정보를 변경할 수 있습니다.

기본값으로 세 사람의 연락처에 대해 같은 정보를 사용합니다. 하나 이상의 연락처에 대해 다른 정보를 입력하려면, 등록 연락처와 동일 값을 비활성 위치로 설정합니다.

> **Note**
>
> .it 도메인의 경우 등록 기관 및 관리자 연락처가 동일해야 합니다.

자세한 내용은 도메인을 등록하거나 이전할 때 지정하는 값 단원을 참조하십시오.

8. 일부 최상위 도메인(TLD)의 경우, 추가 정보를 수집해야 합니다. 이러한 TLD의 경우에는 [Postal/Zip Code] 필드 뒤에 해당 값을 입력합니다.
9. [Contact Type] 값이 [Person]인 경우 WHOIS 쿼리에서 연락처 정보를 숨길지 여부를 선택합니다. 자세한 내용은 도메인 연락처 정보의 개인 정보 보호 활성화 또는 비활성화 단원을 참조하십시오.
10. 제출을 선택합니다.
11. 입력한 정보를 다시 확인하고, 서비스 계약 조건을 읽은 다음, 확인란을 선택하여 서비스 계약 조건을 읽었음을 확인합니다.
12. 요청 제출을 선택합니다.

    도메인을 이전할 수 있는 경우, 도메인 이전 요청 승인을 위해 해당 도메인의 등록 기관 연락처로 이메일을 보냅니다.

13. 탐색 창에서 도메인을 선택한 다음 요청을 선택합니다.

    이 페이지에서 도메인의 상태를 볼 수 있으며 등록 기관 연락처 확인 이메일에 응답해야 하는지 여부도 확인할 수 있습니다. 확인 이메일을 다시 보내도록 선택할 수도 있습니다.

    Route 53에 도메인을 등록하는 데 사용된 적이 없는 등록 기관 담당자의 이메일 주소를 지정한 경우 일부 TLD 레지스트리는 해당 주소가 유효한지 확인하도록 요청합니다.

    다음 이메일 주소 중 하나에서 확인 이메일을 전송합니다.

    - noreply@registrar.amazon - Amazon Registrar에 등록된 TLDs 경우.
    - noreply@domainnameverification.net - 등록 기관 협력사 Gandi에서 등록한 TLD의 경우. TLD의 등록 기관을 확인하려면 등록 기관 찾기을 참조하세요.

    > **Important**
    >
    > 등록자 연락처는 이메일의 지시 사항에 따라 이메일을 받았다는 사실을 확인해야 합니다. 그렇지 않으면 ICANN에서 요구할 경우 도메인을 일시 중지해야 합니다. 도메인이 일시 중지되면 인터넷에서 접속할 수 없습니다.

    a. 확인 이메일을 받은 경우 이메일 주소가 유효한지 확인하는 이메일의 링크를 선택합니다. 이메일이 즉시 도착하지 않으면 스팸 메일함을 살펴보십시오.

    b. 요청 페이지로 돌아갑니다. 상태가 [email-address is verified]로 자동으로 업데이트되지 않으면 [Refresh status]를 선택합니다.

14. 도메인 이전이 완료되면, 그 다음 단계는 도메인에 대한 DNS 서비스로 Route 53를 사용할 것인지 아니면 다른 DNS 서비스를 사용할 것인지에 따라 달라집니다.

    - Route 53 - 도메인을 등록할 때 Route 53가 생성한 호스팅 영역에서 레코드를 생성하여 도메인 및 하위 도메인의 트래픽을 라우팅하는 방식을 Route 53에 지시합니다.

      예를 들어, 누군가 브라우저에 도메인 이름을 입력하고 그 쿼리가 Route 53에 전달될 때, Route 53가 데이터 센터의 웹 서버 IP 주소로 그 쿼리에 응답하길 원하십니까, 아니면 ELB 로드 밸런서의 이름으로 응답하길 원하십니까?

      자세한 내용은 레코드 작업 섹션을 참조하세요.

> **Important**
>
> Route 53가 자동으로 생성한 것이 아닌 다른 호스팅 영역에서 레코드를 생성할 경우 도메인의 이름 서버를 업데이트해야 새 호스팅 영역에 대해 이름 서버를 사용할 수 있습니다.

- 다른 DNS 서비스 - 새 도메인이 DNS 쿼리를 다른 DNS 서비스로 라우팅하도록 구성합니다. 다른 등록자를 사용하도록 이름 서버를 업데이트합니다. 절차를 수행합니다.

6단계: 확인 및 승인 이메일의 링크 클릭

이전을 요청하면 도메인 등록자 연락처로 이메일을 한 개 이상 보내 드립니다.

등록자 연락처가 연락 가능함을 확인하는 이메일

Route 53에 도메인을 등록한 적이 없거나, Route 53으로 도메인을 이전한 적이 없는 경우 해당 이메일 주소가 유효한지 확인하도록 요청하는 이메일을 보내 드립니다. 이 정보를 보유하고 있으므로 이 확인 이메일은 다시 발송하지 않습니다.

도메인 이전에 대한 승인을 받기 위한 이메일

일부 TLD의 경우 도메인 이전을 승인하려면 이메일에 응답해야 합니다.

.com, .net 및 .org와 같은 일반 TLD

.com, .net, .org 같은 일반 TLD가 있는 도메인에는 권한 부여가 필요 없습니다.

.co.uk 및 .jp와 같은 지리적 TLD

지리적 TLD가 있는 도메인의 경우 귀하의 도메인 이전 승인이 필요합니다. 10개의 도메인을 이전하는 경우, 10개의 이메일이 발송되며 각 메일에서 승인 링크를 클릭하셔야 합니다.

모든 이메일은 도메인의 등록자 연락처로 전송됩니다.

- 도메인 등록자 연락처 본인인 경우, 이메일의 지침에 따라 이전 권한을 부여하십시오.
- 등록자 연락처가 다른 사람인 경우, 당사자에게 이메일의 지침에 따른 이전 권한 부여를 요청하십시오.

> **Important**
>
> 지리적 TLD가 있는 도메인을 이전하는 경우에는 등록자 연락처에서 이전을 승인하는 연락을 최장 5일까지 기다립니다. 5일 이내에 등록자 연락처의 응답이 없으면 이전 작업을 취소하고 등록자 연락처로 취소를 알리는 이메일을 보냅니다.

주제

새 소유자 또는 새 이메일 주소에 대한 승인 이메일

다음 값을 변경했을 경우 승인을 요청하는 별개의 이메일이 발송됩니다.

도메인 소유자

도메인 소유자를 변경할 경우 도메인 소유자는 누구입니까?에서 설명한 대로, 도메인 등록자 연락처로 이메일이 발송됩니다.

등록자 연락처의 이메일 주소(일부 TLD만 해당)

일부 TLD는, 등록자 연락처의 이메일 주소를 변경할 경우 등록자 연락처의 이전 이메일 주소와 새 이메일 주소로 이메일이 발송됩니다. 두 이메일 주소의 누군가가 이메일의 지침에 따라 변경을 승인해야 합니다.

도메인 소유자 또는 등록자 연락처의 이메일 주소를 변경하는 경우, 최상위 도메인에 따라 다르지만 3~15일 이내에 변경에 대한 권한 부여를 받지 못하면 ICANN의 요구에 따라 요청을 취소해야 합니다.

승인 이메일을 발송하는 이메일 주소

모든 이메일은 다음 이메일 주소 중 하나에서 발송합니다.

TLD	권한 부여 이메일을 발송하는 이메일 주소
.com.au 및 .net.au	no-reply@ispapi.net

TLD	권한 부여 이메일을 발송하는 이메일 주소
	이 이메일에 http://transfers.ispapi.net에 대한 링크가 포함됩니다.
.fr	nic@nic.fr(도메인을 이전함과 동시에 등록자 연락처를 .fr 도메인 이름으로 변경하는 경우). (이메일은 현재 등록자 연락처 및 새 등록자 연락처 모두에 전송됩니다.)
기타 모두	다음 이메일 주소 중 하나: • noreply@registrar.amazon • noreply@domainnameverification.net

TLD의 등록 대행자를 확인하려면 Amazon Route 53에 등록할 수 있는 도메인을 참조하십시오.

현재 등록자의 승인

등록자 연락처가 이전을 승인하면 현재 등록 기관과 협력하여 도메인 이전을 시작합니다. 도메인의 TLD에 따라 이 단계에는 최대 10일이 소요될 수 있습니다.

- 일반적인 최상위 도메인 - 최대 7일 소요
- 지리적 최상위 도메인(국가 코드 최상위 도메인이라고도 함) - 최대 10일 소요

흔한 일이지만 현재 등록 대행자가 이전 요청에 응답하지 않는 경우, 이전이 자동으로 처리됩니다. 현재 등록 기관이 이전 요청을 거부할 경우 현재 등록자 연락처로 이메일 알림을 보냅니다. 등록자는 현재 등록 대행자에게 연락을 취해 이전과 관련된 문제를 해결해야 합니다.

다음 단계

도메인 이전이 승인되면 등록자 연락처로 또 다른 이메일이 발송됩니다. 이 프로세스에 대한 자세한 내용은 다음(도메인 이전 상태 보기)을 참조하십시오.

이전이 완료되는 즉시 도메인 이전 요금이 AWS 계정에 청구됩니다. TLD에 따른 요금 목록은 Amazon Route 53 도메인 등록 요금을 참조하세요.

> **Note**
>
> 1회적으로 발생하는 요금이므로 CloudWatch 결제 메트릭에는 표시되지 않습니다. CloudWatch 지표에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 Amazon CloudWatch 지표 사용을 참조하세요.

7단계: 도메인 구성 업데이트

이전이 완료된 후 필요하다면 다음 설정을 변경할 수 있습니다.

이전 잠금

도메인을 Route 53으로 이전하려면 이전 잠금을 비활성화해야 했습니다. 무단 이전을 방지하기 위해 잠금을 다시 활성화하려면 다른 등록 대행자로의 무단 이전을 방지하기 위해 도메인 잠그기 단원을 참조하십시오.

자동 갱신

이전된 도메인은 만료 날짜가 다가오면 자동으로 갱신되도록 구성됩니다. 이 설정을 변경하는 자세한 방법은 도메인 자동 갱신 활성화 또는 비활성화 단원을 참조하십시오.

연장 등록 기간

기본적으로 Route 53는 도메인을 1년 단위로 갱신합니다. 이보다 긴 기간 동안 도메인을 등록하려면 도메인의 등록 기간 연장 단원을 참조하십시오.

DNSSEC

도메인의 DNSSEC 구성에 관한 정보는 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 이전 상태 보기

다른 도메인 등록 기관에서 Amazon Route 53으로 도메인 이전을 시작한 후 요청 페이지(새 콘솔) 또는 Route 53 콘솔의 대기 중인 요청(이전 콘솔) 페이지의 상태를 추적할 수 있습니다. [Status] 열은 현재 단계에 대한 간략한 설명을 담고 있습니다. 다음 목록에는 콘솔의 텍스트와 각 단계에 대한 상세 설명이 담겨 있습니다.

> **Note**
>
> 이전 요청을 제출할 때 초기 상태는 [Domain transfer request submitted]입니다. 이 상태는 요청이 접수되었음을 나타냅니다.

[Determining whether the domain meets transfer requirements](도메인이 이전에 관한 요건을 충족하는지 판단하기, 14단계 중 1단계)

도메인의 상태가 이전 요건에 부합하는지 확인하고 있습니다. 도메인의 잠금을 해제해야 하고, 도메인에는 이전 요청 시 제출한 다음의 상태 코드 중 어느 것도 없어야 합니다.

- clientTransferProhibited
- pendingDelete
- pendingTransfer
- redemptionPeriod

지리적 TLD 전용 - WHOIS 정보 확인(14단계 중 2단계)

지리적 TLD가 있는 도메인을 이전하는 경우라면 도메인에 대한 개인 정보 보호가 비활성화되어 있는지 확인하기 위해 도메인에 WHOIS 쿼리를 보냈습니다. 현재 등록 대행자에게서 개인 정보 보호가 여전히 활성화되어 있다면, 저희는 도메인을 이전하는 데 필요한 정보에 액세스할 수 없습니다.

> **Note**
>
> .com, .net, .org 같은 일반 TLD가 있는 도메인에는 권한 부여가 필요 없습니다.

지리적 TLD 전용 - 이전 권한을 획득하기 위해 등록자 연락처에 이메일을 보냄(14단계 중 3단계)

지리적 TLD가 있는 도메인을 이전하는 경우라면 도메인의 등록자 연락처로 이메일을 보냈습니다. 이메일의 목적은 도메인의 권한 있는 연락처에 의해 이전이 요청되었음을 확인하기 위함입니다.

> **Note**
>
> .com, .net, .org 같은 일반 TLD가 있는 도메인에는 권한 부여가 필요 없습니다.

현재 등록 대행자에게 이전 확인(4/14단계)

도메인에 대한 현재 등록 대행자에게 이전을 시작하도록 요청했습니다.

지리적 TLD 전용 - 등록자 연락처로부터 권한 부여 대기 중(14단계 중 5단계)

도메인 등록자 연락처에 이메일을 발송했으며(14단계 중 3단계) 등록자 연락처가 이메일에서 링크를 클릭하여 이전을 승인하기를 기다리고 있습니다. 지리적 TLD가 있는 도메인을 이전하는데 어떠한 이유로 이메일을 받지 못했다면 권한 부여 및 확인 이메일 재전송 단원을 참조하십시오.

현재 등록 대행자에게 연락해 이전을 요청(14단계 중 6단계)

이전을 완료하기 위해 도메인에 대한 현재 등록 대행자와 협력하고 있습니다.

[Waiting for the current registrar to complete the transfer](현재 등록 대행자가 이전을 완료하기를 기다림, 14단계 중 7단계)

현재 등록 대행자가 도메인이 이전 요건을 충족하는지 확인하고 있습니다. 도메인의 TLD에 따라 이 단계에는 최대 10일이 소요될 수 있습니다.

- 일반적인 최상위 도메인 - 최대 7일 소요
- 지리적 최상위 도메인(국가 코드 최상위 도메인이라고도 함) - 최대 10일 소요

> **Note**
>
> .JP 도메인을 이전할 때 Route 53에서 보낸 확인 이메일을 승인했지만 7단계에서 며칠 동안 중지된 경우AWS 지원 센터에 연락하여 지원을 받으십시오.

대부분의 등록 대행자의 경우 프로세스가 완전히 자동화되어 있으며 가속화할 수 없습니다. 일부 등록 대행자는 이전의 승인을 요청하는 이메일을 전송합니다. 등록 대행자가 이 확인 이메일을 전송하면 이전 프로세스가 7~10일보다 더 빠를 수 있습니다.

등록 대행자가 이전을 거부할 수도 있는 사유에 대한 자세한 내용은 최상위 도메인에 따른 이전 요건을 참조하십시오.

등록자 연락처에 그 연락처가 이전을 시작했는지 확인(14단계 중 8단계)

일부 TLD 등록부는 인증된 사용자가 도메인 이전을 요청한 사실을 확인하기 위해 등록자 연락처에 또 다른 이메일을 보냅니다.

이름 서버를 등록부와 동기화하기(14단계 중 9단계)

이 단계는 전송 요청의 일부로 제공된 이름 서버가 현재 등록 대행자와 함께 나열된 이름 서버와 다른 경우에만 발생합니다. 저희는 이름 서버를 귀하가 제공하는 새로운 이름 서버로 업데이트할 것입니다.

설정을 등록부와 동기화하기(14단계 중 10단계)

이전이 성공적으로 완료되었는지 확인하고, 아울러 도메인 관련 데이터를 등록 대행 협력사와 동기화하고 있습니다.

등록부에 업데이트된 연락처 정보를 보냄(14단계 중 11단계)

이전 요청 시 도메인의 소유권을 변경한 경우, 이를 변경하려는 작업을 하고 있는 중입니다. 그러나 대부분의 등록 대행자들은 도메인 이전 절차의 일환으로 소유권 이전을 허용하지 않고 있습니다.

Route 53으로 이전 작업 완료(14단계 중 12단계)

이전 절차가 성공적으로 완료되었는지 확인하는 중입니다.

이전 작업 완료(14단계 중 13단계)

Route 53에 도메인을 설정하고 있습니다.

이전 완료(14단계 중 14단계)

이전이 성공적으로 완료되었습니다.

Amazon Route 53으로 도메인을 이전할 때 도메인 등록에 대한 만료 날짜에 미치는 영향

도메인을 등록 대행자 사이에서 이전할 때 어떤 TLD 등록부는 도메인에 대해 같은 만료 날짜를 유지하도록 하고, 어떤 등록부는 만료 날짜에 1년을 더하며, 어떤 등록부는 만료 날짜를 이전 날짜 이후 1년으로 변경합니다.

> **Note**
>
> 대부분의 TLD의 경우 도메인을 Amazon Route 53으로 이전한 후 도메인 등록 기간을 최대 10년 연장할 수 있습니다. 자세한 내용은 도메인의 등록 기간 연장 단원을 참조하십시오.

일반 TLD

일반 TLD를 지닌 도메인(예: .com)을 Route 53으로 이전할 때, 도메인에 대한 새 만료 날짜는 이전 등록 기관의 만료 날짜에 1년을 더한 것입니다.

지리적 TLD

지리적 TLD를 지닌 도메인(예: .co.uk)을 Route 53으로 이전할 때, 도메인에 대한 새 만료 날짜는 TLD에 따라 달라집니다. 다음 표에서 해당 TLD를 찾아 도메인 이전이 만료 날짜에 어떤 영향을 미치는지 판단하십시오.

대륙	지리적 TLD, 그리고 도메인 이전이 만료 날짜에 미치는 영향
아프리카	.co.za - 만료 날짜에는 변함이 없습니다.
북남미	.cl, .com.ar, .com.br - 만료 날짜에는 변함이 없습니다. .ca, .co, .mx, .us - 이전 만료 날짜에 1년이 추가됩니다.
아시아/오세아니아	.co.nz, .com.au, .com.sg, .jp, .net.au, .net.nz, .org.nz, .sg - 만료 날짜에는 변함이 없습니다. .in - 이전 만료 날짜에 1년이 추가됩니다.
유럽	.ch, .co.uk, .es, .fi, .me.uk, .org.uk, .se - 만료 날짜에는 변함이 없습니다. .berlin, .eu, .io, .me, .ruhr, .wien - 이전 만료 날짜에 1년이 추가됩니다. .be, .de, .fr, .it, .nl - 새 만료 날짜는 도메인을 이전한 날로부터 1년입니다.

도메인을 다른 AWS 계정으로 이전

한 AWS 계정을 사용하여 도메인을 등록하고 도메인을 다른 AWS 계정으로 이전하려는 경우 새 콘솔을 사용하거나 또는 AWS CLI 기타 프로그래밍 방법을 사용하여 도메인을 쉽게 이전할 수 있습니다.

주제

- 1단계: 도메인을 다른 AWS 계정으로 전송
- 2단계(선택 사항): 호스팅 영역을 다른 AWS 계정으로 마이그레이션

1단계: 도메인을 다른 AWS 계정으로 전송

등록 후 첫 14일 이내에는 도메인을 이전할 수 없습니다.

도메인 이전을 시작할 때 루트 계정을 사용하여 로그인하거나 다음 방법 중 하나 이상을 사용하여 IAM 권한이 부여된 사용자를 통해 로그인해야 합니다.

- 사용자에게 AdministratorAccess 관리형 정책을 할당했습니다.
- 사용자에게 AmazonRoute53DomainsFullAccess 관리형 정책을 할당했습니다.
- 사용자에게 AmazonRoute53FullAccess 관리형 정책을 할당했습니다.
- 사용자에게 PowerUserAccess 관리형 정책을 할당했습니다.
- 사용자에게 `TransferDomains`, `DisableDomainTransferLock`, `RetrieveDomainAuthCode` 작업을 모두 수행할 수 있는 권한이 있습니다.

루트 계정을 사용하거나 필수 권한이 없는 사용자를 사용하여 로그인하지 않으면 이전을 수행할 수 없습니다. 이 요구 사항은 권한이 없는 사용자가 도메인을 다른 로 이전하는 것을 방지합니다 AWS 계정.

이전 프로세스는 두 단계로 이루어집니다. 먼저 최초 계정 소유자가 다른 AWS 계정으로 이전 시작 절차에서 이전을 시작하고 대상 계정 소유자가 다른 AWS 계정으로부터의 이전 수락 절차에서 이전을 수락합니다.

도메인을 다른 AWS 계정으로 이전하려면

1. 도메인이 현재 등록된 AWS 계정 AWS 를 사용하여에 로그인합니다.
2. https://console.aws.amazon.com/route53/에서 Route 53 콘솔을 엽니다.
3. 탐색 창에서 등록된 도메인을 선택합니다.
4. 다른 AWS 계정으로 이전하고자 하는 도메인의 이름을 선택합니다.
5. 세부 정보 섹션 위의 송신 드롭다운에서 다른 AWS 계정으로 이전을 선택합니다.
6. 다른 AWS 계정으로 이전 대화 상자에서 대상 계정 ID를 입력합니다. 대상 AWS 계정 소유자로부터 이 ID를 받을 수 있습니다.
7. 확인을 선택합니다.
8. 암호 생성 대화 상자에서 암호를 복사하여 수신 AWS 계정 소유자에게 전달합니다.

   요청 페이지에서 도메인의 상태는 진행 중으로 표시되고 유형은 외부로 내부 이전이 표시됩니다.

다른 AWS 계정에서 도메인 전송을 수락하려면

1. 도메인을 수신하는 AWS 계정 를 AWS 사용하여에 로그인합니다.
2. https://console.aws.amazon.com/route53/에서 Route 53 콘솔을 엽니다.

3. 탐색 창에서 요청을 선택합니다.
4. 요청 페이지에서 다른에서 전송하려는 도메인 이름 옆에 있는 라디오 버튼을 선택합니다 AWS 계정. 도메인을 이전할 준비가 된 경우 상태는 작업 필요이고 유형은 도메인 내부로 내부 이전입니다.

   3일 이내에 요청을 수락해야 합니다. 3일 이내에 이전을 수락하지 않으면 이전 요청이 취소됩니다.
5. 작업 드롭다운에서 수락을 선택합니다.

   거부를 선택하여 이전 프로세스를 취소할 수도 있습니다.
6. 수락한 경우 도메인을 내 계정으로 이전 페이지의 암호 섹션에 원래 계정 소유자로부터 받은 암호를 입력합니다.

   이용 약관을 읽고 다음을 선택합니다.
7. 요청 페이지로 이동하여 이전 상태 및 완료하기 위한 다른 단계를 모니터링합니다.
8. 이전이 완료된 후 연락처 정보를 업데이트할 수 있습니다. 자세한 내용은 도메인 연락처 정보 및 소유권 업데이트 단원을 참조하십시오.

프로그래밍 방식으로 도메인 이전

AWS CLI, SDKs 중 하나 또는 Route 53 API를 AWS 사용하여 프로그래밍 방식으로 도메인을 전송할 수도 있습니다. 자세한 내용은 다음 설명서를 참조하세요.

- Route 53 도메인 등록 API를 통해 도메인을 이전하는 데 사용하는 API 작업에 대한 이전 프로세스 개요와 설명서는 Amazon Route 53 API 참조의 TransferDomainToAnotherAwsAccount를 참조하세요.
- 프로그래밍 방식으로 도메인을 전송하는 다른 옵션에 대한 자세한 내용은 "AWS 문서" 페이지의 가이드 및 API 참조 섹션에서 "SDKs 및 도구 키트"를 참조하세요.
- 수신 계정은 3일 이내에 transfer-domain-to-another-aws-account API를 사용하여 원래 계정으로부터의 이전을 수락해야 합니다. 3일 이내에 이전을 수락하지 않으면 이전 요청이 취소됩니다.

> **Important**
>
> 도메인을 다른 AWS 계정으로 이전하면 도메인의 호스팅 영역이 이전되지 않습니다. 호스팅 영역도 이전하고자 하는 경우 도메인이 전송될 때까지 기다린 후 2단계(선택 사항): 호스팅 영역을 다른 AWS 계정으로 마이그레이션을 확인합니다.

2단계(선택 사항): 호스팅 영역을 다른 AWS 계정으로 마이그레이션

Route 53를 도메인의 DNS 서비스로 사용 중인 경우, 도메인을 다른 AWS 계정으로 이전할 때 Route 53는 호스팅 영역을 이전하지 않습니다. 도메인 등록이 하나의 계정과 연결되어 있고 해당 호스팅 영역은 다른 계정과 연결되어 있다면, 도메인 등록도 DNS 기능도 영향을 받지 않습니다. 영향을 주는 유일한 것은 도메인을 보기 위해 하나의 계정을 이용해 Route 53 콘솔에 로그인하고 호스팅 영역을 보기 위해 다른 계정을 이용해 로그인해야 한다는 것입니다.

도메인을 이전하는 출발 계정과 도착 계정을 보유한 경우 선택에 따라 도메인의 호스팅 영역을 다른 계정으로 마이그레이션할 수 있지만 필수 사항은 아닙니다. Route 53는 기존 호스팅 영역에 있는 레코드를 계속 사용하여 도메인에 대한 트래픽을 라우팅합니다.

> **Important**
>
> 도메인을 이전하는 계정과 도메인을 이전하는 계정을 모두 소유하지 않은 경우 도메인을 이전하는 AWS 계정으로 기존 호스팅 영역을 마이그레이션하거나 소유한 AWS 계정에서 새 호스팅 영역을 생성해야 합니다. 도메인 트래픽을 라우팅하는 호스팅 영역을 생성했던 계정이 사용자 보유 계정이 아닌 경우에는 트래픽 라우팅 방식을 제어할 수 없습니다.

기존 호스팅 영역을 새 계정으로 마이그레이션하려면 호스팅 영역을 다른 AWS 계정으로 마이그레이션 단원을 참조하십시오.

새 호스팅 영역을 생성하려면 Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정 단원을 참조하십시오. 이 주제는 일반적으로 다른 등록 대행자에서 Route 53으로 도메인을 이전할 때 사용되지만, 한 AWS 계정에서 다른 계정으로 도메인을 이전할 때는 프로세스가 동일합니다.

Amazon Route 53에서 다른 등록 기관으로 도메인 이전하기

도메인을 Amazon Route 53에서 다른 등록 기관으로 이전할 때 Route 53에서 일부 정보를 얻어 그 정보를 새로운 등록 기관에 제공합니다. 그러면 새 등록 대행자가 나머지 작업을 처리할 것입니다.

> **Important**
>
> 현재 Route 53를 DNS 서비스 공급자로 사용하고 있는데 DNS 서비스를 다른 공급자로 이전하고 싶다면, 다음의 Route 53 기능은 다른 DNS 서비스 공급자가 제공하는 기능과는 직접 대응되지 않는다는 점에 유의하세요. 새로운 DNS 서비스 공급자들과 협력해 대응되는 기능을 구현하는 방법을 결정해야 합니다.
>
> - 별칭 레코드. 자세한 내용은 별칭 또는 비 별칭 레코드 선택 섹션을 참조하세요.

- 심플 라우팅 정책 이외의 라우팅 정책입니다. 자세한 내용은 라우팅 정책 선택 섹션을 참조하세요.
- 레코드와 연결된 상태 확인입니다. 자세한 내용은 DNS 장애 조치 구성 섹션을 참조하세요.

대부분의 도메인 등록 대행자는 도메인을 다른 등록 대행자로 이전할 때 요구 사항을 적용합니다. 이러한 요구 사항의 주요 목적은 사기 도메인의 소유자가 도메인을 다른 등록 대행자로 반복해서 이전하지 못하도록 하는 것입니다. 요구 사항은 다양하지만, 일반적인 요구 사항은 다음과 같습니다.

- 적어도 14일 전에 현재 등록 대행자에 도메인을 등록하거나 현재 등록 대행자로 도메인 등록을 이전해야 합니다.
- 그 도메인은 다음 도메인 이름 상태 코드 중 어떤 것도 가질 수 없습니다.
  - pendingDelete
  - pendingTransfer
  - redemptionPeriod
  - clientTransferProhibited
  - serverTransferProhibited

도메인 이름 상태 코드의 현재 목록과 각 코드의 의미에 대한 설명을 보시려면 ICANN 웹 사이트로 가서 [epp status codes]를 검색하십시오. ICANN 웹 사이트에서 검색하십시오. 웹 검색 시 때로는 지난 버전의 문서가 표시될 수도 있습니다.

> **Note**
>
> 도메인을 다른 도메인 등록 기관으로 이전하고 싶지만 도메인이 등록된 AWS 계정이 해지, 일시 중지 또는 종료된 경우 AWS Support에 문의하여 도움을 받을 수 있습니다. 등록 후 첫 14일 이내에는 도메인을 이전할 수 없습니다. 자세한 내용은 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.

> **Note**
>
> 새 등록 기관에 REG-ID 코드가 필요한 경우 AWS Support에 문의하여 도움을 받을 수 있습니다. 자세한 내용은 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.

Route 53에서 다른 등록 기관으로 도메인을 이전하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 등록된 도메인을 선택합니다.
3. 다른 등록 대행자에게 이전하고자 하는 도메인의 이름을 선택합니다.
4. 도메인 이름 페이지에서 도메인 이름 상태 코드 값을 확인합니다. 그 값이 다음 값들 중 하나이면, 도메인을 이전할 수 없습니다.

   - pendingDelete
   - pendingTransfer
   - redemptionPeriod
   - clientTransferProhibited
   - serverTransferProhibited

   도메인 이름 상태 코드의 현재 목록과 각 코드의 의미에 대한 설명을 보시려면 ICANN 웹 사이트로 가서 [epp status codes]를 검색하십시오. ICANN 웹 사이트에서 검색하십시오. 웹 검색 시 때로는 지난 버전의 문서가 표시될 수도 있습니다.

   도메인 이름 상태 코드 값이 serverTransferProhibited인 경우 AWS Support에 무료로 문의하여 도메인을 이전하기 위해 수행해야 할 작업을 배울 수 있습니다. 자세한 내용은 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.
5. 이전 잠금 값이 활성인 경우 작업 드롭다운에서 이전 잠금 끄기를 선택합니다.

   > **Note**
   >
   > AWS Support에 문의하여 .jp 도메인의 등록 기관 전송을 잠금 해제합니다. 자세한 내용은 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.

6. .be, .co.za, .ru, .uk, .co.uk, .me.uk 및 .org.uk 도메인을 제외한 모든 도메인 - 도메인 이름 페이지의 Transfer out 드롭다운에서 Transfer to other registrar를 선택합니다.

   다른 등록 대행자로 이전 대화 상자에서 복사를 선택하여 도메인 이전에 대한 승인 코드를 복사합니다. 이 절차 후반에 등록 대행자에게 이 값을 제공할 것입니다.

> **Note**
>
> .eu 도메인의 경우 레지스트리 https://my.eurid.eu/의 'My.eu' 패널을 사용하여 인증 코드를 생성할 수도 있습니다.

.be, .co.za, .es, .ru, .uk, .co.uk, .me.uk, .org.uk 도메인 - 다음을 수행합니다.

.be 도메인

DNS Belgium 웹사이트에서 .be 도메인의 레지스트리에서 권한 부여 코드를 가져옵니다.

.co.za 도메인

.co.za 도메인을 다른 등록 대행자로 이전하는 데는 권한 부여 코드가 필요하지 않습니다.

.ru 도메인

https://www.nic.ru/en/auth/recovery/에서 .ru 도메인의 등록부로부터 권한 부여 코드를 가져옵니다.

a. 도메인 이름을 기준으로 자격 증명을 복구하는 옵션을 선택합니다.

b. 도메인 이름을 입력하고 계속을 선택합니다.

c. 화면에 표시되는 메시지에 따라 RU-CENTER 관리자 페이지에 액세스합니다.

d. Manage your account(계정 관리) 섹션에서 Domain transfer(도메인 이전)를 선택합니다.

e. REGRU-RU에 이전을 확인합니다.

.uk, .co.uk, .me.uk 및 .org.uk 도메인

IPS 태그를 새 등록 대행자의 값으로 변경합니다.

a. Nominet 웹 사이트의 Find a Registrar 페이지로 이동한 다음, 새 등록 대행자의 IPS 태그를 찾습니다. (Nominet은 .uk, co.uk, .me.uk 및 .org.uk 도메인 등록 기관입니다.)

b. 등록된 도메인 > 도메인 이름 페이지에서 전송, 드롭다운을 선택한 다음 IPS 태그 업데이트를 선택하고 6a단계에서 얻은 값을 지정합니다.

c. 업데이트를 선택합니다.

> **Note**
>
> Nominet 콘솔에서 IPS 태그를 업데이트할 수도 있습니다. 지침은 등록 기관 전환을 참조하세요.

7. 현재 Route 53를 도메인에 대한 DNS 서비스 공급자로 사용하고 있지 않다면, 10단계로 건너뛰세요.

   현재 Route 53를 도메인에 대한 DNS 서비스 공급자로 사용하고 있다면 다음 단계를 수행하세요.

   a. Hosted Zones(호스팅 영역)를 선택합니다.

   b. 도메인에 대한 호스팅 영역의 이름을 선택합니다. 도메인과 호스팅 영역은 이름이 같습니다.

   c. Route 53를 도메인에 대한 DNS 서비스 공급자로 계속 사용하려는 경우: Route 53가 호스팅 영역에 할당한 이름 서버 4개의 이름을 적어 두세요. 자세한 내용은 퍼블릭 호스팅 영역에 대한 이름 서버 가져오기 섹션을 참조하세요.

      Route 53를 도메인에 대한 DNS 서비스 공급자로 계속 사용하고 싶지 않은 경우: NS 및 SOA 레코드를 제외한 레코드 전체에 대한 설정을 적어 두세요. 별칭 레코드와 같은 Route 53 특정 기능의 경우 새로운 DNS 서비스 공급자와 협력해 대응되는 기능을 구현하는 방법을 결정해야 합니다.

8. DNS 서비스를 다른 공급자에게 전송하는 경우 새 DNS 서비스에서 제공하는 방법을 사용하여 다음 작업을 수행하십시오.

   - 호스팅 영역 생성
   - Route 53 레코드 기능을 재현하는 레코드 생성
   - 새 DNS 서비스가 호스팅 영역에 할당된 이름 서버를 가져옵니다.

9. 새 등록 대행자가 제공하는 절차를 사용하여 도메인 이전을 요청합니다.

   .co.za, .uk, .co.uk, .me.uk 및 .org.uk 도메인을 제외한 모든 도메인 -이 절차의 6단계에서 Route 53 콘솔에서 가져온 권한 부여 코드를 입력하라는 메시지가 표시됩니다.

10. Route 53를 여전히 DNS 서비스 공급자로 사용하고 싶다면, 새 등록 기관이 제시하는 프로세스에 따라 7단계에서 얻은 Route 53 이름 서버의 이름을 지정합니다. 다른 DNS 서비스 공급자를 사용하고 싶다면, 8단계에서 새 호스팅 영역을 생성할 때 새 공급자가 준 이름 서버의 이름을 지정합니다.

11. 확인 이메일에 응답합니다.

.jp 도메인을 제외한 모든 도메인

Route 53는 도메인 등록자의 이메일 주소로 확인 이메일을 발송합니다.

- 이메일에 답하지 않을 경우 지정된 날짜에 자동으로 전송됩니다.
- 더 일찍 전송되도록 하거나 전송을 취소하고 싶으면 이메일에 포함된 링크를 선택하여 Route 53 웹 사이트로 이동하고 해당 옵션을 선택합니다.
- TLD에 따라 확인 이메일에는 이전을 승인하거나 거부할 수 있는 https://approvemove.com 링크가 포함될 수 있습니다. 도메인 연락처에 개인 정보 보호가 활성화되면 Amazon Registrar에 등록된 TLD에 대한 identity-protect.org 주소에서 이메일이 전송됩니다. TLD의 등록 기관을 확인하려면 등록 기관 찾기을 참조하세요.

.jp 도메인

Route 53는 noreply@domainnameverification.net 주소에서 도메인 등록자 연락처의 이메일 주소로 전송을 확인하는 링크가 포함된 확인 이메일을 보냅니다.

- 이메일에 답하지 않을 경우 지정된 날짜에 이전이 취소됩니다.
- 더 일찍 전송되도록 하거나 전송을 취소하고 싶으면 이메일에 포함된 링크를 선택하여 Route 53 웹 사이트로 이동하고 해당 옵션을 선택합니다. 7단계에서 얻은 도메인 인증 코드를 제공해야 합니다.

또한 Wixi.jp에서 이메일을 수신할 수 있습니다. 이 이메일은 무시해도 됩니다.

12. 도메인이 이전되는 등록 기관이 이전이 실패했다고 보고하는 경우, 해당 등록 기관에 자세한 내용을 문의하세요. 도메인을 다른 등록 기관으로 이전하면 모든 상태 업데이트가 새 등록 기관으로 이동하기 때문에 Route 53에는 이전이 실패한 이유에 대해 아무 정보도 남지 않습니다.

    Route 53에서 받은 권한 부여 코드가 유효하지 않아 새 등록 기관이 전송이 실패했다고 보고하는 경우 AWS Support에서 사례를 엽니다. 지원 계약은 필요 없으며, 수수료도 없습니다. 자세한 내용은 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.

    > **Note**
    >
    > Gandi에서 생성한 권한 부여 코드는 약 5일 동안 유효합니다. 이 기간 이후에 전송 시도가 발생하면 만료된 코드로 인해 전송 시도가 실패할 수 있습니다.

13. 다른 DNS 서비스 공급자에게 DNS 서비스를 이전한 경우 DNS 해석기가 Route 53 이름 서버의 이름을 이용한 DNS 쿼리에 대한 응답을 중지한 후 호스팅 영역의 레코드를 삭제하고 호스팅 영역을

삭제할 수 있습니다. 이 작업은 보통 이틀 정도 걸리는데, 이는 DNS 해석기가 도메인에 대한 이름 서버의 이름을 캐시하는 데 보통 걸리는 시간입니다.

> **Important**
>
> DNS 해석기가 Route 53 이름 서버의 이름을 이용한 DNS 쿼리에 계속 응답하는 동안 호스팅 영역을 삭제하는 경우 인터넷에서 도메인을 사용하지 못하게 됩니다.

호스팅 영역을 삭제한 후 Route 53는 호스팅 영역에 대한 월별 요금 청구를 중지합니다. 자세한 내용은 다음 설명서를 참조하세요.

- 레코드 삭제
- 퍼블릭 호스팅 영역 삭제
- Route 53 가격

Amazon Registrar로 등록 기관 이전

Amazon Route 53 Domains는 두 개의 등록 기관을 사용하여 고객을 위한 도메인을 등록합니다. Amazon Registrar는에서 소유하고 운영하는 등록 기관이고 AWS Gandi는 함께 작업하는 등록 기관 직원입니다. 처음에는 Amazon Registrar가 .com 또는 .club과 같은 다수의 최상위 도메인(TLD)에 대해 직접 승인되지 않았기 때문에 대부분의 Route 53 도메인이 Gandi를 통해 등록되었습니다. 이제 Amazon Registrar가 수백 개(및 성장 중)의 TLD로 직접 인증되었으므로 Gandi를 통해 등록된 도메인을 사용자를 대신하여 Amazon Registrar로 이전하기 시작합니다.

이렇게 해도 Route 53 내에서 도메인을 관리하는 방법은 변경되지 않으며, 도메인의 레코드 등록 기관만 Gandi에서 Amazon Registrar로 업데이트됩니다. 이전은 도메인 갱신 프로세스 중에 이루어지며 표준 갱신 요금만 적용됩니다. 이전이 완료되면 외부의 새 등록 대행자로 도메인을 이전하기 위한 새 요청이 지연될 AWS 수 있습니다. Route 53는 갱신 시 이전이 발생하기 15일 전에 영향을 받는 도메인 등록자에게 알립니다. 이 프로세스는 도메인 이름 등록 계약(3.11.5 섹션 참조)에 설명되어 있습니다.

Route 53 서비스를 계속 사용하여 도메인을 관리하려면 이전이 필수입니다. Amazon Registrar를 사용하여 도메인을 관리하지 않으려면 갱신 시 이전 알림을 받은 후 15일 이내에 도메인을 다른 등록 기관으로 이전해야 합니다 AWS.

권한 부여 및 확인 이메일 재전송

도메인 등록과 관련된 몇몇 작업의 경우, ICANN은 도메인 등록자 연락처의 권한 부여 또는 등록자 연락처의 이메일 주소가 유효하다는 확인을 받을 것을 요구합니다. 승인 또는 확인을 받으려면 링크가 포함된 이메일을 보내드립니다. 작업의 성격과 최상위 도메인에 따라 다르지만 3~15일 사이에 링크를 클릭해야 합니다. 이 기간이 지나면 링크 작동이 정지됩니다.

할당된 기간 안에 이메일의 링크를 클릭하지 않으면 ICANN은 사용자가 시도하는 작업에 따라 일반적으로 도메인 일시 중지 또는 작업 취소를 요구합니다.

도메인 등록

도메인이 일시 중지되며 인터넷에서 접속할 수 없습니다. 확인 이메일을 다시 보내려면 도메인 등록 확인 이메일을 다시 보내려면 단원을 참조하십시오.

지리적 TLD 전용 - 도메인을 Amazon Route 53으로 이전

지리적 TLD가 있는 도메인을 이전하는 경우 이전을 취소합니다. 권한 부여 이메일을 다시 보내려면 도메인 이전 권한 부여 이메일을 다시 보내려면 단원을 참조하십시오.

> **Note**
>
> .com, .net, .org 같은 일반 TLD가 있는 도메인에는 권한 부여가 필요 없습니다.

도메인 등록자 연락처(소유자)의 이름 또는 이메일 주소 변경

변경이 취소됩니다. 권한 부여 이메일을 다시 보내려면 등록자 연락처 업데이트나 도메인 삭제를 위해 권한 부여 이메일을 다시 보내려면 단원을 참조하십시오.

도메인 삭제

삭제 요청이 취소됩니다. 권한 부여 이메일을 다시 보내려면 등록자 연락처 업데이트나 도메인 삭제를 위해 권한 부여 이메일을 다시 보내려면 단원을 참조하십시오.

지리적 TLD 전용 - 도메인을 Route 53에서 다른 등록 기관으로 이전

지리적 TLD가 있는 도메인을 이전하는 경우 새 등록자가 이전을 취소합니다.

> **Note**
>
> .com, .net, .org 같은 일반 TLD가 있는 도메인에는 권한 부여가 필요 없습니다.

주제

이메일 주소 업데이트

확인 및 권한 부여 이메일은 항상 도메인 등록자 연락처의 이메일 주소로 발송합니다. 일부 TLD의 경우, 다음과 같은 사례에서는 등록자 연락처의 이전 이메일 주소와 새 이메일 주소로 이메일을 발송해야 합니다.

- 이미 Amazon Route 53에 등록된 도메인의 이메일 주소를 변경하는 경우
- Route 53으로 이전하는 도메인의 이메일 주소를 변경하는 경우

이메일 다시 보내기

해당 절차를 사용하여 확인 이메일 또는 권한 부여 이메일을 다시 보냅니다.

- 도메인 등록 확인 이메일을 다시 보내려면
- 도메인 이전 권한 부여 이메일을 다시 보내려면
- 등록자 연락처 업데이트나 도메인 삭제를 위해 권한 부여 이메일을 다시 보내려면

도메인 등록 확인 이메일을 다시 보내려면

1. 등록자 연락처의 이메일 주소를 확인하고 필요하다면 업데이트합니다. 자세한 내용은 도메인 연락처 정보 및 소유권 업데이트 단원을 참조하십시오.
2. 이메일 애플리케이션의 스팸 폴더에 다음 이메일 주소 중 하나에서 온 이메일이 있는지 확인합니다.

   너무 많은 시간이 경과하면 링크가 더 이상 작동하지 않지만 다른 이메일을 보내면 어디서 확인 이메일을 찾아야 하는지 알 수 있습니다.

TLD	승인 또는 확인 이메일이 발송되는 이메일 주소
.fr	nic@nic.fr

TLD	승인 또는 확인 이메일이 발송되는 이메일 주소
기타 모두	다음 이메일 주소 중 하나: • noreply@registrar.amazon • noreply@domainnameverification.net

> **Note**
>
> 이 이메일에는 www.verify-whois.com으로 연결되는 링크가 포함되어 있을 수 있습니다. 이 링크는 안전하게 사용할 수 있습니다.

3. Amazon Route 53 콘솔을 사용하여 확인 이메일을 다시 보냅니다.

   a. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
   b. 탐색 창에서 등록된 도메인을 선택합니다.
   c. 이메일을 다시 보내려는 도메인의 이름을 선택합니다.
   d. "Your domain might be suspended"라는 제목의 경고 상자에서 [Send email again]을 선택합니다.

   > **Note**
   >
   > 경고 상자가 없다면 등록자 연락처의 이메일 주소가 유효하다고 이미 확인된 것입니다.

4. 확인 이메일을 다시 보내는 동안 문제가 발생하면 AWS Support에 무료로 문의할 수 있습니다. 자세한 내용은 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.

도메인 이전 권한 부여 이메일을 다시 보내려면

이 방법은.jp 도메인 이전 요청에는 작동하지 않습니다.

1. 현재 도메인 등록 대행자가 제공하는 방법을 사용하여 도메인의 개인 정보 보호가 비활성화되어 있는지 확인합니다. 비활성화되어 있지 않다면 비활성화합니다.

현재 등록 대행자가 WHOIS 데이터베이스에 저장한 이메일 주소로 승인 이메일을 보냅니다. 개인 정보 보호가 활성화되어 있으면 일반적으로 해당 이메일 주소를 알아내기가 어렵습니다. Amazon Route 53가 WHOIS 데이터베이스의 이메일 주소로 보내는 이메일을 현재 등록 기관이 사용자의 실제 이메일 주소로 전달하지 못할 수 있습니다.

> **Note**
>
> 도메인의 현재 등록 대행자가 귀하의 프라이버시 보호 해제를 허가하지 않는 경우, 귀하가 5단계: 이전 요청에 유효한 승인 코드를 지정했다면 도메인을 이전할 수 있습니다.

2. 등록자 연락처의 이메일 주소를 확인하고 필요하다면 업데이트합니다. 도메인의 현재 등록 대행자가 제공하는 방법을 사용하십시오.
3. 이메일 애플리케이션의 스팸 폴더에 다음 이메일 주소 중 하나에서 온 이메일이 있는지 확인합니다.

   너무 많은 시간이 경과하면 링크가 더 이상 작동하지 않지만 다른 이메일을 보내면 인증 이메일을 어디서 찾아야 하는지 알 수 있습니다.

TLD	승인 또는 확인 이메일이 발송되는 이메일 주소
.com.au 및 .net.au	no-reply@ispapi.net 이 이메일에 https://approve.domainadmin.com에 대한 링크가 포함됩니다.
.fr	nic@nic.fr
기타 모두	다음 이메일 주소 중 하나: • noreply@registrar.amazon • noreply@domainnameverification.net

> **Note**
>
> 이 이메일에는 www.verify-whois.com으로 연결되는 링크가 포함되어 있을 수 있습니다. 이 링크는 안전하게 사용할 수 있습니다.

4. 이전이 더 이상 진행되지 않는 경우(너무 많은 시간이 경과하여 이미 취소된 경우) 이전을 다시 요청하시면 승인 이메일이 다시 전송됩니다.

> **Note**
>
> 이전을 요청한 후 처음 15일 동안은 Route 53 콘솔의 대시보드 페이지에 있는 알림 테이블을 확인하여 이전 상태를 확인할 수 있습니다. 15일 후 AWS CLI 를 사용하여 상태를 가져옵니다. 자세한 내용은 AWS CLI 명령 참조에서 route53domains를 참조하세요.

   이전이 여전히 진행 중이면 다음 단계를 수행하여 권한 확인 이메일을 다시 보내십시오.

   a. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
   b. 알림 테이블에서 이전하고자 하는 도메인의 이름을 찾습니다.
   c. 해당 도메인의 상태 열에서 Resend email(이메일 다시 보내기)을 선택합니다.

5. 도메인 전송에 대한 권한 부여 이메일을 재전송하는 동안 문제가 발생하면 AWS Support에 무료로 문의할 수 있습니다. 자세한 내용은 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.

등록자 연락처 업데이트나 도메인 삭제를 위해 권한 부여 이메일을 다시 보내려면

1. 등록자 연락처의 이메일 주소를 확인하고 필요하다면 업데이트합니다. 자세한 내용은 도메인 연락처 정보 및 소유권 업데이트 단원을 참조하십시오.
2. 이메일 애플리케이션의 스팸 폴더에 다음 이메일 주소 중 하나에서 온 이메일이 있는지 확인합니다.

   너무 많은 시간이 경과하면 링크가 더 이상 작동하지 않지만 다른 이메일을 보내면 인증 이메일을 어디서 찾아야 하는지 알 수 있습니다.

TLD	권한 부여 이메일을 발송하는 이메일 주소
.fr	nic@nic.fr
기타 모두	다음 이메일 주소 중 하나: • noreply@registrar.amazon • noreply@domainnameverification.net

> **Note**
>
> 이 이메일에는 www.verify-whois.com으로 연결되는 링크가 포함되어 있을 수 있습니다. 이 링크는 안전하게 사용할 수 있습니다.

3. 변경 또는 삭제를 취소합니다. 여기에는 두 가지 옵션이 있습니다.
   - 3~15일의 대기 기간 동안 기다릴 수 있으며, 이 기간이 지나면 요청된 작업이 자동으로 취소됩니다.
   - 또는 AWS Support에 문의하여 작업을 취소하도록 요청할 수 있습니다.
4. 변경 또는 삭제가 취소되면 연락처 정보를 변경하거나 도메인을 다시 삭제할 수 있습니다. 그러면 승인 이메일을 다시 보내드립니다.
5. 권한 부여 이메일을 재전송하는 동안 문제가 발생하면 AWS Support에 무료로 문의할 수 있습니다. 자세한 내용은 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.

도메인에 대해 DNSSEC 구성

때로 공격자는 DNS 쿼리를 가로채고 인터넷 엔드포인트의 실제 IP 주소 대신 자신의 IP 주소를 DNS 해석기로 반환하여 웹 서버와 같은 인터넷 엔드포인트로 전송되는 트래픽을 가로챕니다. 그러면 사용자는 공격자가 웹 사이트를 위조하기 위해 스푸핑한 응답의 IP 주소로 라우팅됩니다.

DNS 트래픽을 보호하는 프로토콜인 DNSSEC(Domain Name System Security Extensions)를 구성하여 DNS 스푸핑 또는 메시지 가로채기(man-in-the-middle) 공격으로 알려진 이러한 유형의 공격으로부터 도메인을 보호할 수 있습니다.

> **Important**
>
> Amazon Route 53는 도메인 등록을 위한 DNSSEC 서명 및 DNSSEC를 지원합니다. Route 53에 등록된 도메인에 대해 DNSSEC 서명을 구성하려면 Amazon Route 53에서 DNSSEC 서명 구성 섹션을 참조하세요.

주제

DNSSEC가 도메인을 보호하는 방법에 대한 개요

도메인에 대해 DNSSEC를 구성하면 DNS 해석기에서 중간 해석기의 응답에 대해 신뢰 체인을 구축합니다. 신뢰 체인은 도메인의 TLD 등록 기관(도메인의 상위 영역)으로 시작하여 DNS 서비스 공급자의 권한 있는 이름 서버로 끝납니다. 모든 DNS 해석기가 DNSSEC를 지원하는 것은 아닙니다. DNSSEC를 지원하는 해석기만 서명 또는 인증 검사를 수행합니다.

다음은 Amazon Route 53에 등록된 도메인에 대해 DNSSEC를 구성하여 DNS 스푸핑으로부터 인터넷 호스트를 보호하는 방법으로, 명확성을 위해 간단하게 정리했습니다.

1. DNS 서비스 공급자가 제공한 방법을 사용하여 비대칭 키 페어의 프라이빗 키로 호스팅 영역의 레코드에 서명합니다.

> **Important**
>
> Route 53는 도메인 등록을 위한 DNSSEC 서명 및 DNSSEC를 지원합니다. 자세한 내용은 Amazon Route 53에서 DNSSEC 서명 구성을 참조하십시오.

2. 도메인 등록자에게 키 페어의 퍼블릭 키를 제공하고 키 페어를 생성하는 데 사용했던 알고리즘을 지정합니다. 도메인 등록자는 최상위 도메인(TLD)의 등록 기관에 퍼블릭 키와 알고리즘을 전달합니다.

   Route 53에 등록한 도메인에 대해 이 단계를 수행하는 방법에 대한 자세한 내용은 도메인의 퍼블릭 키 추가 섹션을 참조하세요.

다음은 DNSSEC를 구성한 후 DNS 스푸핑으로부터 도메인을 보호하는 방법입니다.

1. 웹 사이트를 탐색하거나 이메일 메시지를 보내는 등의 방식으로 DNS 쿼리를 제출합니다.
2. 요청이 DNS 해석기로 라우팅됩니다. 해석기는 요청에 따라 클라이언트에 적절한 값(예: 웹 서버 또는 이메일 서버를 실행 중인 호스트의 IP 주소)을 반환할 책임이 있습니다.
3. IP 주소가 DNS 해석기에 캐싱되는 경우(다른 사람이 동일한 DNS 쿼리를 이미 제출했고 해석기는 이미 값을 알고 있는 상황), 해석기는 요청을 제출한 클라이언트에 IP 주소를 반환합니다. 그런 다음 클라이언트는 이 IP 주소를 사용하여 호스트에 액세스합니다.

   IP 주소가 DNS 해석기에 캐싱되지 않는 경우, 해석기는 TLD 등록 기관에 있는 해당 도메인의 상위 영역으로 요청을 보냅니다. 그러면 두 개의 값이 반환됩니다.

   - 레코드에 서명하는 데 사용했던 프라이빗 키에 상응하는 퍼블릭 키인 DS(Delegation Signer) 레코드.
   - 도메인의 권한 있는 이름 서버의 IP 주소.
4. DNS 해석기에서 다른 DNS 해석기로 원래 요청을 보냅니다. 그 해석기에도 IP 주소가 없는 경우, 다른 해석기가 DNS 서비스 공급자의 이름 서버로 요청을 보낼 때까지 동일한 프로세스가 반복됩니다. 이름 서버는 다음과 같은 두 개의 값을 반환합니다.
   - 도메인의 레코드(예: example.com). 여기에는 일반적으로 호스트의 IP 주소가 들어 있습니다.
   - DNSSEC를 구성할 때 생성한 레코드의 서명.
5. DNS 해석기는 도메인 등록 기관 및 TLD 등록처로 전달된 등록 기관에 제공한 퍼블릭 키를 사용하여 다음과 같은 두 가지 작업을 합니다.
   - 신뢰 체인을 설정합니다.
   - DNS 서비스 공급자로부터 받은 서명된 응답이 유효하며 공격자의 악성 응답으로 교체되지 않았는지 확인합니다.
6. 응답이 인증된 경우, 해석기는 요청을 제출한 클라이언트에 값을 반환합니다.

   응답을 확인할 수 없는 경우, 해석기는 사용자에게 오류를 반환합니다.

도메인의 TLD 등록 기관에 해당 도메인의 퍼블릭 키가 없는 경우, 해석기는 DNS 서비스 공급자로부터 받은 응답을 사용하여 DNS 쿼리에 응답합니다.

도메인에 대해 DNSSEC를 구성하기 위한 사전 조건 및 최댓값

도메인에 대해 DNSSEC를 구성하려면 해당 도메인과 DNS 서비스 공급자가 다음과 같은 사전 조건을 충족해야 합니다.

- TLD 등록 기관이 DNSSEC를 지원해야 합니다. TLD 등록 기관이 DNSSEC를 지원하는지 여부를 알아보려면 Amazon Route 53에 등록할 수 있는 도메인 단원을 참조하십시오.
- 도메인의 DNS 서비스 공급자가 DNSSEC를 지원해야 합니다.

> **Important**
>
> Route 53는 도메인 등록을 위한 DNSSEC 서명 및 DNSSEC를 지원합니다. 자세한 내용은 Amazon Route 53에서 DNSSEC 서명 구성을 참조하십시오.

- Route 53에 도메인의 퍼블릭 키를 추가하려면 먼저 해당 도메인의 DNS 서비스 공급자로 DNSSEC를 구성해야 합니다.
- 도메인에 추가할 수 있는 퍼블릭 키 수는 해당 도메인의 TLD에 따라 다릅니다.
  - .com 및 .net 도메인 - 키 최대 13개
  - 그 밖의 모든 도메인 - 키 최대 4개

도메인의 퍼블릭 키 추가

키를 교체하거나 도메인에 대해 DNSSEC를 활성화하는 경우, 해당 도메인의 DNS 서비스 공급자로 DNSSEC를 구성한 뒤 다음 절차를 수행하십시오.

도메인의 퍼블릭 키를 추가하려면

1. 아직 DNS 서비스 공급자로 DNSSEC를 구성하지 않았다면 서비스 공급자가 알려 준 방법에 따라 DNSSEC를 구성합니다.
2. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
3. 탐색 창에서 등록된 도메인을 선택합니다.

4. 키를 추가할 도메인의 이름을 선택합니다.
5. DNSSEC 키 탭에서 키 추가를 선택합니다.
6. 다음 값을 지정하세요.

   키 유형

   업로드하려는 것이 KSK(키 서명 키)인지 아니면 ZSK(영역 서명 키)인지 선택합니다.

   알고리즘

   호스팅 영역의 레코드에 서명할 때 사용한 알고리즘을 선택합니다.

   퍼블릭 키

   DNS 서비스 공급자로 DNSSEC를 구성할 때 사용한 비대칭 키 페어에서 퍼블릭 키를 지정합니다.

   다음 사항에 유의하세요.

   - 다이제스트가 아닌 퍼블릭 키를 지정합니다.
   - 키는 base64 형식으로 지정해야 합니다.
7. 추가를 선택합니다.

> **Note**
>
> 퍼블릭 키는 한 번에 하나만 추가할 수 있습니다. 키를 더 추가하려면 Route 53으로부터 확인 이메일을 받을 때까지 기다려야 합니다.

8. 등록처의 응답이 Route 53에 수신되면 해당 도메인의 등록 기관 연락처로 이메일을 보내 드립니다. 이메일에서는 퍼블릭 키가 등록 기관의 도메인에 추가되었음을 확인하거나 키가 추가되지 않은 이유를 설명합니다.

도메인의 퍼블릭 키 삭제

키를 교체하거나 도메인에 대해 DNSSEC를 비활성화하는 경우, DNS 서비스 공급자로 DNSSEC를 비활성화하기 전에 다음 절차에 따라 퍼블릭 키를 삭제하십시오. 다음 사항에 유의하세요.

- 퍼블릭 키를 교체하는 경우, 새 퍼블릭 키를 추가하고 최대 3일 후에 이전 퍼블릭 키를 삭제하는 것이 좋습니다.

- DNSSEC를 비활성화하는 경우, 먼저 도메인의 퍼블릭 키를 삭제합니다. 최대 3일 후에 도메인의 DNS 서비스로 DNSSEC를 비활성화하는 것이 좋습니다.

> **Important**
>
> 도메인에 대해 DNSSEC가 활성화되어 있는데 DNS 서비스로 DNSSEC를 비활성화하는 경우, DNSSEC를 지원하는 DNS 해석기에서 클라이언트에 SERVFAIL 오류를 반환하므로 클라이언트는 해당 도메인과 연결된 엔드포인트에 액세스할 수 없습니다.

도메인의 퍼블릭 키를 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 등록된 도메인을 선택합니다.
3. 키를 삭제할 도메인의 이름을 선택합니다.
4. DNSSEC 키 탭에서 삭제할 키 옆에 있는 라디오 버튼을 선택한 다음 키 삭제를 선택합니다.
5. DNSSEC 키 삭제 대화 상자에서 텍스트 상자에 delete를 입력하여 삭제하려는 키를 확인하고 삭제를 선택합니다.

   > **Note**
   >
   > 퍼블릭 키는 한 번에 하나만 삭제할 수 있습니다. 키를 더 삭제하려면 Amazon Route 53으로부터 확인 이메일을 받을 때까지 기다려야 합니다.

6. 등록처의 응답이 Route 53에 수신되면 해당 도메인의 등록 기관 연락처로 이메일을 보내 드립니다. 이메일에서는 퍼블릭 키가 등록 기관의 도메인에 삭제되었음을 확인하거나 키가 삭제되지 않은 이유를 설명합니다.

등록 기관 및 도메인에 대한 기타 정보 찾기

GetDomainDetail API를 사용하여 도메인 정보를 보려면 SDK 또는 중 하나를 사용할 수 SDKs AWS CLI. 자세한 내용을 알아보려면 get-domain-detail 단원을 참조하세요.

`get-domain-detail` CLI로 도메인 정보 보기

- 다음 CLI 명령을 사용합니다.

```
aws route53domains get-domain-detail \
    --region us-east-1 \
    --domain-name example.com
```

> **Note**
>
> 이 명령은 us-east-1에서만 실행됩니다 AWS 리전.

등록 기관, 등록일, 개인 정보 보호 설정 등을 포함하여 도메인에 대한 모든 정보가 출력에 나열됩니다.

Route 53에 등록된 도메인에 대한 정보 보기

Route 53를 사용하여 등록한 도메인에 대한 정보를 볼 수 있습니다. 이 정보에는 도메인을 최초로 등록한 시기와 도메인 소유자, 기술 담당자, 관리자, 청구 담당자의 연락처 정보와 같은 세부 정보가 포함되어 있습니다.

WHOIS

WHOIS는 도메인 등록자 및 등록기관이 후원하는 도메인에 대한 정보가 포함된 무료 공개 디렉터리입니다. 포트 43에서 쿼리를 수락하는 서비스와 IPv4 및 IPv6를 통해 각각 액세스할 수 있는 웹 사이트로 제공됩니다. WHOIS는 분산형 계층 검색입니다. 자세한 내용은 About WHOIS 섹션을 참조하세요.

계층 구조의 여러 수준에 대한 WHOIS 요청을 통해 다양한 정보를 얻을 수 있습니다.

- 루트 WHOIS(whois.iana.org)에 대한 정보를 요청하면 레지스트리에 대한 정보가 제공됩니다.
- 레지스트리 WHOIS에 대한 정보를 요청하면 등록자에 대한 정보와 도메인에 대한 일부 공개 정보가 제공됩니다.
- 등록기관 WHOIS에 대한 요청은 도메인에 대한 모든 공개 정보를 제공합니다.

TLD 레지스트리 및 도메인 등록 대행사에서 운영하는 WHOIS 조회를 비롯하여 여러 수준의 WHOIS가 있기 때문에 Route 53 콘솔에서 개인 정보 보호를 해제하면 등록자가 제공한 WHOIS에서만 개인 정보 보호 기능이 해제될 수 있습니다. 일부 레지스트리는 Route 53에서 WHOIS 조회 서비스를 비활성화했는지 여부와 상관없이 의도적으로 WHOIS 조회 서비스에 대한 개인 정보 보호 또는 수정 서비스를 유

지합니다. 도메인에 대한 전체 정보를 얻으려면 등록자에서 제공하는 WHOIS를 사용하는 것이 좋습니다.

다음 사항에 유의하세요.

개인 정보 보호가 활성화된 경우 도메인 연락처에 이메일 보내기

도메인에 대해 개인 정보 보호가 활성화되어 있는 경우 등록자, 기술 담당자 및 관리자에 대한 연락처 정보가 Amazon Registrar 개인 정보 보호 서비스의 연락처 정보로 바뀝니다. 예를 들어 example.com 도메인이 Amazon Registrar에 등록되고 개인 정보 보호가 활성화된 경우, WHOIS 쿼리에 대한 응답의 등록자 이메일 값은 oowner1234@example.com.identity-protect.org와 비슷합니다.

개인 정보 보호가 활성화된 상태에서 하나 이상의 도메인 연락처에 연락하려면 해당 이메일 주소로 이메일을 보냅니다. 귀하의 이메일은 해당 연락처로 자동 전달됩니다.

남용 신고

부적절한 콘텐츠, 피싱, 맬웨어 또는 스팸을 포함하여 허용 가능한 사용 정책의 불법 활동 또는 위반을 보고하려면 trustandsafety@support.aws.com으로 이메일을 보내세요.

Route 53에 등록된 도메인에 대한 정보 보기

1. 웹 브라우저에서 다음 웹 사이트 중 하나로 이동합니다.
   - Amazon Registrar WHOIS: https://registrar.amazon.com/whois
   - Amazon Registrar RDAP: https://registrar.amazon.com/rdap
   - Gandi WHOIS: https://whois.gandi.net
2. 정보를 보려는 도메인의 이름을 입력하고 검색을 선택합니다.

도메인 이름 등록 삭제

TLD(최상위 도메인)에 대해 등록을 더 이상 원하지 않는 경우 등록을 삭제할 수 있습니다. 등록 기관에서 등록을 삭제하도록 허용하는 경우 이 항목의 절차를 수행하십시오.

다음 사항에 유의하세요.

등록 수수료는 환불되지 않습니다.

등록이 만료되기 전에 도메인 이름 등록을 삭제할 경우 AWS 는 등록 수수료를 환불하지 않습니다.

도메인 등록을 삭제할 수 있는 TLD

도메인 등록 삭제 가능 여부를 알아보려면 Amazon Route 53에 등록할 수 있는 도메인 단원을 참조하십시오. TLD 섹션에 "도메인 등록 삭제" 하위 항목이 없는 경우 도메인을 삭제할 수 있습니다. 도메인을 삭제하기 전에 도메인 잠금을 비활성화했는지 확인하세요. 도메인 잠금 비활성화에 대한 자세한 내용은 DisableDomainTransferLock을 참조하세요.

도메인 등록을 삭제할 수 없으면 어떻게 해야 합니까?

도메인 등록 기관에서 도메인 이름 등록 삭제를 허용하지 않는 경우 도메인이 만료될 때까지 기다려야 합니다. 도메인이 자동으로 갱신되지 않도록 하려면 도메인의 자동 갱신을 비활성화하십시오. 만료(Expires on) 날짜가 지나면, Route 53는 자동으로 도메인에 대한 등록을 삭제합니다. 자동 갱신 설정을 변경하는 방법에 대한 자세한 내용은 도메인 자동 갱신 활성화 또는 비활성화 단원을 참조하십시오.

도메인 삭제 후 다시 등록할 수 있을 때까지의 기간

대부분의 등록 기관에서는 만료된 도메인을 즉시 등록할 수 없습니다. 일반적인 기간은 TLD에 따라 1 ~ 3개월입니다. 자세한 내용은 Amazon Route 53에 등록할 수 있는 도메인의 TLD에 대한 “도메인 갱신 및 복원 기한” 단원을 참조하십시오.

> **Important**
>
> 도메인을 삭제하지 말고 AWS 계정 간에 도메인을 이전하거나 도메인을 다른 등록 기관으로 이전하려는 경우 다시 등록해야 합니다. 대신 해당 설명서를 참조하십시오.
>
> - 도메인을 다른 AWS 계정으로 이전
> - Amazon Route 53에서 다른 등록 기관으로 도메인 이전하기

도메인 이름 등록을 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 등록된 도메인을 선택합니다.
3. 도메인 이름을 선택합니다.

   .co.uk, .me.uk, .org.uk, 또는 .uk 도메인을 삭제하려면 .co.uk, .me.uk, .org.uk, .uk 도메인 이름 등록을 삭제하려면 섹션을 참조하세요.
4. TLD 레지스트리에서 도메인 이름 등록을 삭제하도록 허용하면, 도메인 삭제를 선택합니다.

일부 도메인은 등록자가 도메인 삭제를 원하는지 확인하기 위한 이메일을 도메인 등록자에게 전송하도록 요구합니다. 이메일을 수신하는 경우 다음 이메일 주소 중 하나에서 발송됩니다.

- noreply@registrar.amazon - Amazon Registrar에 등록된 TLDs 경우.
- noreply@domainnameverification.net - 등록 기관 협력사 Gandi에서 등록한 TLD의 경우.

TLD의 등록 기관을 확인하려면 Amazon Route 53에 등록할 수 있는 도메인을 참조하세요.

5. 확인 이메일을 수신하면 이메일의 링크를 선택한 후 도메인 삭제 요청을 수락하거나 거절합니다.

> **Important**
>
> 등록 담당자는 즉시 이메일의 지시 사항에 따라야 합니다. 그렇지 않으면 ICANN의 요구에 따라 1일 후 삭제 요청을 취소할 수밖에 없습니다.

도메인이 삭제되면 또 다른 이메일이 전송됩니다. 귀하의 요청이 현재 어떤 처리 상태에 있는지 확인하시려면, 다음(도메인 등록 상태 보기)을 참조하십시오.

6. 삭제된 도메인에 대해 호스팅 영역의 레코드를 삭제한 후 호스팅 영역을 삭제합니다. 호스팅 영역을 삭제하면 Route 53는 호스팅 영역에 대한 월별 요금 청구를 중지합니다. 자세한 내용은 다음 설명서를 참조하세요.

   - 레코드 삭제
   - 퍼블릭 호스팅 영역 삭제
   - Route 53 가격

7. 도메인 이름 등록을 삭제하는 동안 문제가 발생하면 AWS Support에 무료로 문의할 수 있습니다. 자세한 내용은 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.

.co.uk, .me.uk, .org.uk, .uk 도메인 이름 등록을 삭제하려면

.co.uk, .me.uk, .org.uk, .uk 도메인을 삭제하려면 .uk 도메인에 대한 레지스트리인 Nominet을 사용하여 계정을 만듭니다. 자세한 내용은 Nominet 웹 사이트 https://www.nominet.uk/domain-support/의 “도메인 이름 취소”를 참조하십시오.

> **Important**
>
> .uk 도메인 이름을 삭제(취소)하면 며칠 내에 삭제되고 누구나 등록할 수 있게 됩니다. 도메인을 이전하기만 하려는 경우에는 삭제하지 마십시오.

다음은 이 프로세스를 요약한 것입니다.

1. Nominet 웹 사이트에서 처음으로 로그인하기 위한 지침을 따르십시오. https://secure.nominet.org.uk/auth/login.html을 참조하십시오. Nominet은 암호 생성 지침이 포함된 이메일을 발송합니다.
2. Nominet에서 받은 이메일의 지침을 따릅니다.
3. Nominet 웹 사이트에 로그인하고 도메인 이름 취소(삭제) 지침을 따릅니다.

도메인 등록 문제에 대한 AWS 지원 문의

AWS 는 모든 AWS 고객에게 기본 지원 플랜을 무료로 제공합니다. 이 계획에는 도메인 등록과 관련된 다음과 같은 문제에 대한 지원이 포함됩니다.

- 도메인의 Amazon Route 53으로 이전
- AWS 계정 간 도메인 전송
- 등록 가능한 도메인 수와 같은 Route 53 엔터티의 할당량 상향(할당량 참조)
- 도메인 소유자 변경
- 도메인 소유자의 연락처 정보 변경
- 확인 및 권한 부여 이메일 재전송
- 도메인 갱신
- 만료된 도메인 복원
- Route 53 청구 관련 정보 가져오기
- .uk 도메인에 대한 신분 증명서 제공
- AWS 계정을 해지한 후 도메인 삭제 또는 자동 갱신 비활성화

이러한 문제 및 도메인 등록과 관련된 기타 문제에 대해 AWS Support에 문의하려면 해당 절차를 수행합니다.

주제

AWS 계정에 로그인할 수 있는 경우 AWS Support에 문의

AWS 계정에 로그인할 수 있을 때 AWS Support에 문의하려면 다음 절차를 수행합니다.

1. 도메인이 현재 등록된 AWS 계정을 사용하여 AWS 지원 센터에 로그인합니다.

   > **Important**
   >
   > 도메인이 현재 등록되어 있는 루트 계정을 이용해 로그인해야 합니다. 이는 권한이 없는 사용자가 계정을 탈취하는 것을 방지하기 위한 조치입니다.

2. 다음 값을 지정하세요.

   관련

   [Account and Billing Support]의 기본값을 수락합니다.

   Service

   도메인의 기본값을 수락합니다.

   범주

   등록 문제의 기본값을 수락합니다.

   심각도

   다음 중 심각도를 선택합니다.

   제목

   문제를 간단히 요약합니다.

   설명

   문제를 상세히 설명하고 관련 문서나 스크린샷이 있으면 첨부합니다.

   연락 방법

   연락 방법인 웹을 선택합니다. AWS 계정과 연결된 이메일 주소를 사용하여 연락드리겠습니다.

3. 제출을 선택합니다.

AWS 계정에 로그인할 수 없는 경우 AWS Support에 문의

AWS 계정에 로그인할 수 없을 때 AWS Support에 문의하려면 다음 절차를 수행합니다.

1. 고객인데 결제 또는 계정 지원 페이지를 찾고 AWS 있습니다.
2. 양식을 작성합니다.
3. 제출을 선택합니다.

도메인 결제 보고서 다운로드

여러 도메인을 관리하는 경우 지정된 기간 동안 도메인별 요금을 보려면 도메인 결제 보고서를 다운로드할 수 있습니다. 이 보고서에는 다음 항목을 포함하여 도메인 등록에 적용되는 모든 요금이 포함됩니다.

- 도메인 등록
- 도메인 등록 갱신
- 도메인의 Amazon Route 53으로 이전
- 도메인 소유자 변경(일부 TLD의 경우 이 작업은 무료임)

도메인 자동 갱신 프로세스는 도메인 만료 한 달 전부터 시작되므로 때때로 청구 보고서에 현재 시점이 아닌 미래 기간의 청구 내용이 표시될 수 있습니다. 예를 들어 도메인이 만료되기 한 달 전인 8월 보고서에서 9월 이후 청구 기간이 시작되어 다음 해 9월까지 적용되는 청구 기간이 표시될 수 있습니다.

콘솔을 사용하여 보고서를 실행할 때 다음 옵션을 선택할 수 있습니다.

- 지난 12개월: 보고서에는 보고서를 실행하기 1년 전부터 현재 날짜까지의 요금이 포함됩니다. 예를 들어 6월 3일에 보고서를 실행하면 전년도 6월 3일부터 당일까지의 요금이 포함됩니다.
- 작년의 개별 개월: 보고서에는 지정된 달의 요금이 포함됩니다.

보고서를 프로그래밍 방식으로 실행하는 경우 2014년 7월 31일부터 원하는 날짜 범위의 요금을 볼 수 있습니다. 이 날짜는 Route 53에서 도메인 등록을 지원하기 시작한 날짜입니다. 예를 들어AWS CLI 명령 참조의 view-billing 섹션을 참조하세요.

결제 보고서는 CSV 형식이며 내용은 ViewBilling API에 설명되어 있습니다.

도메인 결제 보고서를 다운로드하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 [Registered Domains]를 선택합니다.
3. [Domain billing report]를 선택합니다.
4. 보고서의 날짜 범위를 선택한 다음 [Download domain report]를 선택합니다.
5. 메시지에 따라 보고서를 열거나 저장합니다.
6. 도메인 결제 보고서를 다운로드하는 동안 문제가 발생하면 AWS Support에 무료로 문의할 수 있습니다. 자세한 내용은 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.

Amazon Route 53에 등록할 수 있는 도메인

> **Important**
>
> Route 53 DNS 서비스는 선택한 모든 최상위 도메인 및 도메인 등록 기관과 함께 사용할 수 있습니다. 이 페이지의 정보는 Route 53에 등록 가능한 도메인에만 적용됩니다. Route 53를 DNS 서비스로 사용에 대한 자세한 내용은 웹 사이트 또는 웹 애플리케이션으로 인터넷 트래픽을 라우팅하는 방식 섹션을 참조하세요.

다음의 일반 및 지리적 최상위 도메인 목록에는 Amazon Route 53에 도메인을 등록하는 데 사용할 수 있는 최상위 도메인(TLD)이 나와 있습니다.

Route 53에 도메인 등록

TLD는 일부 도메인 이름에 특별 또는 프리미엄 가격을 지정하고 있습니다. Route 53를 사용하여 특별 또는 프리미엄 가격이 적용되는 도메인을 등록할 수 없습니다. Route 53에 등록할 수 있는 TLD는 다음 목록에 포함되어 있습니다. TLD가 포함되지 않은 경우에는 Route 53에 도메인을 등록할 수 없습니다.

Route 53으로 도메인 이전

다음 목록에 TLD가 포함되어 있는 경우 도메인을 Route 53으로 이전할 수 있습니다. TLD가 포함되지 않은 경우 도메인을 Route 53으로 이전할 수 없습니다.

대부분의 TLD의 경우 도메인을 이전하려면 현재 등록 대행자에서 권한 부여 코드를 얻어야 합니다. 권한 부여 코드가 필요한지 여부를 확인하려면 TLD에 대한 '이전하는 데 필요한 권한 부여 코드' 섹션을 참조하세요.

도메인 등록 및 이전 요금

도메인 등록 또는 Route 53으로 이전 요금에 대한 자세한 내용은 Amazon Route 53 도메인 등록 요금 문서를 참조하세요.

Route 53를 DNS 서비스로 사용

TLD이 다음 목록에 포함되지 않은 경우에도 Route 53를 임의 도메인의 DNS 서비스로 사용할 수 있습니다. Route 53를 DNS 서비스로 사용에 대한 자세한 내용은 웹 사이트 또는 웹 애플리케이션으로 인터넷 트래픽을 라우팅하는 방식 섹션을 참조하세요. 도메인의 DNS 서비스를 Route 53으로 이전하는 방법에 대한 자세한 내용은 Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정 섹션을 참조하세요.

다국어 도메인 이름

모든 TLD가 다국어 도메인 이름(IDN)을 지원하는 것은 아닙니다. IDN이란 ASCII 문자 a-z, 0-9 및 -(하이픈) 이외의 문자를 포함한 도메인 이름을 의미합니다. 각 TLD의 목록에는 해당 TLD가 IDN을 지원하는지 여부가 표시됩니다. 국제화 도메인 이름에 대한 자세한 내용은 DNS 도메인 이름 형식을 참조하십시오.

TLD로 지리적 도메인 등록

지리적 TLD 등록 규칙은 나라마다 다릅니다. 세상 사람 누구나 등록할 수 있도록 제한을 두지 않는 나라도 있고, 거주자 등으로 제한하는 나라도 있습니다. 각 지리적 TLD의 목록에는 제한 사항이 표시됩니다.

지원되는 최상위 도메인에 대한 인덱스

주제

일반적인 최상위 도메인

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | WXYZ

A

.ac, .academy, .accountants, .actor, .adult, .agency, .airforce, .apartments, .associates, .auction, .audio

B

.band, .bargains, .beer,.bet, .bid, .bike, .bingo, .bio, .biz, .black, .blue, .boutique, .builders, .business, .buzz

C

.cab, .cafe, .camera, .camp, .capital, .cards, .care, .careers, .cash, .casino, .catering, .cc, .center, .ceo, .chat, .cheap, .christmas, .church, .city, .claims, .cleaning, .click, .clinic, .clothing, .cloud, .club, .coach, .codes, .coffee, .college, .com, .community, .company, .computer, .condos, .construction, .consulting, .contact, .contractors, .cool, .coupons, .credit, .creditcard, .cruises

D

.dance, .dating, .deals, .degree, .delivery, .democrat, .dental, .design, .diamonds, .diet, .digital, .direct, .directory, .discount, .dog, .domains

E

.education, .email, .energy, .engineering, .enterprises, .equipment, .estate, .events, .exchange, .expert, .exposed, .express

F

.fail, .fan, .farm, .finance, .financial, .fish, .fitness, .flights, .florist, .flowers, .fm, .football, .forsale, .foundation, .fun, .fund, .furniture, .futbol, .fyi

G

.gallery, .games, .gift, .gifts, .gives, .glass, .global, .gmbh, .gold, .golf, .graphics, .gratis, .green, .gripe, .group, .guide, .guitars, .guru

H

.haus, .healthcare, .help, .hiv, .hockey, .holdings, .holiday, .host, .hosting, .house

I

.im, .immo, .immobilien, .industries, .info, .ink, .institute, .insure, .international, .investments, .io, .irish

J

.jewelry, .juegos

K

.kaufen, .kim, .kitchen, .kiwi

L

.land, .law, .lease, .legal, .lgbt, .life, .lighting, .limited, .limo, .link, .live, .llc, .loan, .loans, .lol, .ltd

M

.maison, .management, .marketing, .mba, .media, .memorial, .mobi, .moda, .money, .mortgage, .movie

N

.name, .net, .network, .news, .ninja

O

.onl, .online, .org

P

.partners, .parts, .photo, .photography, .photos, .pics, .pictures, .pink, .pizza, .place, .plumbing, .plus, .poker, .porn, .press, .pro, .productions, .properties, .property, .pub. .pw(팔라우)

Q

.qpon

R

.recipes, .red, .reise, .reisen, .rentals, .repair, .report, .republican, .restaurant, .reviews, .rip, .rocks, .run

S

.sale, .sarl, .school, .schule, .services, .sex, .sexy, .shiksha, .shoes, .shopping, .show, .singles, .site, .ski, .soccer, .social, .solar, .solutions, .software, .space, .store, .stream, .studio, .style, .sucks, .supplies, .supply, .support, .surgery, .systems

T

.tattoo, .tax, .taxi, .team, .tech,.technology, .tennis, .theater, .tienda, .tips, .tires, .today, .tools, .tours, .town, .toys, .trade, .training, .tv

U

.university, .uno

V

.vacations, .vegas, .ventures, .vg, .viajes, .video, .villas, .vision, .vote, .voyage

WXYZ

.watch, .website, .wedding, .wiki, .wine, .work, .works, .world, .wtf, .xyz, .zone

지리적 최상위 도메인

아프리카

.ac(어센션 섬), .co.za(남아프리카), .sh(세인트 헬레나)

북남미

.ca(캐나다), .cl(칠레), .co(콜롬비아), .com.ar(아르헨티나), .com.br(브라질), .com.mx(멕시코), .mx(멕시코), .us(미국), .vc(세인트 빈센트 그레나딘), .vg(영국령 버진 제도)

아시아/오세아니아

.au(오스트레일리아), .cc(코코스(킬링) 제도), .co.nz(뉴질랜드), .com.au(호주), .com.sg(싱가포르), .fm(미크로네시아 연방 공화국), .in(인도), .jp(일본), .io(영국령 인도양 식민지), .net.au(호주), .net.nz (뉴질랜드), .org.nz(뉴질랜드), .pw(팔라우), .qa(카타르), .ru(러시아 연방), .sg(싱가포르)

유럽

.be(벨기에), .berlin(독일 베를린 시), .ch(스위스), .co.uk(영국), .cz(체코 공화국), .de(독일), .es(스페인) , .eu(유럽 연합), .fi(핀란드), .fr(프랑스), .gg(건지), .im(맨 섬), .it(이탈리아), .me(몬테네그로), .me.uk(영국), .nl(네덜란드), .org.uk(영국), .ruhr(독일 서부 루르 지방), .se(스웨덴), .uk(영국), .wien(오스트리아 비엔나 시)

일반적인 최상위 도메인

gTLD(일반적인 최상위 도메인)란 .com, .net, .org 등 전 세계 어디서나 사용되고 인식되는 전역 확장명입니다. .bike, .condos, .marketing 같은 특수 도메인도 여기에 포함됩니다.

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | WXYZ

A

.ac, .academy, .accountants, .actor, .adult, .agency, .airforce, .apartments, .associates, .auction, .audio

B

.band, .bargains, .beer, .bet, .bid, .bike, .bingo, .bio, .biz, .black, .blue, .boutique, .builders, .business, .buzz

C

.cab, .cafe, .camera, .camp, .capital, .cards, .care, .careers, .cash, .casino, .catering, .cc, .center, .ceo, .chat, .cheap, .church, .christmas, .city, .claims, .cleaning, .click, .clinic, .clothing, .cloud, .club, .coach, .codes, .coffee, .college, .com, .community, .company, .computer, .condos, .construction, .consulting, .contact, .contractors, .cool, .coupons, .credit, .creditcard, .cruises

D

.dance, .dating, .deals, .degree, .delivery, .democrat, .dental, .design, .diamonds, .diet, .digital, .direct, .directory, .discount, .dog, .domains

E

.education, .email, .energy, .engineering, .enterprises, .equipment, .estate, .events, .exchange, .expert, .exposed, .express

F

.fail, .fan, .farm, .finance, .financial, .fish, .fitness, .flights, .florist, .flowers, .fm, .football, .forsale, .foundation, .fun, .fund, .furniture, .futbol, .fyi

G

.gallery, .games, .gift, .gifts, .gives, .glass, .global, .gmbh, .gold, .golf, .graphics, .gratis, .green, .gripe, .group, .guide, .guitars, .guru

H

.haus, .healthcare, .help, .hiv, .hockey, .holdings, .holiday, .host, .hosting, .house

I

.im, .immo, .immobilien, .industries, .info, .ink, .institute, .insure, .international, .investments, .io, .irish

J

.jewelry, .juegos

K

.kaufen, .kim, .kitchen, .kiwi

L

.land, .law, .lease, .legal, .lgbt, .life, .lighting, .limited, .limo, .link, .live, .llc, .loan, .loans, .lol , .ltd

M

.maison, .management, .marketing, .mba, .media, .memorial, .mobi, .moda, .money, .mortgage, .movie

N

.name, .net, .network, .news, .ninja

O

.onl, .online, .org

P

.partners, .parts, .photo, .photography, .photos, .pics, .pictures, .pink, .pizza, .place, .plumbing, .plus, .poker, .porn, .press, .pro, .productions, .properties, .property, .pub

Q

.qpon

R

.recipes, .red, .reise, .reisen, .rentals, .repair, .report, .republican, .restaurant, .reviews, .rip, .rocks, .run

S

.sale, .sarl, .school, .schule, .services, .sex, .sexy, .shiksha, .shoes, .shopping, .show, .singles, .site, .ski, .soccer, .social, .solar, .solutions, .software, .space, .store, .stream, .studio, .style, .sucks, .supplies, .supply, .support, .surgery, .systems

T

.tattoo, .tax, .taxi, .team,.tech, .technology, .tennis, .theater, .tienda, .tips, .tires, .today, .tools, .tours, .town, .toys, .trade, .training, .tv

U

.university, .uno

V

.vacations, .vegas, .ventures, .vg, .viajes, .video, .villas, .vision, .vote, .voyage

WXYZ

.watch, .website, .wedding, .wiki, .wine, .work, .works, .world, .wtf, .xyz, .zone

.ac

.ac(어센션 섬)을 참조하세요.

Return to index

.academy

학교, 대학 등 교육 기관에서 사용합니다. 채용 담당자, 상담자, 광고인, 학생, 교사 및 교육 기관 관련 업무를 하는 행정가들도 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.accountants

회계 관련 기업, 단체 및 관계자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.actor

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 75일

.adult

성인용 콘텐츠를 호스팅하는 웹 사이트에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.agency

기관으로 분류되는 단체 또는 기업체에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.airforce

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.apartments

부동산 중개인, 임대주 및 임차인이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.associates

직함에 "어소시에이트"라는 단어를 포함시키는 기업 및 회사에서 사용합니다. 또한 조직의 전문성을 나타내고자 하는 단체 또는 기관에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.auction

경매 및 경매 방식 매매와 관련된 행사에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어 및 라틴어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지

- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.audio

> **Important**
>
> 더 이상 Route 53를 사용하여 새 .audio 도메인을 등록하거나 .audio 도메인을 Route 53으로 이전할 수 없습니다. 이미 Route 53에 등록된 .audio 도메인은 계속 지원됩니다.

시청각 산업을 비롯하여 방송, 음향 기기, 오디오 제작 및 오디오 스트리밍에 관심이 있는 누구나 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

키릴 자모(주로 러시아어), 프랑스어, 독일어, 이탈리아어, 포르투갈어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

지원하지 않음. 더 이상 Route 53으로 .audio 도메인을 이전할 수 없습니다.

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.band

음악 밴드 및 밴드 행사에 대한 정보를 공유하는 데 사용됩니다. 또한 뮤지션이 팬과 소통하고 밴드 관련 상품을 판매하는 데 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어 및 라틴어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지

- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.bargains

영업 및 프로모션 관련 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 75일

.beer

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.bet

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.bid

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.bike

자전거 매장, 오토바이 판매점, 수리점 등 자전거 애호가를 위한 맞춤 서비스 제공 단체 또는 기업체에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.bingo

온라인 게임 웹 사이트에서 사용되거나 빙고 게임에 대한 정보를 공유하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.bio

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지

- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.biz

기업용 또는 영리 목적으로 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어(간체), 중국어(번체), 덴마크어, 핀란드어, 독일어, 헝가리어, 일본어, 한국어, 라트비아어, 리투아니아어, 노르웨이어, 폴란드어, 포르투갈어, 스페인어, 스웨덴어가 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.black

검은색을 좋아하는 경우 또는 기업 이미지나 브랜드에서 검은색을 떠올리게 하려는 경우에 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.blue

파란색을 좋아하는 경우 또는 기업 이미지나 브랜드에서 파란색을 떠올리게 하려는 경우에 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.boutique

부티크 또는 소규모 전문점에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.builders

건설업체 및 건설업 관계자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.business

모든 유형의 기업에서 사용합니다. .biz 확장명 대신 사용할 수 있습니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.buzz

최신 뉴스 및 이벤트 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지

- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.cab

택시업체 및 택시 업종 관계자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.cafe

카페 사업체 및 카페 문화에 관심이 있는 사람이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.camera

사진 애호가이거나 사진을 공유하고 싶은 경우에 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.camp

공원과 휴양지, 여름 캠프, 작가 워크숍, 피트니스 캠프 및 캠핑 애호가들이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.capital

금융 자본 또는 도시 자본 등 모든 종류의 자본을 설명하는 일반 범주로 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.cards

e카드, 인쇄된 인사말 카드, 비즈니스 카드 및 플레잉 카드와 같은 카드를 전문으로 제작하는 기업에서 사용합니다. 또한 카드 게임의 규칙과 전략을 논의하고자 하는 게이머에게 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.care

요양 서비스를 제공하는 기업 또는 기관에서 사용합니다. 또한 자선 단체에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.careers

구인 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 75일

.cash

통화 관련 활동에 종사하는 조직, 단체 또는 개인이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.casino

도박 산업 또는 도박과 카지노 게임에 대한 정보를 공유하고자 하는 게이머가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.catering

요식업체 또는 음식 관련 행사에 대한 정보를 공유하는 사람이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.cc

.cc(코코스(킬링) 제도)을 참조하세요.

Return to index

.center

연구 기관에서 커뮤니티 센터까지 모든 것을 가리키는 일반 확장명입니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.ceo

CEO 및 고위 임원에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

독일어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

지원하지 않음.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.chat

모든 종류의 온라인 채팅 웹 사이트에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.cheap

전자 상거래 웹 사이트에서 저렴한 제품을 프로모션 및 판매할 때 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.christmas

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 43일까지
- Route 53에서 도메인 삭제: 만료 후 44일
- 레지스트리 복원: 만료 후 44일~86일
- 레지스트리에서 도메인 삭제: 만료 후 86일

.church

규모 또는 교파에 관계없이 모든 교회에서 신도와 소통하고 교회 관련 행사 및 활동에 대한 정보를 게시하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.city

안내 표시, 지역 명소 또는 근린 활동 등 특정 도시에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.claims

보험 청구를 처리하거나 법률 서비스를 제공하는 회사에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.cleaning

청소 서비스를 제공하는 기업 또는 개인이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.click

웹 사이트의 제품을 클릭하여 제품을 구매하는 것과 같이 웹 사이트에서 클릭 동작을 지원하고자 하는 기업에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

키릴 자모(주로 러시아어), 프랑스어, 독일어, 이탈리아어, 포르투갈어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.clinic

의료 산업 및 의료 전문가가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.clothing

소매업체, 백화점, 디자이너, 양복점 및 할인점 등 패션 산업 종사자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 75일

.cloud

일반 확장명으로 사용되나, 클라우드 컴퓨팅 기술 및 서비스를 제공하는 회사에 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.club

모든 유형의 클럽 또는 조직에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

스페인어 및 일본어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.coach

스포츠 전문가, 라이프스타일 코치 또는 기업 트레이너 등 지도하는 데 관심이 있는 누구나 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.codes

행동 강령, 건축 법규 또는 프로그래밍 코드 등 모든 종류의 규정에 사용되는 일반 확장명입니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.coffee

커피 산업 종사자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.college

학교, 대학 등 교육 기관에서 사용합니다. 채용 담당자, 상담자, 광고인, 학생, 교사 및 교육 기관 관련 업무를 하는 행정가들도 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

아랍어, 간체 및 번체 중국어, 키릴 자모, 그리스어, 히브리어, 일본이 및 태국어를 지원합니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.com

상업용 웹 사이트에서 사용됩니다. 인터넷에서 가장 인기가 좋은 확장명입니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

모든 정보가 숨겨집니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지

- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.community

모든 종류의 커뮤니티, 클럽, 조직 또는 특수 이해 집단에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.company

모든 종류의 회사에 사용되는 일반 확장명입니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.computer

컴퓨터 관련 정보에 사용되는 일반 확장명입니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.condos

콘도미니엄 관련 기업 및 관계자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.construction

건설업체 및 도급업체 등 건설 산업 종사자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.consulting

컨설턴트 등 컨설팅 산업 종사자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

아랍어, 중국어, 프랑스어, 키릴 문자, 데바나가리 문자, 독일어, 그리스어, 히브리어, 일본어, 한국어, 라틴어, 스페인어, 타밀어, 태국어가 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.contact

규모 또는 교파에 관계없이 모든 교회에서 신도와 소통하고 교회 관련 행사 및 활동에 대한 정보를 게시하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.contractors

건설 업종의 도급업체 등 도급업체가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 75일

.cool

최신 유행하는 브랜드로 만들고 싶은 단체 및 조직에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.coupons

온라인 쿠폰 및 쿠폰 코드를 제공하는 소매업체와 제조업체에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.credit

신용업계에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.creditcard

신용카드를 발급하는 회사 또는 은행에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.cruises

선박 여행 업종에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.dance

댄서, 댄스 강사, 댄스 학교에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 라틴어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

지원하지 않음.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지

- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.dating

데이트 웹 사이트에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 75일

.deals

온라인 특가 및 할인 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.degree

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.delivery

모든 종류의 상품 또는 서비스를 제공하는 회사에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.democrat

민주당 관련 정보를 제공하는 데 사용됩니다. 또한 선출직 공무원에 출마하는 사람과 선출된 공무원, 정당 지지자, 컨설턴트, 보좌관 등도 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 라틴어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

지원하지 않음.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.dental

치과 전문의 및 치과용품 공급업체에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.design

규모 또는 교파에 관계없이 모든 교회에서 신도와 소통하고 교회 관련 행사 및 활동에 대한 정보를 게시하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.diamonds

판매업체, 재판매업체, 구매업체 등 다이아몬드 산업 종사자 및 다이아몬드 애호가가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지

- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.diet

> **Important**
>
> 더 이상 Route 53를 사용하여 새 .diet 도메인을 등록하거나 .diet 도메인을 Route 53으로 이전할 수 없습니다. 이미 Route 53에 등록된 .diet 도메인은 계속 지원됩니다.

건강 및 피트니스 전문가가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

키릴 자모(주로 러시아어), 프랑스어, 독일어, 이탈리아어, 포르투갈어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

지원하지 않음. 더 이상 Route 53으로 .diet 도메인을 이전할 수 없습니다.

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지

- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.digital

디지털과 관련된 모든 산업에서 사용되나, 기술 기업에 특히 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.direct

일반 확장명으로 사용되나, 전자 상거래 웹 사이트를 통해 고객에게 직접 제품을 판매하는 경우에 특히 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.directory

언론 분야에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.discount

가격을 대폭 인하하는 할인 웹 사이트 및 기업에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.dog

애견인 및 반려견 서비스와 제품을 제공하는 업체에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.domains

도메인 이름에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.education

교육에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.email

프로모션 이메일에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 75일

.energy

일반 확장명으로 사용되나, 에너지 또는 에너지 보존 분야와 관련된 경우에 특히 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.engineering

엔지니어링 기업 및 전문가가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.enterprises

대기업 및 기업에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.equipment

장비, 장비 소매업체 또는 제조업체, 임대 매장에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.estate

주택 및 주택 분야에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.events

모든 종류의 이벤트에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.exchange

증권 거래, 상품 거래, 심지어 단순한 정보 교환 등 모든 종류의 교환에 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 75일

.expert

다양한 분야에 대해 전문 지식을 보유한 사람들이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.exposed

사진, 타블로이드 잡지, 폭로성 보도 등 다양한 주제에 사용되는 일반 확장명입니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.express

일반 확장명으로 사용되나, 상품 또는 서비스의 빠른 배송을 강조하고자 하는 경우에 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.fail

실수를 한 적이 있는 누구나 사용하나, 유머러스한 실수를 게시하는 데 특히 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.fan

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.farm

농부, 농공학자 등 농업 분야 종사자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.finance

금융 부문에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 75일

.financial

금융 부문에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.fish

일반 확장명으로 사용되나, 물고기 및 낚시와 관련된 웹 사이트에 특히 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.fitness

피트니스 및 피트니스 서비스를 홍보하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.flights

여행사, 항공사 등 여행 업종 종사자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.florist

꽃집에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.flowers

> **Important**
>
> 더 이상 Route 53를 사용하여 새 .flowers 도메인을 등록하거나 .flowers 도메인을 Route 53으로 이전할 수 없습니다. 이미 Route 53에 등록된 .flowers 도메인은 계속 지원됩니다.

온라인 꽃 판매 또는 화훼 재배 및 번식에 대한 정보 등 꽃과 관련된 모든 것에 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

키릴 자모(주로 러시아어), 프랑스어, 독일어, 이탈리아어, 포르투갈어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

지원하지 않음. 더 이상 Route 53으로 .flowers 도메인을 이전할 수 없습니다.

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.fm

.fm(미크로네시아 연방 공화국)을 참조하세요.

Return to index

.football

풋볼과 관련된 누구나 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.forsale

상품 및 서비스를 판매하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 라틴어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.foundation

비영리 단체, 자선 단체 및 각종 재단에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일

- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.fun

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.fund

펀딩과 관련된 모든 것의 일반 확장명으로 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.furniture

가구 제조업체 및 판매업체를 비롯하여 가구 산업과 관련된 누구나 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.futbol

축구에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 라틴어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

지원하지 않음.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.fyi

일반 확장명으로 사용되나, 모든 종류의 정보를 공유하는 데 특히 적합합니다. "FYI"는 "for your information"의 머리글자어입니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.gallery

미술관 소유자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.games

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 75일

.gift

선물을 판매하거나 선물 관련 서비스를 제공하는 기업 또는 조직에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

키릴 자모(주로 러시아어), 프랑스어, 독일어, 이탈리아어, 포르투갈어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.gifts

선물을 판매하거나 선물 관련 서비스를 제공하는 기업 또는 조직에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.gives

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.glass

유리 절단업체, 창호 시공업체 등 유리 산업 종사자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.global

국제적인 시장 또는 비전을 보유한 기업 또는 단체에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

아랍어, 벨로루시어, 보스니아어, 불가리아어, 중국어(간체), 중국어(번체), 덴마크어, 독일어, 힌디어, 헝가리어, 아이슬란드어, 한국어, 라트비아어, 리투아니아어, 마케도니아어, 몬테네그로어, 폴란드어, 러시아어, 세르비아어, 스페인어, 스웨덴어 및 우크라이나어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.gmbh

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지

- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.gold

일반 확장명으로 사용되나, 금 또는 금과 관련된 제품을 구매/판매하는 기업에 특히 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.golf

골프 전용 웹 사이트에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.graphics

그래픽 산업 종사자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.gratis

판촉 물품, 다운로드 또는 쿠폰 등 무료 제품을 제공하는 웹 사이트에서 사용됩니다. "Gratis"는 "무료"를 의미하는 스페인어입니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.green

보존, 생태, 환경 및 환경 친화적인 생활 방식을 다루는 웹 사이트에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.gripe

불만 및 비판을 공유하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.group

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지

- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.guide

일반 확장명으로 사용되나, 관광지, 여행 서비스 및 제품을 중점적으로 취급하는 웹 사이트에 특히 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 75일

.guitars

> **Important**
>
> 더 이상 Route 53를 사용하여 새 .guitars 도메인을 등록하거나 .guitars 도메인을 Route 53으로 이전할 수 없습니다. 이미 Route 53에 등록된 .guitars 도메인은 계속 지원됩니다.

기타 애호가가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

키릴 자모(주로 러시아어), 프랑스어, 독일어, 이탈리아어, 포르투갈어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

지원하지 않음. 더 이상 Route 53으로 .guitars 도메인을 이전할 수 없습니다.

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 75일

.guru

다양한 주제에 대해 자신의 지식을 공유하는 사람이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.haus

부동산 및 건설업계에서 사용됩니다. "Haus"는 "집"을 의미하는 독일어입니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 라틴어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.healthcare

의료 서비스 부문에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.help

일반 확장명으로 사용되나, 온라인 도움말 및 정보를 제공하는 웹 사이트에 특히 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

키릴 자모(주로 러시아어), 프랑스어, 독일어, 이탈리아어, 포르투갈어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.hiv

HIV와의 전쟁을 다루는 웹 사이트에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

키릴 자모(주로 러시아어), 프랑스어, 독일어, 이탈리아어, 포르투갈어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.hockey

하키 전용 웹 사이트에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지

- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.holdings

재정 고문, 주식 중개인, 투자업 종사자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.holiday

여행업 종사자 및 파티 플래너, 특별한 행사 관련 업체와 개인이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.host

웹 호스팅 플랫폼 및 서비스를 제공하는 회사가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

아랍어, 중국어(간체), 중국어(번체), 그리스어, 히브리어, 한국어, 태국어가 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.hosting

> **Important**
>
> 더 이상 Route 53를 사용하여 새 .hosting 도메인을 등록하거나 .hosting 도메인을 Route 53으로 이전할 수 없습니다. 이미 Route 53에 등록된 .hosting 도메인은 계속 지원됩니다.

호스팅 웹 사이트 또는 호스팅 산업에 종사하는 사람이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

지원하지 않음. 더 이상 Route 53으로 .hosting 도메인을 이전할 수 없습니다.

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.house

부동산 중개인 및 주택 매수인과 매도인이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.im

.im(맨 섬)을 참조하세요.

Return to index

.immo

부동산 분야에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.immobilien

부동산에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

지원하지 않음.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.industries

하나의 기업으로 간주되고자 하는 기업체 또는 영리 기업에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.info

정보 전파에 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 75일

.ink

타투 애호가 또는 인쇄 및 출판업 등 잉크 관련 산업에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

아랍어 및 라틴어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.institute

특히 연구 및 교육 기관 등 모든 기관이나 단체에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.insure

보험 회사 및 보험 중개인이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.international

해외 지사가 있는 기업, 해외 여행을 하는 개인, 또는 국제적 영향력이 있는 자선 단체에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.investments

일반 확장명으로 사용되나, 투자 기회를 홍보하는 데 특히 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.io

.io(영국령 인도양 식민지)을 참조하세요.

Return to index

.irish

아일랜드 문화 및 조직을 홍보하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

아랍어, 중국어(간체), 중국어(번체), 프랑스어, 독일어, 그리스어, 히브리어, 일본어, 한국어, 스페인어, 타밀어, 태국어가 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.jewelry

보석 판매업체 및 구매업체에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.juegos

> **Important**
>
> 더 이상 Route 53를 사용하여 새 .juegos 도메인을 등록하거나 .juegos 도메인을 Route 53으로 이전할 수 없습니다. 이미 Route 53에 등록된 .juegos 도메인은 계속 지원됩니다.

모든 종류의 게임 웹 사이트에서 사용됩니다. "Juegos"는 "게임"을 의미하는 스페인어입니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

키릴 자모(주로 러시아어), 프랑스어, 독일어, 이탈리아어, 포르투갈어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

지원하지 않음. 더 이상 Route 53으로 .juegos 도메인을 이전할 수 없습니다.

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.kaufen

전자 상거래에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 라틴어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

지원하지 않음.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 75일

.kim

성이나 이름이 Kim인 사람들이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.kitchen

주방 관련 소매업체, 요리사, 음식 블로거 및 식품 산업 관계자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.kiwi

뉴질랜드 키위 문화를 지지하는 회사와 개인이 사용합니다. 2010년과 2011년에 지진 피해를 입은 크라이스트처치 재건 사업을 위한 기부 플랫폼으로도 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

마오리어에 지원됩니다

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.land

농부, 부동산 중개인, 토지 개발업체 및 부동산에 관심이 있는 사람이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.law

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.lease

부동산업자, 임대주 및 임차인이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.legal

법률 직종에 종사하는 사람이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지

- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.lgbt

레즈비언, 게이, 양성애자 및 트랜스젠더 커뮤니티에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.life

일반 확장자로 사용되며, 다양한 기업, 단체 및 개인이 사용할 수 있습니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.lighting

사진가, 디자이너, 건축가, 엔지니어 및 조명에 관심이 있는 사람이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.limited

일반 확장자로 사용되며, 다양한 기업, 단체 및 개인이 사용할 수 있습니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.limo

운전 기사, 리무진 업체, 렌터카 업체에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.link

온라인 바로 가기 링크를 만드는 방법에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

Uniregistry는 .LINK 도메인에 대한 레지스트리입니다. Uniregistry 정책으로 인해 레지스트리 수준 WHOIS는 “REDACTED FOR PRIVACY(개인 정보 보호를 위해 편집됨)”를 표시합니다. 개인 정보 보호 기능을 제거하면 등록 기관 수준 Amazon Registrar WHOIS에 표시되는 정보에만 영향을 미칩니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

키릴 자모(주로 러시아어), 프랑스어, 독일어, 이탈리아어, 포르투갈어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.live

일반 확장자로 사용되며, 다양한 기업, 단체 및 개인이 사용할 수 있습니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 라틴어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.llc

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 75일

.loan

채권자, 채무자 및 신용 거래업 종사자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

덴마크어 , 독일어 , 노르웨이어 및 스웨덴어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.loans

채권자, 채무자 및 신용 거래업 종사자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.lol

유머 및 코미디 웹 사이트에서 사용됩니다. "LOL"은 "laugh out loud"의 머리글자어입니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

키릴 자모, 프랑스어, 독일어, 이탈리아어, 포르투갈어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.ltd

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.maison

부동산 분야에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.management

기업 환경 및 회사 경영에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.marketing

마케팅 분야에서 다양한 목적으로 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 75일

.mba

경영학 석사 학위(MBA)에 대한 정보를 제공하는 웹 사이트에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.media

미디어 및 엔터테인먼트 부문에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.memorial

사건 및 인물을 기념하는 조직에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.mobi

휴대폰으로 웹 사이트에 액세스할 수 있게 만들려는 기업과 개인이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.moda

패션에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 라틴어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

지원하지 않음.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.money

통화 및 통화 관련 활동을 중점적으로 다루는 웹 사이트에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지

- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.mortgage

모기지 산업에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 라틴어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.movie

영화 및 영화 제작에 대한 정보를 제공하는 웹 사이트에서 사용됩니다. 전문가 및 애호가 모두 사용할 수 있습니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.name

맞춤형 웹 프레즌스를 생성하려는 경우에 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

.name TLD의 등록처인 Verisign을 사용하면 두 번째 수준 도메인(name.name) 및 세 번째 수준 도메인(FirstName.LastName.name)을 모두 등록할 수 있습니다. Route 53는 도메인 등록 및 기존 도메인의 Route 53으로 이전 모두에 대해 2단계 도메인만 지원합니다.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.net

모든 종류의 웹 사이트에 사용됩니다. 확장명 .net은 네트워크(network)의 약어입니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

모든 정보가 숨겨집니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.network

네트워크 산업에 종사하는 사람 또는 네트워킹을 통해 연결을 구축하고자 하는 사람이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.news

저널리즘 및 커뮤니케이션과 관련된 시사 또는 정보 등 뉴스거리가 되는 정보를 퍼뜨리는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 라틴어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.ninja

닌자의 능력을 가지고 싶은 기업과 개인이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 라틴어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.onl

확장명 .onl은 "온라인(online)"의 약어이며, 스페인어로 비영리 단체를 뜻하는 줄임말이기도 합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

아랍어, 벨로루시어, 보스니아어, 불가리아어, 중국어(간체 및 번체), 덴마크어, 독일어, 힌디어, 헝가리어, 아이슬란드어, 한국어, 리투아니아어, 라트비아어, 마케도니아어, 폴란드어, 러시아어, 세르비아어, 스페인어가 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.online

확장명 .onl은 "온라인(online)"의 약어이며, 스페인어로 비영리 단체를 뜻하는 줄임말이기도 합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지

- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.org

모든 종류의 조직에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

모든 정보가 숨겨집니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.partners

법률 사무소, 투자자 및 다양한 회사에서 사용합니다. 또한 관계를 구축하는 소셜 웹 사이트에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.parts

일반 확장명으로 사용되나, 부품 제조업체, 판매업체 및 구매업체에 특히 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.photo

사진가 및 사진에 관심이 있는 사람이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

키릴 자모(주로 러시아어), 프랑스어, 독일어, 이탈리아어, 포르투갈어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.photography

사진가 및 사진에 관심이 있는 사람이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.photos

사진가 및 사진에 관심이 있는 사람이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.pics

사진가 및 사진에 관심이 있는 사람이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

키릴 자모(주로 러시아어), 프랑스어, 독일어, 이탈리아어, 포르투갈어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지

- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.pictures

사진, 예술 및 미디어에 관심이 있는 누구나 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.pink

분홍색을 좋아하는 경우 또는 기업 이미지나 브랜드에서 분홍색을 떠올리게 하려는 경우에 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.pizza

피자 레스토랑 및 피자 애호가가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.place

일반 확장명으로 사용되나, 가정 및 여행 부문에 특히 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.plumbing

배관 산업 종사자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.plus

일반 확장명으로 사용되나, 큰 사이즈 의류, 부가 소프트웨어 또는 "추가" 기능 또는 치수를 제공하는 제품에 특히 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.poker

포커 플레이어 및 게임 웹 사이트에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.porn

성인용 웹 사이트에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 75일

.press

성인용 웹 사이트에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.pro

라이센스와 자격 증명을 갖춘 전문가 및 전문 조직이 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.productions

광고, 라디오 광고, 뮤직 비디오를 제작하는 스튜디오 및 프로덕션에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.properties

부동산 또는 지적 재산 등 모든 종류의 재산에 대한 정보를 제공하는 데 사용됩니다. 또한 주택, 건물 또는 토지를 매도 또는 임대하려는 경우에 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.property

부동산 또는 지적 재산 등 모든 종류의 재산에 대한 정보를 제공하는 데 사용됩니다. 또한 주택, 건물 또는 토지를 매도 또는 임대하려는 경우에 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

키릴 자모(주로 러시아어), 프랑스어, 독일어, 이탈리아어, 포르투갈어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

지원하지 않음. 더 이상 Route 53으로 .property 도메인을 이전할 수 없습니다.

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.pub

출판업, 광고업 또는 양조업체 종사자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 라틴어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.qpon

쿠폰 및 프로모션 코드에 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.recipes

레시피를 공유하려는 경우에 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지

- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.red

빨간색을 좋아하는 경우 또는 기업 이미지나 브랜드에서 빨간색을 떠올리게 하려는 경우에 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.reise

여행과 관련된 웹 사이트에서 사용됩니다. "Reise"는 "오르다", "일어나다" 또는 "여행을 떠나다"를 의미하는 독일어입니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.reisen

여행과 관련된 웹 사이트에서 사용됩니다. ‘Reisen’은 ‘여행하다’라는 뜻의 독일어입니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.rentals

모든 종류의 임대에 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.repair

수리 서비스 업체 또는 모든 종류의 물품 수리 방법을 타인에게 알려 주려는 경우에 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.report

일반 확장명으로 사용되나, 업무 보고서, 지역 사회 간행물, 독후감 또는 뉴스 보고에 대한 정보를 제공하는 데 특히 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.republican

공화당 관련 정보를 제공하는 데 사용됩니다. 또한 선출직 공무원에 출마하는 사람과 선출된 공무원, 정당 지지자, 컨설턴트, 보좌관 등도 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 라틴어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.restaurant

레스토랑 산업에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일

- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.reviews

자신의 의견을 표명하고 타인의 댓글을 읽고자 하는 경우에 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 라틴어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

지원하지 않음.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.rip

죽음 및 기념비를 다루는 웹 사이트에서 사용됩니다. "RIP"은 "rest in peace"의 머리글자어입니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 라틴어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.rocks

일반 확장명으로 사용되나, 음악가, 지질학자, 보석 전문가, 등반가 등 "rock(록 또는 암석)" 전문가에게 특히 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 라틴어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.run

일반 확장명으로 사용되나, 피트니스 및 스포츠 산업에 특히 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.sale

전자 상거래 웹 사이트에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 라틴어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.sarl

일반적으로 프랑스에 위치한 유한 책임 회사에서 사용합니다. "SARL"는 Société à Responsabilité Limité의 머리글자어입니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.school

교육, 교육 기관 및 학교 관련 활동에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지

- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.schule

독일어 관련 교육, 교육 기관 및 학교 관련 활동에 대한 정보를 제공하는 데 사용됩니다. "Schule"은 "학교"를 의미하는 독일어입니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.services

모든 종류의 서비스를 중점적으로 다루는 웹 사이트에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.sex

성인용 콘텐츠에 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.sexy

성적인 콘텐츠에 사용됩니다. 또한 가장 인기가 높고 신나는 브랜드, 제품, 정보 및 웹 사이트를 묘사하는 데도 사용됩니다.

Return to index

Important

더 이상 Route 53를 사용하여 새 .sexy 도메인을 등록하거나 .sexy 도메인을 Route 53으로 이전할 수 없습니다. 이미 Route 53에 등록된 .sexy 도메인은 계속 지원됩니다.

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

키릴 자모(주로 러시아어), 프랑스어, 독일어, 이탈리아어, 포르투갈어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

지원하지 않음. 더 이상 Route 53으로 .sexy 도메인을 이전할 수 없습니다.

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.shiksha

교육 기관에서 사용됩니다. "Shiksha"는 학교를 가리키는 인도어입니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.shoes

신발 소매업체, 디자이너, 제조업체 또는 패션 블로거가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.shopping

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.show

일반 확장명으로 사용되나, 엔터테인먼트 산업에 특히 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지

- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.singles

데이트 주선 서비스 업체, 리조트 및 인간 관계를 맺고자 하는 고객에게 서비스를 제공하는 기타 기업에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.site

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.ski

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.soccer

축구 전용 웹 사이트에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.social

소셜 미디어, 포럼 및 온라인 대화에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 라틴어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.solar

태양광 시스템 또는 태양열 에너지에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지

- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.solutions

컨설턴트, DIY 서비스 업체 및 모든 종류의 조언자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.software

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.space

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.store

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.stream

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.studio

일반 확장명으로 사용되나, 부동산, 예술 또는 엔터테인먼트 산업과 관련된 경우에 특히 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 라틴어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.style

일반 확장명으로 사용되나, 특히 패션, 디자인, 건축 및 예술계의 트렌드 등 최신 트렌드를 다루는 웹 사이트에 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지

- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.sucks

일반 확장명으로 사용되나, 부정적 경험을 공유하거나 다른 사람에게 사기 또는 제품 결함을 경고하려는 경우에 특히 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.supplies

온라인으로 상품을 판매하는 기업에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.supply

온라인으로 상품을 판매하는 기업에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.support

고객, 제품, 시스템 지원 또는 정서적, 재정적, 정신적 지지를 비롯하여 모든 종류의 지원을 제공하는 기업, 단체 또는 자선 단체에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.surgery

수술, 의학 및 의료에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.systems

주로 기술 업종에서 기술 서비스를 제공하는 경우에 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.tattoo

타투 애호가 및 타투 업종에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

키릴 자모(주로 러시아어), 프랑스어, 독일어, 이탈리아어, 포르투갈어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.tax

세금, 세금 준비 및 세법에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 75일

.taxi

택시, 운전 기사 및 셔틀 서비스 업체에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.team

하나의 팀으로 간주되고자 하는 기업체 또는 조직에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.tech

기술 애호가 및 일반 회사, 서비스 업체, 제조업체의 기술 담당자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.technology

기술 애호가 및 일반 회사, 서비스 업체, 제조업체의 기술 담당자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.tennis

테니스와 관련된 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.theater

연극, 희곡 및 뮤지컬을 다루는 웹 사이트에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.tienda

스페인어권 소비자에게 접근하려는 소매업체에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 75일

.tips

거의 모든 주제에 대한 지식과 조언을 나누고자 하는 경우에 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.tires

타이어 제조업체, 유통업체 또는 구매업체에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.today

최신 이벤트, 뉴스, 날씨, 엔터테인먼트 등에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.tools

모든 종류의 도구에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.tours

일반 확장명으로 사용되나, 여행업체에 특히 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.town

도시의 지역, 문화 및 지역 사회를 홍보하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.toys

장난감 산업에서 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지

- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.trade

일반 확장명으로 사용되나, 전자 상거래 웹 사이트 또는 무역 서비스에 특히 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

덴마크어 , 독일어 , 노르웨이어 및 스웨덴어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.training

강사, 코치 및 교육자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.tv

텔레비전 및 언론에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

없음.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.university

대학 및 기타 교육 기관에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.uno

히스패닉, 포르투갈인, 이탈리아인 커뮤니티에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.vacations

여행 및 관광 업종에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.vegas

라스베이거스 및 라스베이거스 생활 방식을 홍보하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.ventures

기업가, 스타트업, 벤처 투자자, 투자 은행, 금융업체 등에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지

- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.vg

.vg(영국령 버진 제도)을 참조하세요.

Return to index

.viajes

여행사, 투어 운영사, 여행 블로그, 관광업체, 임대 서비스 업체, 여행 블로거 및 여행 소매업체에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지

- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.video

미디어 및 비디오 산업에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 라틴어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.villas

부동산 중개인 및 빌라를 매도 또는 임대하려는 부동산 소유자가 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.vision

일반 확장명으로 사용되나, 검안사 및 안과 의사 등 시력 전문가에게 특히 적합합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.vote

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.voyage

여행사, 투어 운영사, 여행 블로그, 관광업체, 임대 서비스 업체, 여행 블로거 및 여행 소매업체에서 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.watch

스트리밍 웹 사이트, 웹 TV, 동영상 또는 시청에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.website

웹 사이트 개발, 홍보, 개선 및 경험에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

아랍어, 중국어(간체), 중국어(번체), 그리스어, 히브리어, 일본어, 한국어, 태국어가 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지

- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.wedding

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

없음.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

중국어, 프랑스어, 독일어, 스페인어를 지원합니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 75일

.wiki

온라인 문서에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

아랍어 및 라틴어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.wine

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호

지원

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.work

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.works

일자리, 구인 및 채용 서비스에 대한 정보를 얻기 위해 기업, 단체 및 개인이 사용합니다. .com, .net 또는 .org 확장명 대신 이 확장명을 사용할 수 있습니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.world

글로벌 주제에 대한 정보를 제공하고자 하는 누구나 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.wtf

대중적이지만 비속한 머리글자어 "WTF"로 식별되고자 하는 누구나 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.xyz

모든 목적을 위한 일반 확장명으로 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

.xyz 도메인의 등록부 Generation XYZ에서는 일부 도메인 이름을 프리미엄 도메인 이름으로 간주합니다. 프리미엄 .xyz 도메인을 Route 53로 등록하거나 이전할 수 없습니다. 자세한 내용은 Generation XYZ 웹 사이트를 참조하십시오.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.zone

시간대, 기후대, 스포츠 경기의 구역 등 모든 종류의 영역에 대한 정보를 제공하는 데 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

프랑스어 및 스페인어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일

- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

지리적 최상위 도메인

다음 도메인 확장명은 지역을 기준으로 나눈 것이며, ccTLD(국가 코드 최상위 도메인)라고 부르는 국가별 공식 확장명이 포함되어 있습니다. 예를 들어 벨기에는 .be, 인도는 .in, 멕시코는 .mx입니다. ccTLD 등록 규칙은 나라마다 다릅니다. 세상 사람 누구나 등록할 수 있도록 제한을 두지 않는 나라도 있고, 거주자 등으로 제한하는 나라도 있습니다. 각 ccTLD의 목록에는 제한 사항이 표시됩니다.

> **Important**
>
> .cc 및 .tv를 제외한 모든 ccTLD를 Route 53으로 전송하는 경우 소유자 연락처에 대한 업데이트는 사용되지 않고 레지스트리의 소유자 연락처 데이터가 사용됩니다. 이전이 완료된 후 소유자 연락처 정보를 업데이트할 수 있습니다. 자세한 내용은 도메인 연락처 정보 및 소유권 업데이트 단원을 참조하십시오.

Return to index

아프리카

.ac(어센션 섬), .co.za(남아프리카), .sh(세인트 헬레나)

북남미

.ca(캐나다), .cl(칠레), .co(콜롬비아), .com.ar(아르헨티나), .com.br(브라질), .com.mx(멕시코), .mx(멕시코), .us(미국), .vc(세인트 빈센트 그레나딘), .vg(영국령 버진 제도)

아시아/오세아니아

.au(오스트레일리아), .cc(코코스(킬링) 제도), .co.nz(뉴질랜드), .com.au(호주), .com.sg(싱가포르), .fm(미크로네시아 연방 공화국), .in(인도), .jp(일본), .io(영국령 인도양 식민지), .net.au(호주), .net.nz (뉴질랜드), .org.nz(뉴질랜드), .pw(팔라우), .qa(카타르), .ru(러시아 연방), .sg(싱가포르)

유럽

.be(벨기에), .berlin(독일 베를린 시), .ch(스위스), .co.uk(영국), .cz(체코 공화국), .de(독일), .es(스페인) , .eu(유럽 연합), .fi(핀란드), .fr(프랑스), .gg(건지), .im(맨 섬), .it(이탈리아), .me(몬테네그로), .me.uk(영국), .nl(네덜란드), .org.uk(영국), .ruhr(독일 서부 루르 지방), .se(스웨덴), .uk(영국), .wien(오스트리아 비엔나 시)

아프리카

Amazon Route 53에 도메인을 등록하는 데 다음 최상위 도메인(TLD)을 아프리카에서 사용할 수 있습니다.

, ,

Return to index

.ac(어센션 섬)

Return to index

학계에서 인기 있는 일반 TLD로도 사용됩니다.

등록 및 갱신을 위한 임대 기간

1년.

제한 사항

제한 없이 일반에 공개되어 있습니다.

개인 정보 보호

등록처에 따라 결정됨

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지

- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 80일

.co.za(남아프리카)

Return to index

등록 및 갱신을 위한 임대 기간

1년.

제한 사항

.za 확장명에는 2단계 도메인만 사용할 수 있습니다. Route 53는 2단계 도메인인 .co.za를 지원합니다.

일반에 공개되어 있지만 다음과 같은 몇 가지 제한이 있습니다.

- 확인 가능한 법적 주체(개인 및 법인)가 등록할 수 있습니다.
- 도메인 이름은 등록 과정에서 구역 확인을 거쳐야 합니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원하지 않음. 무단 이전을 방지하려면 등록자 이메일 주소 및 소유권 변경을 허용할 수 있는 Route 53 API(예: UpdateDomainContact)에 대한 액세스를 제한합니다. 자세한 내용은 서비스 승인 참조에서 Route 53 Domains에 사용되는 작업, 리소스 및 조건 키 및 도메인 레코드 소유자에 대한 사용 권한 예제 단원을 참조하세요.

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

아니요

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신: 만료 날짜 1일 전까지
- Route 53를 사용한 늦은 갱신: 불가능
- Route 53에서 도메인 삭제: 만료 1일 전
- 레지스트리 복원: 만료 후 1일 ~ 9일 사이
- 레지스트리에서 도메인 삭제: 만료 후 9일

.sh(세인트 헬레나)

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

제한 없이 일반에 공개되어 있습니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지

- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 80일

북남미

Amazon Route 53에 도메인을 등록하는 데 다음 최상위 도메인(TLD)을 북남미에서 사용할 수 있습니다.

, , , , , , , , ,

Return to index

.ca(캐나다)

Return to index

도메인 이름의 (à) 또는 (a) 억양 표시가 없는 변형은 자동으로 등록자에게 예약되며 관리 번들의 일부가 됩니다. 번들에서 도메인을 활성화하려면 등록자가 도메인에 대한 등록 요청을 해야 합니다. 번들 내의 모든 도메인은 동일한 등록자 및 동일한 등록 기관에 의해 등록되어야 합니다. 또한 등록자는 이전을 완료하기 위해 번들의 모든 도메인에 대한 이전 요청을 제출해야 합니다.

TLD 등록부의 확인 이메일

.ca 도메인을 등록하면 등록 계약의 수락 절차를 안내하는 링크를 이메일로 보내 드립니다. 7일 이내에 이 절차를 완료하지 않으면 도메인이 등록되지 않습니다.

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

일반에 공개되어 있지만 다음과 같은 몇 가지 제한이 있습니다.

- CPRR(캐나다 주민 등록을 위한 거주 요건)에 설명된 것과 같이 캐나다와 관계가 있는 개인 또는 단체가 등록할 수 있습니다.
- 등록 문의: 도메인 소유자의 정확한 정식 법적 이름을 제시해야 합니다.
- 관리 및 기술 문의: 연락처 유형으로 [Person]을 지정하고 캐나다에 거주하는 개인의 연락처 정보를 제공해야 합니다.

- 등록 과정에서 다음과 같은 법적 유형 중 하나를 선택해야 합니다.
  - ABO: 캐나다 원주민(개인 또는 단체)
  - ASS: 캐나다의 비법인 단체
  - CCO: 캐나다 기업, 캐나다 지방 또는 영토
  - CCT: 캐나다 시민
  - EDU: 캐나다 교육 기관
  - GOV: 캐나다 정부 또는 정부 기관
  - HOP: 캐나다 병원
  - INB: 캐나다의 인디언 보호법에서 인정한 인디언 보호 구역
  - LAM: 캐나다 도서관, 아카이브 또는 박물관
  - LGR: 캐나다 시민 또는 영주권자의 법정 대리인
  - MAJ: 영연방 여왕 폐하/국왕 폐하
  - OMK: 캐나다에 등록된 공식 마크
  - PLT: 캐나다 정당
  - PRT: 캐나다에 등록된 제휴 관계
  - RES: 캐나다 영주권자
  - TDM: 캐나다에 등록된 상표(비-캐나다 소유자 유형)
  - TRD: 캐나다 노동조합
  - TRS: 캐나다에 설립된 신탁

개인 정보 보호

- 사람 - CIRA는 개인 정보 보호를 자동으로 적용하므로 모든 연락처에서 연락처 이름, 주소, 전화 번호, 팩스 번호, 이메일 주소는 숨겨집니다. 개인 정보 보호 옵션은 등록 기관 Whois에서만 적용됩니다.
- 회사, 협회 또는 공공 단체 - 등록 수준에서 지원되지 않습니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 경우에 따라 달라짐 AWS Support에 문의하세요.

도메인 등록 삭제

.ca 도메인을 등록했다고 해서 등록된 도메인을 삭제할 수 있는 것은 아닙니다. 그 대신, 자동 갱신을 해제하고 도메인이 만료되기를 기다려야 합니다. 자세한 내용은 도메인 이름 등록 삭제 단원을 참조하십시오.

.cl(칠레)

> **Important**
>
> 더 이상 Route 53를 사용하여 새 .cl 도메인을 등록하거나 .cl 도메인을 Route 53으로 이전할 수 없습니다. 이미 Route 53에 등록된 .cl 도메인은 계속 지원됩니다.

Return to index

갱신 기간

2년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원하지 않음. RetrieveDomainAuthCode API 작업에 대한 액세스를 제한하여 무단 이전을 방지하는 것이 좋습니다. (이 Route 53 API에 대한 액세스를 제한할 때 Route 53 콘솔, AWS SDKs 및 기

타 프로그래밍 방법을 사용하여 권한 부여 코드를 생성할 수 있는 사용자도 제한합니다.) 자세한 내용은 Amazon Route 53의 Identity and Access Management 단원을 참조하십시오.

이전하는 데 필요한 권한 부여 코드

지원하지 않음. 더 이상 Route 53으로 .cl 도메인을 이전할 수 없습니다.

DNSSEC

지원하지 않음.

도메인 갱신 및 복원 기한

- 갱신 가능: AWS Support에 문의하세요.
- Route 53를 사용한 늦은 갱신: AWS Support에 문의하세요.
- Route 53에서 도메인 삭제: AWS Support에 문의하세요.
- 등록처 복원 가능: AWS Support에 문의하세요.
- 등록처에서 도메인 삭제: AWS Support에 문의하세요.

.co(콜롬비아)

Return to index

등록 및 갱신을 위한 임대 기간

1~5년.

제한 사항

.co 도메인의 등록 기관 Go.co에서는 일부 도메인 이름을 프리미엄 도메인 이름으로 간주합니다. 프리미엄 .co 도메인을 Route 53로 등록하거나 이전할 수 없습니다. 자세한 내용은 Go.co 웹 사이트를 참조하십시오.

개인 정보 보호(적용 대상: 개인)

모든 정보가 숨겨집니다.

연락처 유형이 사람이 아닌 경우 WHOIS는 회사 이름과 국가를 표시합니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 29일까지
- Route 53에서 도메인 삭제: 만료 후 30일
- 레지스트리 복원: 만료 후 30일 ~ 45일 사이
- 레지스트리에서 도메인 삭제: 만료 후 50일

.com.ar(아르헨티나)

> **Important**
>
> 더 이상 Route 53를 사용하여 새 .com.ar 도메인을 등록하거나 .com.ar 도메인을 Route 53으로 이전할 수 없습니다. 이미 Route 53에 등록된 .com.ar 도메인은 계속 지원됩니다.

Return to index

갱신 기간

1년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원하지 않음. 무단 이전을 방지하려면 등록자 이메일 주소 및 소유권 변경을 허용할 수 있는 Route 53 API(예: UpdateDomainContact)에 대한 액세스를 제한합니다. 자세한 내용은 서비스 승인 참조에서 Route 53 Domains에 사용되는 작업, 리소스 및 조건 키 및 도메인 레코드 소유자에 대한 사용 권한 예제 단원을 참조하세요.

이전하는 데 필요한 권한 부여 코드

지원하지 않음. 더 이상 Route 53으로 .com.ar 도메인을 이전할 수 없습니다.

DNSSEC

지원하지 않음.

도메인 갱신 및 복원 기한

- 갱신 가능: AWS Support에 문의하세요.
- Route 53를 사용한 늦은 갱신: AWS Support에 문의하세요.
- Route 53에서 도메인 삭제: AWS Support에 문의하세요.
- 등록처 복원 가능: AWS Support에 문의하세요.
- 등록처에서 도메인 삭제: AWS Support에 문의하세요.

.com.br(브라질)

> **Important**
>
> 더 이상 Route 53를 사용하여 새 .com.br 도메인을 등록하거나 .com.br 도메인을 Route 53으로 이전할 수 없습니다. 이미 Route 53에 등록된 .com.br 도메인은 계속 지원됩니다.

Return to index

갱신 기간

1년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

이전하는 데 필요한 권한 부여 코드

지원하지 않음. 더 이상 Route 53으로 .com.br 도메인을 이전할 수 없습니다.

DNSSEC

지원하지 않음.

도메인 갱신 및 복원 기한

- 갱신: 만료 날짜 30일 전 ~ 만료 날짜 사이
- Route 53를 사용한 늦은 갱신: 만료 후 119일까지
- Route 53에서 도메인 삭제: 만료 후 119일
- 레지스트리 복원: 불가능
- 레지스트리에서 도메인 삭제: 만료 후 119일

.com.mx(멕시코)

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

제한 없이 일반에 공개되어 있습니다.

개인 정보 보호

등록처에 따라 결정됨

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지

- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.mx(멕시코)

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

제한 없이 일반에 공개되어 있습니다.

개인 정보 보호

등록처에 따라 결정됨

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 75일

.us(미국)

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

.us 도메인을 등록하는 경우 Federal Communications Commission v. Pacifica Foundation No. 77-528의 “법원 판결에 대한 부록”에 나오는 7개 단어 중 어느 단어라도 포함하는 도메인 이름은 허용하지 않습니다.

일반에 공개되어 있지만 한 가지 제한이 있습니다.

- .us 확장명은 미합중국에 위치하는 웹 사이트 또는 활동에 사용됩니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 29일까지
- Route 53에서 도메인 삭제: 만료 후 30일

- 레지스트리 복원: 만료 후 30일 ~ 60일 사이
- 레지스트리에서 도메인 삭제: 만료 후 65일

.vc(세인트 빈센트 그레나딘)

벤처 캐피털 금융, 대학 등의 관계자들이 종종 일반 TLD로도 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

제한 없이 일반에 공개되어 있습니다.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

모든 정보가 숨겨집니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이

- 레지스트리에서 도메인 삭제: 만료 후 80일

.vg(영국령 버진 제도)

비디오 게임 관련 조직들이 종종 일반 TLD로도 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

제한 없이 일반에 공개되어 있습니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

지원하지 않음.

도메인 갱신 및 복원 기한

- 갱신: 만료 날짜 후 44일까지 가능
- Route 53를 사용한 늦은 갱신 가능: 예
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 74일 사이
- 다시 공개 도메인으로 사용 가능: 만료 후 80일

아시아/오세아니아

Amazon Route 53에 도메인을 등록하는 데 다음 최상위 도메인(TLD)을 아시아 및 오세아니아에서 사용할 수 있습니다.

, , , , , , , , , , , , , , ,

Return to index

.au(오스트레일리아)

Return to index

TLD 등록부의 확인 이메일

등록 대행 협력사인 Gandi에서는 DomainDirectors를 통해 .au 도메인을 재판매합니다. Route 53으로 도메인 이름을 이전하는 경우, DomainDirectors에서 연락처 정보를 확인하는 이메일이나 이전 요청을 허가하는 이메일을 도메인 등록자의 연락처로 보내 드립니다.

등록 및 갱신을 위한 임대 기간

1년.

제한 사항

일반에 공개되어 있지만 다음과 같은 몇 가지 제한이 있습니다.

- .au 도메인은 호주에 등록되어 있는 법인, 무역업체, 제휴업체 또는 개인 사업자, 호주에서 사업 허가를 받은 해외 기업, 호주 등록 상표를 출원한 신청자 또는 상표 소유자가 사용할 수 있습니다. 개인은 .au 도메인을 등록할 수 없습니다. 등록자 연락처는 회사여야 합니다.
- 도메인 이름은 해당하는 호주 당국에 등록된 등록자의 이름 또는 상표(또는 그 약어나 두문자어)와 일치해야 합니다.
- 도메인 이름은 등록자의 활동을 의미해야 합니다. 예를 들어, 등록자가 판매하는 제품이나 제공하는 서비스를 나타낼 수 있습니다.
- 등록 과정에서 다음을 제시해야 합니다.
  - 등록 유형: ABN(호주 기업 번호), ACN(호주 회사 번호) 또는 도메인 이름이 상표와 일치하는 경우 TM(상표)
  - ID 번호: Medicare 카드 번호, TFN(납세자 번호), 주 운전면허증 번호 또는 ABN(호주 기업 번호)
  - 해당 주 또는 지방

- 이름, ABN 또는 상표(TM) 번호를 비롯한 연락처 정보가 잘못되거나 일치하지 않으면 등록, 거래 및 갱신이 실패합니다. 기존 도메인에 대한 정보를 수정하려면 소유권을 변경해야 할 수 있습니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원하지 않음. RetrieveDomainAuthCode API 작업에 대한 액세스를 제한하여 무단 이전을 방지하는 것이 좋습니다. (이 Route 53 API에 대한 액세스를 제한할 때 Route 53 콘솔, AWS SDKs 및 기타 프로그래밍 방법을 사용하여 권한 부여 코드를 생성할 수 있는 사용자도 제한합니다.) 자세한 내용은 Amazon Route 53의 Identity and Access Management 단원을 참조하십시오.

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예. Route 53 콘솔 외에도 .au 레지스트리에서 전송 코드를 가져올 수도 있습니다.

DNSSEC

도메인 등록에 대해 지원됩니다. 키를 설정할 때 DNS 보안 알고리즘 2(DH)를 선택해야 합니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신: 만료 날짜 60일 전 ~ 만료 날짜 사이
- Route 53를 사용한 늦은 갱신: 만료 후 29일까지
- Route 53에서 도메인 삭제: 만료 후 29일
- 레지스트리 복원: 불가능
- 레지스트리에서 도메인 삭제: 만료 후 30일

도메인 등록 삭제

.au 도메인을 등록했다고 해서 등록된 도메인을 삭제할 수 있는 것은 아닙니다. 그 대신, 자동 갱신을 해제하고 도메인이 만료되기를 기다려야 합니다. 자세한 내용은 도메인 이름 등록 삭제 단원을 참조하십시오.

소유권 변경

Route 53 콘솔을 사용하여 소유자를 변경합니다. 도메인 연락처 정보 업데이트을 참조하세요. 그런 후 다음 프로세스를 완료하여 소유권 변경을 완료합니다.

1. 이전 등록자와 새 등록자는 모두 transfers@1api.net에서 이메일 주소로 받은 링크를 클릭해야 합니다. 14일 이내에 완료하지 않는 경우, 프로세스를 다시 시작해야 합니다.

2. 응답이 확인되면 레지스트리의 소유자 변경이 추가 확인없이 짧은 시간 내에 처리됩니다.

.cc(코코스(킬링) 제도)

Return to index

컨설팅 회사, 클라우드 컴퓨팅 회사 또는 자전거 클럽처럼 이름에 "cc"가 있는 조직들이 종종 일반 TLD로도 사용합니다. 이 확장명은 ".com"의 인기 있는 대안입니다.

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

제한 없이 일반에 공개되어 있습니다.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

- 숨김 - 주소, 전화번호, 팩스 번호 및 이메일 주소
- 숨기지 않음 - 연락처 이름 및 조직 이름

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지

- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 30일 ~ 60일 사이
- 레지스트리에서 도메인 삭제: 만료 후 65일

.co.nz(뉴질랜드)

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

.co.nz, .net.nz, .org.nz와 같은 두 번째 수준 도메인을 Route 53에 등록할 수 있습니다. Route 53를 통해 .nz(첫 번째 수준) 도메인을 등록하거나 .nz 도메인을 Route 53으로 이전할 수 없습니다.

일반에 공개되어 있지만 다음과 같은 몇 가지 제한이 있습니다.

- 개인의 경우 18세 이상이어야 합니다.
- 단체의 경우 등록된 단체여야 합니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원하지 않음. RetrieveDomainAuthCode API 작업에 대한 액세스를 제한하여 무단 이전을 방지하는 것이 좋습니다. (이 Route 53 API에 대한 액세스를 제한할 때 Route 53 콘솔, AWS SDKs 및 기타 프로그래밍 방법을 사용하여 권한 부여 코드를 생성할 수 있는 사용자도 제한합니다.) 자세한 내용은 Amazon Route 53의 Identity and Access Management 단원을 참조하십시오.

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 44일
- 레지스트리 복원: 만료 후 44일~134일
- 레지스트리에서 도메인 삭제: 만료 후 134일

.com.au(호주)

Return to index

TLD 등록부의 확인 이메일

등록 대행 협력사인 Gandi에서는 DomainDirectors를 통해 .com.au 도메인을 재판매합니다. Route 53으로 도메인 이름을 이전하는 경우, DomainDirectors에서 연락처 정보를 확인하는 이메일이나 이전 요청을 허가하는 이메일을 도메인 등록자의 연락처로 보내 드립니다.

등록 및 갱신을 위한 임대 기간

1~5년.

제한 사항

일반에 공개되어 있지만 다음과 같은 몇 가지 제한이 있습니다.

- .com.au 및 .net.au 도메인은 호주에 등록되어 있는 제휴 업체 또는 개인 사업자, 호주에서 사업 허가를 받은 해외 기업, 호주 등록 상표를 출원한 신청자 또는 상표 소유자가 사용할 수 있습니다. 개인은 .com.au/.net.au 도메인을 등록할 수 없습니다. 등록자 연락처는 회사여야 합니다.
- 도메인 이름은 등록자의 이름(해당하는 호주 당국에 등록된 이름) 또는 상표(또는 상표의 약어나 두문자어)와 일치해야 합니다.
- 도메인 이름은 등록자의 활동을 의미해야 합니다. 예를 들어, 등록자가 판매하는 제품이나 제공하는 서비스를 나타낼 수 있습니다.
- 등록 과정에서 다음 정보를 제공해야 합니다.
  - 등록 유형: ABN(호주 기업 번호), ACN(호주 회사 번호) 또는 도메인 이름이 상표와 일치하는 경우 TM(상표)
  - 도메인 이름이 상표에 해당하는 경우 호주 사업자 번호(ABN), 호주 회사 번호(ACN) 또는 상표 번호(TM)가 될 수 있는 사용자의 ID 번호.
  - 해당 주 또는 지방

- 이름, ABN 또는 상표(TM) 번호를 비롯한 연락처 정보가 잘못되거나 일치하지 않으면 등록, 거래 및 갱신이 실패합니다. 기존 도메인에 대한 정보를 수정하려면 소유권을 변경해야 할 수 있습니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원하지 않음. RetrieveDomainAuthCode API 작업에 대한 액세스를 제한하여 무단 이전을 방지하는 것이 좋습니다. (이 Route 53 API에 대한 액세스를 제한할 때 Route 53 콘솔, AWS SDKs 및 기타 프로그래밍 방법을 사용하여 권한 부여 코드를 생성할 수 있는 사용자도 제한합니다.) 자세한 내용은 Amazon Route 53의 Identity and Access Management 단원을 참조하십시오.

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 키를 설정할 때 DNS 보안 알고리즘 2(DH)를 선택해야 합니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신: 만료 날짜 60일 전 ~ 만료 날짜 사이
- Route 53를 사용한 늦은 갱신: 만료 후 29일까지
- Route 53에서 도메인 삭제: 만료 후 29일
- 레지스트리 복원: 불가능
- 레지스트리에서 도메인 삭제: 만료 후 30일

도메인 등록 삭제

.com.au 도메인을 등록했다고 해서 등록된 도메인을 삭제할 수 있는 것은 아닙니다. 그 대신, 자동 갱신을 해제하고 도메인이 만료되기를 기다려야 합니다. 자세한 내용은 도메인 이름 등록 삭제 단원을 참조하십시오.

소유권 변경

프로그래밍 방식으로 또는 Route 53 콘솔을 사용하여 소유자를 변경합니다. 도메인 연락처 정보 업데이트을 참조하세요. 그런 후 다음 프로세스를 완료하여 소유권 변경을 완료합니다.

1. 이전 등록자와 새 등록자는 모두 transfers@1api.net에서 이메일 주소로 받은 링크를 클릭해야 합니다. 14일 이내에 완료하지 않는 경우, 프로세스를 다시 시작해야 합니다.

2. 응답이 확인되면 레지스트리의 소유자 변경이 추가 확인없이 짧은 시간 내에 처리됩니다.

.com.sg(싱가포르)

> **Important**
>
> 더 이상 Route 53를 사용하여 새 .com.sg 도메인을 등록하거나 .com.sg 도메인을 Route 53으로 이전할 수 없습니다. 이미 Route 53에 등록된 .com.sg 도메인은 계속 지원됩니다.

Return to index

갱신 기간

1~2년.

도메인 등록 삭제

.com.sg 도메인을 등록했다고 해서 등록된 도메인을 삭제할 수 있는 것은 아닙니다. 그 대신, 자동 갱신을 해제하고 도메인이 만료되기를 기다려야 합니다. 자세한 내용은 도메인 이름 등록 삭제 단원을 참조하십시오.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

이전하는 데 필요한 권한 부여 코드

지원하지 않음. 더 이상 Route 53으로 .com.sg 도메인을 이전할 수 없습니다.

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지

- Route 53를 사용한 늦은 갱신: 만료 후 29일까지
- Route 53에서 도메인 삭제: 만료 후 30일
- 레지스트리 복원: 만료 후 30일 ~ 60일 사이
- 레지스트리에서 도메인 삭제: 만료 후 60일

.fm(미크로네시아 연방 공화국)

온라인 미디어 및 방송 관련 조직들이 종종 일반 TLD로도 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

제한 없이 일반에 공개되어 있습니다.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지

- Route 53에서 도메인 삭제: 만료 후 44일
- 레지스트리 복원: 만료 후 44일 ~ 79일 사이
- 레지스트리에서 도메인 삭제: 만료 후 84일

.in(인도)

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

제한 없이 일반에 공개되어 있습니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

지원하지 않음.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 29일까지
- Route 53에서 도메인 삭제: 만료 후 30일
- 레지스트리 복원: 만료 후 30일 ~ 60일 사이
- 레지스트리에서 도메인 삭제: 만료 후 65일

.jp(일본)

Return to index

등록 및 갱신을 위한 임대 기간

1년.

제한 사항

일반에 공개되어 있지만 한 가지 제한이 있습니다.

- 일본 국내의 개인 또는 회사만 .jp 도메인 이름을 등록할 수 있습니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

일본어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예.

.jp 레지스트리는 Timetime-to-live로 권한 부여 코드를 관리하며 만료될 수 있습니다. 도메인이 있는 경우 도메인에서 전송 잠금(clientTransferProhibited) 상태를 제거하여 인증 코드를 새로 고칠 수 있습니다. 도메인에 전송 잠금이 없는 경우 먼저 켠 다음 꺼서 인증 코드를 새로 고칠 수 있습니다.

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신: 만료 날짜 30일 전~7일 전
- Route 53를 사용한 늦은 갱신: 불가능
- Route 53에서 도메인 삭제: 만료 6일 전
- 등록처 복원 가능: AWS Support에 문의하세요.
- 등록처에서 도메인 삭제: AWS Support에 문의하세요.

> **Note**
>
> .co.jp 및 .or.jp와 같은 범용이 아닌 JP 도메인은 현재 등록할 수 없습니다.

.io(영국령 인도양 식민지)

온라인 서비스, 브라우저 기반 게임, 신생 기업 같은 컴퓨터 관련 조직들이 종종 일반 TLD로도 사용합니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

제한 없이 일반에 공개되어 있습니다.

개인 정보 보호

시/도 및 국가를 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

또한 .io 도메인용 레지스트리는 개인 정보 보호를 활성화하거나 비활성화하는 등의 일부 작업에 대한 일회용 암호로 권한 부여 코드를 사용합니다. 암호가 필요한 작업을 두 개 이상 수행할 경우 각 작업마다 다른 권한 부여 코드를 생성해야 합니다.

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지

- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 90일

.net.au(호주)

Return to index

TLD 등록부의 확인 이메일

등록 대행 협력사인 Gandi에서는 DomainDirectors를 통해 .net.au 도메인을 재판매합니다. Route 53으로 도메인 이름을 이전하는 경우, DomainDirectors에서 연락처 정보를 확인하는 이메일이나 이전 요청을 허가하는 이메일을 도메인 등록자의 연락처로 보내 드립니다.

등록 및 갱신을 위한 임대 기간

1~5년.

제한 사항

두 번째 수준 도메인만 사용할 수 있습니다. Route 53는 두 번째 수준 도메인(.com.au 및 net.au.)을 지원합니다.

일반에 공개되어 있지만 다음과 같은 몇 가지 제한이 있습니다.

- .com.au 및 .net.au 도메인은 호주에 등록되어 있는 법인, 무역업체, 제휴업체 또는 개인 사업자, 호주에서 사업 허가를 받은 해외 기업, 호주 등록 상표를 출원한 신청자 또는 상표 소유자가 사용할 수 있습니다.
- 도메인 이름은 해당하는 호주 당국에 등록된 등록자의 이름 또는 상표(또는 그 약어나 두문자어)와 일치해야 합니다.
- 도메인 이름은 등록자의 활동을 의미해야 합니다. 예를 들어, 등록자가 판매하는 제품이나 제공하는 서비스를 나타낼 수 있습니다.
- 등록 과정에서 다음을 제시해야 합니다.
  - 등록 유형: ABN(호주 기업 번호), ACN(호주 회사 번호) 또는 도메인 이름이 상표와 일치하는 경우 TM(상표)
  - 도메인 이름이 상표에 해당하는 경우 호주 사업자 번호(ABN), 호주 회사 번호(ACN) 또는 상표 번호(TM)가 될 수 있는 사용자의 ID 번호.
  - 해당 주 또는 지방

- 이름, ABN 또는 상표(TM) 번호를 비롯한 연락처 정보가 잘못되거나 일치하지 않으면 등록, 거래 및 갱신이 실패합니다. 기존 도메인에 대한 정보를 수정하려면 소유권을 변경해야 할 수 있습니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원하지 않음. RetrieveDomainAuthCode API 작업에 대한 액세스를 제한하여 무단 이전을 방지하는 것이 좋습니다. (이 Route 53 API에 대한 액세스를 제한할 때 Route 53 콘솔, AWS SDKs 및 기타 프로그래밍 방법을 사용하여 권한 부여 코드를 생성할 수 있는 사용자도 제한합니다.) 자세한 내용은 Amazon Route 53의 Identity and Access Management 단원을 참조하십시오.

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 키를 설정할 때 DNS 보안 알고리즘 2(DH)를 선택해야 합니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신: 만료 날짜 60일 전 ~ 만료 날짜 사이
- Route 53를 사용한 늦은 갱신: 만료 후 29일까지
- Route 53에서 도메인 삭제: 만료 후 29일
- 레지스트리 복원: 불가능
- 레지스트리에서 도메인 삭제: 만료 후 30일

도메인 등록 삭제

.net.au 도메인을 등록했다고 해서 등록된 도메인을 삭제할 수 있는 것은 아닙니다. 그 대신, 자동 갱신을 해제하고 도메인이 만료되기를 기다려야 합니다. 자세한 내용은 도메인 이름 등록 삭제 단원을 참조하십시오.

소유권 변경

프로그래밍 방식으로 또는 Route 53 콘솔을 사용하여 소유자를 변경합니다. 도메인 연락처 정보 업데이트을 참조하세요. 그런 후 다음 프로세스를 완료하여 소유권 변경을 완료합니다.

1. 이전 등록자와 신규 등록자 모두 transfers@1api.net에서 이메일 주소로 받은 링크를 클릭해야 합니다. 14일 이내에 완료하지 않는 경우, 프로세스를 다시 시작해야 합니다.

2. 응답이 확인되면 레지스트리의 소유자 변경이 추가 확인없이 짧은 시간 내에 처리됩니다.

.net.nz (뉴질랜드)

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

.co.nz, .net.nz, .org.nz와 같은 두 번째 수준 도메인을 Route 53에 등록할 수 있습니다. Route 53를 통해 .nz(첫 번째 수준) 도메인을 등록하거나 .nz 도메인을 Route 53으로 이전할 수 없습니다.

일반에 공개되어 있지만 다음과 같은 몇 가지 제한이 있습니다.

- 개인의 경우 18세 이상이어야 합니다.
- 단체의 경우 등록된 단체여야 합니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원하지 않음. RetrieveDomainAuthCode API 작업에 대한 액세스를 제한하여 무단 이전을 방지하는 것이 좋습니다. (이 Route 53 API에 대한 액세스를 제한할 때 Route 53 콘솔, AWS SDKs 및 기타 프로그래밍 방법을 사용하여 권한 부여 코드를 생성할 수 있는 사용자도 제한합니다.) 자세한 내용은 Amazon Route 53의 Identity and Access Management 단원을 참조하십시오.

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 44일
- 레지스트리 복원: 만료 후 44일~134일
- 레지스트리에서 도메인 삭제: 만료 후 134일

.org.nz(뉴질랜드)

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

.co.nz, .net.nz, .org.nz와 같은 두 번째 수준 도메인을 Route 53에 등록할 수 있습니다. Route 53를 통해 .nz(첫 번째 수준) 도메인을 등록하거나 .nz 도메인을 Route 53으로 이전할 수 없습니다.

일반에 공개되어 있지만 다음과 같은 몇 가지 제한이 있습니다.

- 개인의 경우 18세 이상이어야 합니다.
- 단체의 경우 등록된 단체여야 합니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원하지 않음. RetrieveDomainAuthCode API 작업에 대한 액세스를 제한하여 무단 이전을 방지하는 것이 좋습니다. (이 Route 53 API에 대한 액세스를 제한할 때 Route 53 콘솔, AWS SDKs 및 기타 프로그래밍 방법을 사용하여 권한 부여 코드를 생성할 수 있는 사용자도 제한합니다.) 자세한 내용은 Amazon Route 53의 Identity and Access Management 단원을 참조하십시오.

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 44일
- 레지스트리 복원: 만료 후 44일~134일
- 레지스트리에서 도메인 삭제: 만료 후 134일

.pw(팔라우)

Return to index

.pw는 원래 서태평양의 오세아니아 미크로네시아 하위 리전에 있는 섬 국가인 팔라우 거주자를 위해 예약되었지만, 이제는 일반적으로 '전문 웹'을 나타내는 데 사용되며 누구나 사용할 수 있습니다.

등록 및 갱신을 위한 임대 기간

1~10년.

개인 정보 보호(개인, 회사, 협회, 공공 단체와 같은 모든 유형의 연락처 유형에 적용됨)

조직 이름을 제외한 모든 정보를 숨깁니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 75일

.qa(카타르)

> **Important**
>
> 더 이상 Route 53를 사용하여 새 .qa 도메인을 등록하거나 .qa 도메인을 Route 53으로 이전할 수 없습니다. 이미 Route 53에 등록된 .qa 도메인은 계속 지원됩니다.

Return to index

갱신 기간

1~5년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원하지 않음. RetrieveDomainAuthCode API 작업에 대한 액세스를 제한하여 무단 이전을 방지하는 것이 좋습니다. (이 Route 53 API에 대한 액세스를 제한할 때 Route 53 콘솔, AWS SDKs 및 기타 프로그래밍 방법을 사용하여 권한 부여 코드를 생성할 수 있는 사용자도 제한합니다.) 자세한 내용은 Amazon Route 53의 Identity and Access Management 단원을 참조하십시오.

이전하는 데 필요한 권한 부여 코드

지원하지 않음. 더 이상 Route 53으로 .qa 도메인을 이전할 수 없습니다.

DNSSEC

지원하지 않음.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지

- Route 53를 사용한 늦은 갱신: 만료 후 29일까지
- Route 53에서 도메인 삭제: 만료 후 30일
- 레지스트리 복원: 불가능
- 레지스트리에서 도메인 삭제: 만료 후 31일

.ru(러시아 연방)

> **Important**
>
> 더 이상 Route 53를 사용하여 새 .ru 도메인을 등록하거나 .ru 도메인을 Route 53으로 이전할 수 없습니다. 이미 Route 53에 등록된 .ru 도메인은 계속 지원됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1년.

> **Note**
>
> .ru 도메인의 등록 기관은 도메인이 만료되는 날에 도메인 만료 날짜를 업데이트합니다. WHOIS 쿼리는 Route 53으로 도메인을 갱신하는 시기와 관계없이 해당 날짜까지 도메인의 이전 만료 날짜를 표시합니다.

제한 사항

일반에 공개되어 있지만 다음과 같은 몇 가지 제한이 있습니다.

- 개인은 여권 번호 또는 정부 발행 ID 번호를 제시해야 할 수 있습니다.
- 해외 회사는 회사 ID 또는 회사 등록 정보를 제시해야 할 수 있습니다.

개인 정보 보호

등록처에 따라 결정됨

무단 이전을 방지하기 위한 도메인 잠금

지원하지 않음. RetrieveDomainAuthCode API 작업에 대한 액세스를 제한하여 무단 이전을 방지하는 것이 좋습니다. (이 Route 53 API에 대한 액세스를 제한할 때 Route 53 콘솔, AWS SDKs 및 기

타 프로그래밍 방법을 사용하여 권한 부여 코드를 생성할 수 있는 사용자도 제한합니다.) 자세한 내용은 Amazon Route 53의 Identity and Access Management 단원을 참조하십시오.

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

지원하지 않음. 더 이상 Route 53으로 .ru 도메인을 이전할 수 없습니다.

DNSSEC

지원하지 않음.

도메인 갱신 및 복원 기한

- 갱신: 만료 날짜 2일 전까지
- Route 53를 사용한 늦은 갱신: 불가능
- Route 53에서 도메인 삭제: 만료 2일 전
- 레지스트리 복원: 만료 2일 전 ~ 만료 후 28일 사이
- 레지스트리에서 도메인 삭제: 만료 후 28일

도메인 등록 삭제

.ru 도메인을 등록했다고 해서 등록된 도메인을 삭제할 수 있는 것은 아닙니다. 그 대신, 자동 갱신을 해제하고 도메인이 만료되기를 기다려야 합니다. 자세한 내용은 도메인 이름 등록 삭제 단원을 참조하십시오.

.sg(싱가포르)

> **Important**
>
> 더 이상 Route 53를 사용하여 새 .sg 도메인을 등록하거나 .sg 도메인을 Route 53으로 이전할 수 없습니다. 이미 Route 53에 등록된 .sg 도메인은 계속 지원됩니다.

Return to index

갱신 기간

1~2년.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

이전하는 데 필요한 권한 부여 코드

지원하지 않음. 더 이상 Route 53으로 .sg 도메인을 이전할 수 없습니다.

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 29일까지
- Route 53에서 도메인 삭제: 만료 후 30일
- 레지스트리 복원: 만료 후 30일 ~ 60일 사이
- 레지스트리에서 도메인 삭제: 만료 후 60일

도메인 등록 삭제

.sg 도메인을 등록했다고 해서 등록된 도메인을 삭제할 수 있는 것은 아닙니다. 그 대신, 자동 갱신을 해제하고 도메인이 만료되기를 기다려야 합니다. 자세한 내용은 도메인 이름 등록 삭제 단원을 참조하십시오.

유럽

Amazon Route 53에 도메인을 등록하는 데 다음 최상위 도메인(TLD)을 유럽에서 사용할 수 있습니다.

, , , , , , , , , , , , , , , , , , , ,

Return to index

.be(벨기에)

Return to index

등록 및 갱신을 위한 임대 기간

1년.

제한 사항

제한 없이 일반에 공개되어 있습니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예. DNS 벨기에 웹사이트에서 이전 코드를 가져올 수 있습니다.

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 불가능
- Route 53에서 도메인 삭제: 만료 날짜
- 레지스트리 복원: 만료 후 40일까지
- 레지스트리에서 도메인 삭제: 만료 후 40일

.berlin(독일 베를린 시)

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

일반에 공개되어 있지만 다음과 같은 몇 가지 제한이 있습니다.

- 소유자, 관리자 또는 기술 담당자는 베를린 내 주소가 있어야 하며 관리 담당자는 개인이어야 합니다.
- .berlin 도메인을 등록하고 12개월 이내에 도메인을 활성화하고 사용해야 합니다(웹 사이트, 리디렉션 또는 이메일 주소에 해당).
- .berlin 도메인으로 웹 사이트를 게시하거나 .berlin 도메인에서 다른 웹 사이트로 리디렉션하는 경우, 해당 웹 사이트의 콘텐츠가 베를린과 관련된 것이어야 합니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

라틴어 및 키릴 자모에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 80일

.ch(스위스)

Return to index

등록 및 갱신을 위한 임대 기간

1년.

제한 사항

제한 없이 일반에 공개되어 있습니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원하지 않음. RetrieveDomainAuthCode API 작업에 대한 액세스를 제한하여 무단 이전을 방지하는 것이 좋습니다. (이 Route 53 API에 대한 액세스를 제한할 때 Route 53 콘솔, AWS SDKs 및 기타 프로그래밍 방법을 사용하여 권한 부여 코드를 생성할 수 있는 사용자도 제한합니다.) 자세한 내용은 Amazon Route 53의 Identity and Access Management 단원을 참조하십시오.

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 9일까지
- Route 53에서 도메인 삭제: 만료 후 9일
- 레지스트리 복원: 만료 후 9일 ~ 49일 사이
- 레지스트리에서 도메인 삭제: 만료 후 49일

.co.uk(영국)

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

제한 없이 일반에 공개되어 있습니다.

개인 정보 보호

모든 정보가 숨겨집니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

.co.uk 도메인을 Route 53으로 이전할 경우, 권한 부여 코드를 얻지 않아도 됩니다. 대신에 현재 도메인 등록 대행자가 제공하는 방법을 사용해 도메인에 대한 IPS 태그의 값을 [GANDI](모두 대문자)로 업데이트합니다. (IPS 태그는 .uk 도메인 이름 등록부인 Nominet에 필요한 것입니다). 등록 대행자가 IPS 태그의 값을 변경하지 않으려 하면 Nominet에 연락하십시오.

> **Note**
>
> .co.uk 도메인을 등록하면 Route 53에서 해당 도메인의 IPS 태그를 자동으로 GANDI로 설정합니다.

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신: 만료 날짜 180일 전 ~ 만료 날짜 후 30일 사이
- Route 53를 사용한 늦은 갱신: 만료 후 30일~90일 사이
- Route 53에서 도메인 삭제: 만료 후 90일
- 레지스트리 복원: 불가능

- 레지스트리에서 도메인 삭제: 만료 후 92일

도메인 등록 삭제

.co.uk 도메인을 등록했다고 해서 등록된 도메인을 삭제할 수 있는 것은 아닙니다. 그 대신, 자동 갱신을 해제하고 도메인이 만료되기를 기다려야 합니다. 자세한 내용은 도메인 이름 등록 삭제 단원을 참조하십시오.

.cz(체코 공화국)

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

제한 없이 일반에 공개되어 있습니다.

개인 정보 보호

지원되지 않지만 이메일 주소와 전화 번호는 모든 연락처에서 숨겨져 있습니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

현재 등록 기관이 승인 코드를 제공하지 않는 경우 `https://www.nic.cz/whois/send-password/`로 이동하여 CZ 도메인 레지스트리에서 등록자 이메일 주소로 승인 코드를 전송해달라고 요청하십시오.

DNSSEC

지원하지 않음.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지

- Route 53를 사용한 늦은 갱신: 만료 후 58일까지
- Route 53에서 도메인 삭제: 만료 후 59일
- 레지스트리 복원: 불가능
- 레지스트리에서 도메인 삭제: 만료 후 60일

.de(독일)

Return to index

등록 및 갱신을 위한 임대 기간

1년.

제한 사항

일반에 공개되어 있지만 다음과 같은 몇 가지 제한이 있습니다.

- 본인이 독일에 거주하거나, 독일에 거주하고 사서함이 아닌 주소를 보유한 관리 담당자(실제 인물)를 두어야 합니다.
- 등록 기관의 구역 확인을 통과할 수 있도록 등록 과정에서 도메인 이름의 DNS(A, MX, CNAME)를 정확히 구성해야 합니다. 두 가지 C 클래스의 서버 세 개가 필요합니다.
- Route 53 이외의 DNS 서비스를 사용하는 경우 도메인의 이름 서버가 올바르게 구성되었는지 확인하려면 확인을 통과해야 합니다. 다음과 같이 도메인의 이름 서버가 확인을 통과할지 여부를 판단하려면 https://www.denic.de/en/service/tools/nast/ 섹션을 참조하세요.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원하지 않음. RetrieveDomainAuthCode API 작업에 대한 액세스를 제한하여 무단 이전을 방지하는 것이 좋습니다. (이 Route 53 API에 대한 액세스를 제한할 때 Route 53 콘솔, AWS SDKs 및 기타 프로그래밍 방법을 사용하여 권한 부여 코드를 생성할 수 있는 사용자도 제한합니다.) 자세한 내용은 Amazon Route 53의 Identity and Access Management 단원을 참조하십시오.

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 불가능
- Route 53에서 도메인 삭제: 만료 날짜
- 등록처 복원 가능: AWS Support에 문의하세요.
- 등록처에서 도메인 삭제: AWS Support에 문의하세요.

.es(스페인)

Return to index

도메인 구입 또는 이전

> **Important**
>
> 현재 새 .es 도메인을 구매하거나 .es 도메인을 Route 53으로 이전할 수 있습니다. 등록자 연락처의 연락처 유형에는 제한이 없습니다. 관리자/기술 담당자/청구 담당자 연락처 유형은 사람이어야 합니다.

등록 및 갱신을 위한 임대 기간

1~5년.

제한 사항

일반에 공개되어 있으며 스페인과 관계가 있거나 스페인에 관심이 있는 경우 사용할 수 있습니다.

2016년부터 ES 도메인 등록자는 등록자 연락처 이메일을 제공해야 합니다. 이 정보를 제공하지 않은 경우, 도메인을 Route 53으로 이전하기 전에 현재 등록 대행자에게 정보를 제공해야 합니다.

다음 정보가 필요합니다.

- ESNIC 식별자는 *AAAA0-ESNIC-F0*과 유사합니다.
- ESNIC 식별자를 모르는 경우 현재 등록 대행자에게 받을 수 있습니다. 등록 대행자는 https://www.dominios.es/en에서 찾을 수 있습니다.

등록 대행자에서 암호를 기억하고 있는지 여부에 따라 다음 절차 중 하나를 수행하여 등록자 이메일을 업데이트할 수 있습니다.

- 암호가 기억나는 경우 ESNIC ID과 암호를 사용하여 https://www.nic.es/sgnd/login.action에 로그인합니다.

  로그인한 후 레지스트리 페이지에서 편집 탭을 선택하여 등록자 이메일 연락처를 편집할 수 있습니다.
- 암호를 잊어버린 경우 https://www.nic.es/sgnd/peticion/editCorreo.action?request_locale=en으로 이동합니다.

  양식에 ESNIC 식별자, 유효한 새 등록자 이메일 연락처를 작성합니다. 그런 다음 eID/인증서 없이 처리를 선택하여 양식을 확인하고 요청된 자격 증명 문서를 업로드합니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

.es 레지스트리는 time-to-live로 권한 부여 코드를 관리하며 만료될 수 있습니다. 도메인이 있는 경우 도메인에서 전송 잠금(clientTransferProhibited) 상태를 제거하여 인증 코드를 새로 고칠 수 있습니다. 도메인에 전송 잠금이 없는 경우 먼저 켠 다음 꺼서 인증 코드를 새로 고칠 수 있습니다.

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신: 만료 날짜 6일 전까지
- Route 53를 사용한 늦은 갱신: 불가능
- Route 53에서 도메인 삭제: 만료 6일 전
- 레지스트리 복원: 만료 6일 전 ~ 만료 후 4일 사이

- 레지스트리에서 도메인 삭제: 만료 후 4일

.eu(유럽 연합)

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

일반에 공개되어 있지만 한 가지 제한이 있습니다.

- 유럽 경제 지역(EEA) 30개 국가 중 하나에서 유효한 우편 주소를 제공해야 하며, 유럽 연합(EU) 27개 회원국 중 한 국가의 시민인 경우 EU 국적을 지정해야 합니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원하지 않음. RetrieveDomainAuthCode API 작업에 대한 액세스를 제한하여 무단 이전을 방지하는 것이 좋습니다. (이 Route 53 API에 대한 액세스를 제한할 때 Route 53 콘솔, AWS SDKs 및 기타 프로그래밍 방법을 사용하여 권한 부여 코드를 생성할 수 있는 사용자도 제한합니다.) 자세한 내용은 Amazon Route 53의 Identity and Access Management 단원을 참조하십시오.

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

레지스트리의 'My.eu' 패널 https://my.eurid.eu/을 사용하여 인증 코드를 생성할 수도 있습니다.

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 불가능

- Route 53에서 도메인 삭제: 만료 날짜
- 레지스트리 복원: 만료 후 40일까지
- 레지스트리에서 도메인 삭제: 만료 후 40일

WHOIS 검색

기존 .eu 도메인에 대한 자세한 내용은 https://whois.eurid.eu/en/을 참조하세요.

.fi(핀란드)

Return to index

등록 및 갱신을 위한 임대 기간

1~5년.

제한 사항

일반에 공개되어 있지만 다음과 같은 몇 가지 제한이 있습니다.

- .fi 확장명은 핀란드에 거주지가 있고 핀란드 국민 식별 번호가 있는 개인 및 핀란드에 등록된 법인 또는 사기업에서 사용할 수 있습니다.
- 등록자 연락처 주소가 핀란드에 있다면 개인 등록자의 경우 핀란드 ID 번호가 필요하고 회사 등록자의 경우 핀란드 회사 번호가 필요합니다. 등록 시 다음 정보를 제공해야 합니다.
  - 실제로 또는 기록상 핀란드에 있는 사람이 담당자인지 여부
  - 기록상 이름을 사용하는 경우, 해당 이름이 기록된 명부의 식별 정보
  - 기록상 이름을 사용하는 경우, 해당 이름이 기록된 명부의 기록 정보
  - 기록상 인물의 핀란드 국내 식별 번호
  - 실제 인물의 핀란드 국내 식별 번호
  - 등록자가 비 핀란드 회사인 경우 사업자 번호를 VAT_Number로 제공해야 합니다.
- 등록자 주소가 핀란드에 있지 않다면 핀란드 신분증이나 회사 번호는 필요하지 않습니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원하지 않음. RetrieveDomainAuthCode API 작업에 대한 액세스를 제한하여 무단 이전을 방지하는 것이 좋습니다. (이 Route 53 API에 대한 액세스를 제한할 때 Route 53 콘솔, AWS SDKs 및 기

타 프로그래밍 방법을 사용하여 권한 부여 코드를 생성할 수 있는 사용자도 제한합니다.) 자세한 내용은 Amazon Route 53의 Identity and Access Management 단원을 참조하십시오.

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 29일까지
- Route 53에서 도메인 삭제: 만료 후 30일
- 레지스트리 복원: 불가능
- 레지스트리에서 도메인 삭제: 불가능

도메인 등록 삭제

도메인 삭제에 대한 자세한 내용은 도메인 이름 등록 삭제 섹션을 참조하세요.

.fr(프랑스)

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

일반에 공개되어 있지만 다음과 같은 몇 가지 제한이 있습니다.

- 개인은 18세 이상이어야 하며 생년월일을 제시해야 합니다.
- 단체는 유럽경제지역 또는 스위스에 위치해야 합니다.
- 단체는 나중에 AFNIC에서 신속하게 확인할 수 있도록 모든 회사 식별 필드(VAT 번호, SIREN, WALDEC, DUNS 등)에 값을 입력해야 합니다.

- 관리 담당자에게도 동일한 자격 조건이 적용됩니다.
- 이름과 용어는 AFNIC의 사전 검토(Naming Charter Article 2.4)에 따라 변경될 수 있으며 다음과 같은 추가 조건이 적용될 수 있습니다.
  - 이전에 예약 또는 금지된 도메인 이름은 정당한 법적 권한을 가지고 선의로 행동하는 신청자가 사용할 수 있습니다.
  - ville, mairie, agglo, cc, cg 및 cr로 시작하는 이름에는 AFNIC 명명 규정이 적용될 수 있습니다.

개인 정보 보호

등록처에 따라 결정됨

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 27일까지
- Route 53에서 도메인 삭제: 만료 후 28일
- 레지스트리 복원: 만료 후 28일 ~ 58일 사이
- 레지스트리에서 도메인 삭제: 만료 후 58일

.gg(건지)

Return to index

등록 및 갱신을 위한 임대 기간

1년.

제한 사항

제한 없이 일반에 공개되어 있습니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 29일까지
- Route 53에서 도메인 삭제: 만료 후 30일
- 레지스트리 복원: 만료 후 30일 ~ 35일 사이
- 레지스트리에서 도메인 삭제: 만료 후 35일

.im(맨 섬)

"I am" 개인 브랜드를 개발하려는 개인들의 인스턴트 메시징 서비스에서 종종 일반 TLD로도 사용됩니다.

Return to index

등록 및 갱신을 위한 임대 기간

1~2년.

제한 사항

제한 없이 일반에 공개되어 있습니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

지원하지 않음.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 29일까지
- Route 53에서 도메인 삭제: 만료 후 30일
- 레지스트리 복원: 불가능
- 레지스트리에서 도메인 삭제: 만료 후 30일

.it(이탈리아)

Return to index

등록 및 갱신을 위한 임대 기간

1년.

제한 사항

일반에 공개되어 있지만 다음과 같은 몇 가지 제한이 있습니다.

- 개인 또는 단체는 유럽 연합 내에 등록된 주소가 있어야 합니다.
- 원산지 국가가 이탈리아인 경우, 회계 코드를 입력해야 합니다. 원산지 국가가 유럽 연합에 속하는 경우, ID 서류 번호(ID 번호)를 입력해야 합니다.

- 연락처 유형에 대해 [Company], [Association] 또는 [Public body]를 지정하는 경우 VAT 번호(부가가치세 식별 번호)가 필요합니다.
- 도메인의 이름 서버는 DNS 확인을 통과해야 합니다. 변경 요청을 제출하기 전에 https://dns-check.nic.it/에서 이름 서버를 확인하는 것이 좋습니다. 도메인 이름이 기술적 요구 사항에 맞지 않고(예를 들어, 작업 이름 서버와 연결되지 않은 경우) 30일 이내에 이를 수정하지 않은 경우, 등록처에서 도메인 이름을 삭제합니다. 기술 요구 사항을 충족하지 않기 때문에 삭제되는 도메인에 대해서는 수수료가 환불되지 않습니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원하지 않음. RetrieveDomainAuthCode API 작업에 대한 액세스를 제한하여 무단 이전을 방지하는 것이 좋습니다. (이 Route 53 API에 대한 액세스를 제한할 때 Route 53 콘솔, AWS SDKs 및 기타 프로그래밍 방법을 사용하여 권한 부여 코드를 생성할 수 있는 사용자도 제한합니다.) 자세한 내용은 Amazon Route 53의 Identity and Access Management 단원을 참조하십시오.

다국어 도메인 이름

지원

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

지원하지 않음.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 13일까지
- 레지스트리에서 도메인 삭제: 만료 후 49일
- 레지스트리 복원: 만료 후 14일 ~ 44일 사이
- 등록처에서 도메인 삭제: AWS Support에 문의하세요.

.me(몬테네그로)

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

.me 도메인 등록 기관 Domain.me에서는 2자 도메인 이름 및 일부 긴 도메인 이름을 프리미엄 도메인 이름으로 간주합니다. 프리미엄 .me 도메인을 Route 53로 등록하거나 이전할 수 없습니다. 프리미엄 .me 도메인 이름에 대한 자세한 정보는 domain.me 웹 사이트를 참조하십시오.

개인 정보 보호

모든 정보가 숨겨집니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

아랍어, 벨로루시어, 보스니아어, 불가리아어, 중국어(간체), 중국어(번체), 크로아티아어, 덴마크어, 프랑스어, 독일어, 힌디어, 헝가리어, 아이슬란드어, 이탈리아어, 한국어, 라트비아어, 리투아니아어, 몽골어, 몬테네그로어, 폴란드어, 포르투갈어, 러시아어, 세르비아어, 스페인어, 스웨덴어, 터키어, 우크라이나어가 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 29일까지
- Route 53에서 도메인 삭제: 만료 후 30일
- 레지스트리 복원: 만료 후 30일 ~ 60일 사이
- 레지스트리에서 도메인 삭제: 만료 후 65일

.me.uk(영국)

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

제한 없이 일반에 공개되어 있습니다.

개인 정보 보호

모든 정보가 숨겨집니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

.me.uk 도메인을 Route 53으로 이전하는 경우, 권한 부여 코드를 얻지 않아도 됩니다. 대신에 현재 도메인 등록 대행자가 제공하는 방법을 사용해 도메인에 대한 IPS 태그의 값을 [GANDI](모두 대문자)로 업데이트합니다. (IPS 태그는 .uk 도메인 이름 등록부인 Nominet에 필요한 것입니다). 등록 대행자가 IPS 태그의 값을 변경하지 않으려 하면 Nominet에 연락하십시오.

> **Note**
>
> .me.uk 도메인을 등록하면 Route 53에서 해당 도메인의 IPS 태그를 자동으로 GANDI로 설정합니다.

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신: 만료 날짜 180일 전 ~ 만료 날짜 후 30일 사이
- Route 53를 사용한 늦은 갱신: 만료 후 30일~90일 사이
- Route 53에서 도메인 삭제: 만료 후 90일
- 레지스트리 복원: 불가능

- 레지스트리에서 도메인 삭제: 만료 후 92일

도메인 등록 삭제

.me.uk 도메인의 등록처에서는 등록된 도메인을 삭제하도록 허용하지 않습니다. 그 대신, 자동 갱신을 해제하고 도메인이 만료되기를 기다려야 합니다. 자세한 내용은 도메인 이름 등록 삭제 단원을 참조하십시오.

.nl(네덜란드)

Return to index

등록 및 갱신을 위한 임대 기간

1년.

제한 사항

일반에 공개되어 있지만 다음과 같은 몇 가지 제한이 있습니다.

- 소유자 또는 관리 담당자의 유효한 네덜란드 국내 주소를 제시해야 합니다. 현지에 거주해야 합니다.
- 유효한 네덜란드 국내 주소가 없는 경우, SIDN 등록 기관에서 거주지 주소 절차에 따라 거주지 주소를 제공합니다.
- 도메인 이름은 .nl을 제외한 3-63자여야 합니다.

개인 정보 보호

등록처에 따라 결정됨

무단 이전을 방지하기 위한 도메인 잠금

지원하지 않음. RetrieveDomainAuthCode API 작업에 대한 액세스를 제한하여 무단 이전을 방지하는 것이 좋습니다. (이 Route 53 API에 대한 액세스를 제한할 때 Route 53 콘솔, AWS SDKs 및 기타 프로그래밍 방법을 사용하여 권한 부여 코드를 생성할 수 있는 사용자도 제한합니다.) 자세한 내용은 Amazon Route 53의 Identity and Access Management 단원을 참조하십시오.

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신: 만료 날짜 1일 전까지
- Route 53를 사용한 늦은 갱신: 불가능
- Route 53에서 도메인 삭제: 만료 1일 전
- 레지스트리 복원: 만료 1일 전 ~ 만료 후 39일 사이
- 레지스트리에서 도메인 삭제: 만료 후 39일

.org.uk(영국)

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

제한 없이 일반에 공개되어 있습니다.

개인 정보 보호

모든 정보가 숨겨집니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

.org.uk 도메인을 Route 53으로 이전할 경우, 권한 부여 코드를 얻지 않아도 됩니다. 대신에 현재 도메인 등록 대행자가 제공하는 방법을 사용해 도메인에 대한 IPS 태그의 값을 [GANDI](모두 대문자)로 업데이트합니다. (IPS 태그는 .uk 도메인 이름 등록부인 Nominet에 필요한 것입니다). 등록 대행자가 IPS 태그의 값을 변경하지 않으려 하면 Nominet에 연락하십시오.

> **Note**
>
> .org.uk 도메인을 등록하면 Route 53에서 해당 도메인의 IPS 태그를 자동으로 GANDI로 설정합니다.

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신: 만료 날짜 180일 전 ~ 만료 날짜 후 30일 사이
- Route 53를 사용한 늦은 갱신: 만료 후 30일~90일 사이
- Route 53에서 도메인 삭제: 만료 후 90일
- 레지스트리 복원: 불가능
- 레지스트리에서 도메인 삭제: 만료 후 92일

도메인 등록 삭제

.org.uk 도메인을 등록했다고 해서 등록된 도메인을 삭제할 수 있는 것은 아닙니다. 그 대신, 자동 갱신을 해제하고 도메인이 만료되기를 기다려야 합니다. 자세한 내용은 도메인 이름 등록 삭제 단원을 참조하십시오.

.ruhr(독일 서부 루르 지방)

Return to index

.ruhr 확장명은 루르 지방(독일 서부)과 관련하여 사용합니다.

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

일반에 공개되어 있지만 한 가지 제한이 있습니다.

- 관리 담당자는 독일 국내 주소가 있는 개인이어야 합니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원됨(ä, ö, ü, ß).

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 등록처에서 도메인 삭제: AWS Support에 문의하세요.

.se(스웨덴)

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

일반에 공개되어 있지만 다음과 같은 몇 가지 제한이 있습니다.

- 스웨덴에 위치하는 경우 유효한 스웨덴 ID 번호를 제시해야 합니다. ID 번호 형식은 YYMMDD-NNNN입니다.
- 스웨덴 국외에 위치하는 경우 납세자 번호 등 유효한 ID 번호를 입력해야 합니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원하지 않음. RetrieveDomainAuthCode API 작업에 대한 액세스를 제한하여 무단 이전을 방지하는 것이 좋습니다. (이 Route 53 API에 대한 액세스를 제한할 때 Route 53 콘솔, AWS SDKs 및 기타 프로그래밍 방법을 사용하여 권한 부여 코드를 생성할 수 있는 사용자도 제한합니다.) 자세한 내용은 Amazon Route 53의 Identity and Access Management 단원을 참조하십시오.

다국어 도메인 이름

라틴어, 스웨덴어, 이디시어가 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신: 만료 날짜 1일 전까지
- Route 53를 사용한 늦은 갱신: 불가능
- Route 53에서 도메인 삭제: 만료 1일 전
- 레지스트리 복원: 만료 1일 전 ~ 만료 후 59일 사이
- 레지스트리에서 도메인 삭제: 만료 후 64일

.uk(영국)

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

제한 없이 일반에 공개되어 있습니다.

개인 정보 보호

모든 정보가 숨겨집니다.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

지원하지 않음.

이전하는 데 필요한 권한 부여 코드

uk 도메인을 Route 53으로 이전하는 경우, 권한 부여 코드를 얻지 않아도 됩니다. 대신에 현재 도메인 등록 대행자가 제공하는 방법을 사용해 도메인에 대한 IPS 태그의 값을 [GANDI](모두 대문자)로 업데이트합니다. (IPS 태그는 .uk 도메인 이름 등록부인 Nominet에 필요한 것입니다). 등록 대행자가 IPS 태그의 값을 변경하지 않으려 하면 Nominet에 연락하십시오.

> **Note**
>
> .uk 도메인을 등록하면 Route 53에서 해당 도메인의 IPS 태그를 자동으로 GANDI로 설정합니다.

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신: 만료 날짜 180일 전 ~ 만료 날짜 후 30일 사이
- Route 53를 사용한 늦은 갱신: 만료 후 30일~90일 사이
- Route 53에서 도메인 삭제: 만료 후 90일
- 레지스트리 복원: 불가능
- 레지스트리에서 도메인 삭제: 만료 후 92일

도메인 등록 삭제

.uk 도메인을 등록했다고 해서 등록된 도메인을 삭제할 수 있는 것은 아닙니다. 그 대신, 자동 갱신을 해제하고 도메인이 만료되기를 기다려야 합니다. 자세한 내용은 도메인 이름 등록 삭제 단원을 참조하십시오.

.wien(오스트리아 비엔나 시)

Return to index

등록 및 갱신을 위한 임대 기간

1~10년.

제한 사항

일반에 공개되어 있지만 다음과 같은 몇 가지 제한이 있습니다.

- 오스트리아 비엔나 시와 경제적, 문화적, 관광, 역사적, 사회적 또는 기타 관계가 있음을 입증해야 합니다.
- .wien 도메인 이름은 등록 기간이 끝날 때까지 반드시 위의 조건에 따라 사용해야 합니다.

개인 정보 보호

지원하지 않음.

무단 이전을 방지하기 위한 도메인 잠금

지원

다국어 도메인 이름

라틴어에 지원됩니다.

이전하는 데 필요한 권한 부여 코드

예

DNSSEC

도메인 등록에 대해 지원됩니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 단원을 참조하십시오.

도메인 갱신 및 복원 기한

- 갱신 가능: 만료 날짜까지
- Route 53를 사용한 늦은 갱신: 만료 후 44일까지
- Route 53에서 도메인 삭제: 만료 후 45일
- 레지스트리 복원: 만료 후 45일 ~ 75일 사이
- 레지스트리에서 도메인 삭제: 만료 후 80일

Amazon Route 53을 DNS 서비스로 구성

Amazon Route 53를 도메인의 DNS 서비스(예: example.com)로 사용할 수 있습니다. Route 53를 DNS 서비스로 사용할 경우, www.example.com과 같은 친숙한 도메인 이름을 컴퓨터 간 연결에 사용되는 192.0.2.1 등 숫자 IP 주소로 변환하여 인터넷 트래픽을 웹 사이트로 라우팅합니다. 사용자가 브라우저에 도메인 이름을 입력하거나 이메일을 보내면 DNS 쿼리가 Route 53로 전달되며 이에 따라 적절한 값으로 응답합니다. 예를 들어, Route 53가 example.com 웹 서버의 IP 주소를 사용하여 응답할 수 있습니다.

이 장에서는 인터넷 트래픽을 적절한 곳으로 라우팅하기 위해 Route 53를 구성하는 방법에 대해 설명합니다. 또한 현재 다른 DNS 서비스를 사용 중인 경우 DNS 서비스를 Route 53로 마이그레이션하는 방법, 그리고 새 도메인에 대한 DNS 서비스로 Route 53를 사용하는 방법을 설명합니다.

주제

Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정

Route 53로 하나 이상의 도메인 등록을 전송하는 경우, 그리고 현재 유료 DNS 서비스를 제공하지 않는 도메인 등록 기관을 사용하는 경우 도메인을 마이그레이션하기 전에 DNS 서비스를 마이그레이션해야 합니다. 그렇지 않은 경우 도메인을 전송할 때 등록 대행자가 DNS 서비스 제공을 중단하고, 연결된 웹 사이트 및 웹 애플리케이션을 인터넷에서 사용할 수 없게 됩니다. (또한, 현재 등록 기관에서 다른 DNS 서비스 공급자로 DNS 서비스를 마이그레이션할 수 있습니다. Route 53에 등록된 도메인에 대한 DNS 서비스 공급자로서 Route 53를 사용할 필요는 없습니다.)

이 프로세스는 현재 도메인을 사용 중인지에 따라 좌우됩니다.

- 도메인에 현재 트래픽이 발생 중인 경우(예: 사용자가 도메인 이름을 사용하여 웹 사이트를 검색하거나 웹 애플리케이션에 액세스하는 경우) Route 53를 사용 중인 도메인에 대한 DNS 서비스로 설정 섹션을 참조하세요.
- 도메인에 트래픽이 전혀 또는 거의 발생하지 않는 경우 Route 53를 비활성 도메인에 대한 DNS 서비스로 설정 섹션을 참조하십시오.

두 옵션 모두에 대해, 전체 마이그레이션 프로세스 중에 도메인이 사용 가능 상태로 남아야 합니다. 하지만 가능성은 낮더라도 문제가 있는 경우, 첫 번째 옵션을 통해 마이그레이션을 빠르게 롤백할 수 있습니다. 두 번째 옵션을 사용하면 도메인이 이틀 정도 사용 불가능한 상태가 될 수 있습니다.

에서 전문가와 연결하려면 영업 지원을 AWS참조하세요.

Route 53를 사용 중인 도메인에 대한 DNS 서비스로 설정

현재 트래픽이 발생 중인 도메인에 대해 DNS 서비스를 Amazon Route 53로 마이그레이션하려는 경우(예: 사용자가 도메인 이름을 사용하여 웹 사이트를 검색하거나 웹 애플리케이션에 액세스하는 경우) 이 섹션의 절차를 따르세요.

주제

- 1단계: 현재 DNS 서비스 공급자로부터 현재 DNS 구성 가져오기(선택 사항이지만 권장함)
- 2단계: 호스팅 영역 생성
- 3단계: 레코드 만들기
- 4단계: TTL 설정 낮춤
- 5단계: (DNSSEC를 구성한 경우) 상위 영역에서 DS 레코드 제거
- 6단계: 이전 TTL의 만료 대기
- 7단계: Route 53 이름 서버를 사용하도록 NS 레코드 업데이트
- 8단계: 도메인의 트래픽 모니터링
- 9단계: NS 레코드의 TTL을 더 높은 값으로 다시 변경
- 10단계: 도메인 등록을 Amazon Route 53로 이전
- 11단계: DNSSEC 서명 다시 사용(필요한 경우)

1단계: 현재 DNS 서비스 공급자로부터 현재 DNS 구성 가져오기(선택 사항이지만 권장함)

다른 공급자로부터 Route 53로 DNS 서비스를 마이그레이션할 때 Route 53에서 현재 DNS 구성을 재현합니다. Route 53에서 도메인과 이름이 같은 호스팅 영역을 생성하고 호스팅 영역에 레코드를 생성합니다. 각각의 레코드는 지정된 도메인 또는 하위 도메인 이름에 대해 트래픽을 라우팅할 방법을 나타냅니다. 예를 들어, 웹 브라우저에 도메인 이름을 입력하는 경우 그 트래픽이 데이터 센터의 웹 서버, Amazon EC2 인스턴스, CloudFront 배포 또는 다른 위치로 라우팅되도록 하고 싶습니까?

사용하는 프로세스는 현재 DNS 구성의 복잡성에 따라 다릅니다.

- 현재 DNS 구성이 간단한 경우 - 단지 몇몇 하위 도메인에 대해서만 인터넷 트래픽을 소수의 리소스(예: 웹 서버 또는 Amazon S3 버킷)로 라우팅하는 경우에는 Route 53 콘솔에서 몇 개의 레코드를 수동으로 생성할 수 있습니다.
- 현재 DNS 구성이 더 복잡하고 현재 구성을 재현하기만 하려는 경우 - 현재 DNS 서비스 공급자로부터 영역 파일을 받아 Route 53로 가져올 수 있는 경우 마이그레이션을 단순화할 수 있습니다. (모든 DNS 서비스 공급자가 영역 파일을 제공하는 것은 아닙니다.) 영역 파일을 가져올 때 Route 53는 호스팅 영역에 해당 레코드를 생성하여 기존 구성을 자동으로 재현합니다.

  현재 DNS 서비스 공급자에게 영역 파일 또는 레코드 목록을 얻는 방법에 대해 고객 지원을 요청해 보십시오. 필요한 영역 파일 형식에 대한 자세한 내용은 영역 파일을 가져와 레코드 생성 단원을 참조하십시오.
- 현재 DNS 구성이 더 복잡하고 Route 53 라우팅 기능에 관심이 있는 경우 - 다음 문서를 검토하여 다른 DNS 서비스 공급자는 제공하지 않는 Route 53 기능이 필요한지 확인하세요. 그러한 기능을 사용하고 싶으면 레코드를 수동으로 생성하거나 영역 파일을 가져온 다음에 레코드를 생성하거나 업데이트할 수 있습니다.
  - 별칭 또는 비 별칭 레코드 선택 에서는 CloudFront 배포 및 Amazon S3 버킷과 같은 일부 AWS 리소스로 트래픽을 무료로 라우팅하는 Route 53 별칭 레코드의 이점을 설명합니다. Amazon S3
  - 라우팅 정책 선택 섹션에서는 예를 들어 사용자의 위치를 기반으로 하는 라우팅, 사용자와 리소스 사이의 지연 시간을 기반으로 하는 라우팅, 리소스 상태가 양호한지 여부를 기반으로 하는 라우팅, 개발자 자신이 지정하는 가중치를 기반으로 하는 리소스에 대한 라우팅과 같은 Route 53 라우팅 옵션에 대해 설명합니다.

> **Note**
>
> 별칭 레코드와 복잡한 라우팅 정책을 이용하기 위해 영역 파일을 가져온 후 구성을 변경할 수도 있습니다.

영역 파일을 가져올 수 없거나 Route 53에 레코드를 수동으로 생성하려는 경우, 마이그레이션할 수 있는 레코드는 다음과 같은 레코드를 포함합니다.

- A(주소) 레코드 - 도메인 이름 또는 하위 도메인 이름을 해당 리소스의 IPv4 주소(예: 192.0.2.3)와 연결
- AAAA(주소) 레코드 - 도메인 이름 또는 하위 도메인 이름을 해당 리소스의 IPv6 주소(예: 2001:0db8:85a3:0000:0000:abcd:0001:2345)와 연결
- 메일 서버(MX) 레코드 - 트래픽을 메일 서버로 라우팅
- CNAME 레코드 - 한 도메인 이름(example.net)의 트래픽을 다른 도메인 이름(example.com)으로 다시 라우팅
- 기타 지원되는 DNS 레코드 유형에 대한 레코드 - 지원되는 레코드 유형의 목록은 지원되는 DNS 레코드 유형 섹션을 참조하세요.

2단계: 호스팅 영역 생성

도메인에 대한 트래픽을 라우팅할 방법을 Amazon Route 53에 알려주려면 도메인과 이름이 같은 호스팅 영역을 생성한 다음 호스팅 영역에 레코드를 생성합니다.

> **Important**
>
> 관리자 권한이 있는 도메인만 호스팅 영역을 생성할 수 있습니다. 일반적으로 도메인을 소유하고 있다는 뜻이지만 도메인 등록자용 애플리케이션을 개발하는 경우도 해당될 수 있습니다.

호스팅 영역을 생성하면 Route 53에서 해당 영역에 대한 NS(이름 서버) 레코드 및 SOA(권한 시작) 레코드를 자동으로 생성합니다. NS 레코드는 Route 53가 호스팅 영역과 연결된 4개의 이름 서버를 식별합니다. Route 53를 도메인을 위한 DNS 서비스로 설정하려면 도메인에서 이 4개의 이름 서버를 사용하도록 등록을 업데이트합니다.

> **Important**
>
> NS(이름 서버) 또는 SOA(권한 시작) 레코드를 추가로 생성하지 말고, 기존 NS 및 SOA 레코드를 삭제하지 마십시오.

호스팅 영역 생성

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. Route 53를 처음 사용하는 경우 DNS 관리(DNS management)에서 시작하기(Get started)를 선택한 다음 호스팅 영역 생성(Create hosted zones)을 선택합니다.

   Route 53를 이미 사용하고 있는 경우 탐색 창에서 호스팅 영역(Hosted zones)을 선택한 다음 호스팅 영역 생성(Create hosted zones)을 선택합니다.
3. 호스팅 영역 생성(Create hosted zones) 창에서 도메인 이름과 메모(선택 사항)를 입력합니다. 설정에 대한 자세한 내용을 보려면 오른쪽의 도움말 패널을 선택하여 엽니다.

   a-z, 0-9, -(하이픈) 이외의 문자를 지정하는 방법과 국제 도메인 이름을 지정하는 방법은 다음(DNS 도메인 이름 형식)을 참조하십시오.
4. 유형(Type)의 경우 퍼블릭 호스팅 영역(Public hosted zone)의 기본값을 허용합니다.
5. 호스팅 영역 생성(Create hosted zone)을 선택합니다.

3단계: 레코드 만들기

호스팅 영역을 생성한 후 도메인(example.com) 또는 하위 도메인(www.example.com)에 대한 트래픽을 라우팅하려는 위치를 정의하는 레코드를 호스팅 영역에 생성합니다. 예를 들어, example.com 및 www.example.com에 대한 트래픽을 Amazon EC2 인스턴스의 웹 서버로 라우팅하려는 경우 example.com과 www.example.com으로 명명된 레코드를 하나씩 만듭니다. 각 레코드에 EC2 인스턴스에 대한 IP 주소를 지정합니다.

다양한 방법으로 레코드를 생성할 수 있습니다.

영역 파일 가져오기

이 방법은 1단계: 현재 DNS 서비스 공급자로부터 현재 DNS 구성 가져오기(선택 사항이지만 권장함)에서 현재 DNS 서비스를 통해 영역 파일을 받는 경우 가장 쉬운 방법입니다. Amazon Route 53에서는 별칭 레코드를 생성하거나 가중치 기반 또는 장애 조치 같은 특별한 라우팅 유형을 사용할 시점을 예측할 수 없습니다. 따라서 영역 파일을 가져오는 경우 Route 53는 간단한 라우팅 정책을 사용하여 표준 DNS 레코드를 생성합니다.

자세한 내용은 영역 파일을 가져와 레코드 생성 단원을 참조하십시오.

콘솔에서 레코드 개별 생성

영역 파일을 가져오지 않고 단지 시작하기 위해 Simple의 라우팅 정책으로 몇 개의 레코드만 생성하려는 경우 Route 53 콘솔에서 레코드를 생성할 수 있습니다. 별칭 레코드와 그 밖의 레코드를 모두 생성할 수 있습니다.

자세한 정보는 다음의 주제를 참조하세요.

- 라우팅 정책 선택
- 별칭 또는 비 별칭 레코드 선택
- Amazon Route 53 콘솔을 사용하여 레코드 생성

프로그래밍 방식으로 레코드 생성

AWS SDKs, AWS CLI또는 중 하나를 사용하여 레코드를 생성할 수 있습니다 AWS Tools for Windows PowerShell. 자세한 내용은 AWS 설명서를 참조하세요.

SDK를 제공하지 AWS 않는 프로그래밍 언어를 사용하는 경우 Route 53 API를 사용할 수도 있습니다. 자세한 내용은 Amazon Route 53 API Reference를 확인하십시오.

4단계: TTL 설정 낮춤

레코드에 대한 TTL(Time To Live) 설정으로 DNS 해석기가 얼마나 오랫동안 레코드를 캐시하고 캐시한 정보를 사용하도록 할지 지정합니다. TTL이 만료되면 해석기가 도메인의 DNS 서비스 공급자에게 최신 정보를 획득하라는 다른 쿼리를 전송합니다.

NS 레코드에 대한 일반적인 TTL 설정은 172,800초 또는 2일입니다. NS 레코드는 Domain Name System(DNS)이 도메인에 대한 트래픽 라우팅 방법에 대한 정보를 가져오는 데 사용할 수 있는 이름 서버를 나열합니다. 현재 DNS 서비스 공급자와 Amazon Route 53를 둘 다 사용하여 NS 레코드에 대한 TTL을 낮추면 DNS를 Route 53로 마이그레이션하는 동안 문제를 발견하는 경우 도메인의 가동 중지 시간이 감소합니다. TTL을 낮추지 않을 경우 뭔가 문제가 있을 때 최장 2일간 인터넷에서 도메인에 접속할 수 없을 수 있습니다.

> **Note**
>
> 일부 전체 해석기는 상위 권한 서버에 있는 NS 레코드의 TTL을 캐시할 수 있으므로 상위 권한 DNS 서버에 등록된 NS 레코드의 TTL도 줄여야 합니다.

다음 NS 레코드에 대한 TTL을 변경하는 것이 좋습니다.

- 현재 DNS 서비스 공급자에 대해 호스팅 영역에 있는 NS 레코드. (현재 공급자는 다른 용어를 사용할 수 있습니다.)
- 2단계: 호스팅 영역 생성에서 생성한 호스팅 영역에 있는 NS 레코드.

현재 DNS 서비스 공급자와 함께 NS 레코드에 대한 TTL 설정을 낮추는 방법

- 도메인에 대해 제공되는 현재 DNS 서비스 공급자가 제공하는 방법을 사용하여 도메인에 대한 호스팅 영역에 있는 NS 레코드의 TTL을 변경합니다.

Route 53 호스팅 영역에 있는 NS 레코드에 대한 TTL 설정을 낮추려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 [Hosted Zones]를 선택합니다.
3. 호스팅 영역의 이름을 선택합니다.
4. NS 레코드를 선택한 다음 편집(Edit)을 선택합니다.
5. [TTL (Seconds)]의 값을 변경합니다. 60초에서 900초(15분) 사이의 값을 지정하는 것이 좋습니다.
6. Save changes(변경 사항 저장)를 선택합니다.

5단계: (DNSSEC를 구성한 경우) 상위 영역에서 DS 레코드 제거

도메인에 대해 DNSSEC를 구성한 경우 도메인을 Route 53로 마이그레이션하기 전에 상위 영역에서 DS(Delegation Signer) 레코드를 제거합니다.

상위 영역이 Route 53 또는 다른 등록 기관을 통해 호스팅되는 경우, 해당되는 등록 기관에 연락해 DS 레코드를 제거합니다.

현재 두 공급자에서 DNSSEC 서명을 사용할 수 없으므로 DS 또는 DNSSEC 서명을 제거하여 DNSSEC를 비활성화해야 합니다. 이는 일시적으로 DNS Resolver에 DNSSEC 검증을 사용하지 않도록 신호를 보냅니다. 11단계에서 Route 53로의 전환이 완료된 후에도 원하는 경우 DNSSEC 검증을 다시 사용할 수 있습니다.

자세한 내용은 도메인의 퍼블릭 키 삭제 단원을 참조하십시오.

6단계: 이전 TTL의 만료 대기

도메인이 사용 중인 경우(예: 사용자가 도메인 이름을 사용하여 웹 사이트를 검색하거나 웹 애플리케이션에 액세스하는 경우) DNS Resolver가 현재 DNS 서비스 공급자에 의해 제공된 이름 서버의 이름을 캐시했습니다. 몇 분 전에 그 정보를 캐시한 DNS 해석기는 거의 이틀 더 해당 정보를 저장할 것입니다.

Route 53로의 DNS 서비스 마이그레이션을 모두 한 번에 수행하려면 TTL을 낮춘 후 이틀간 기다리세요. 이틀 후에 TTL이 만료되고 해석기가 도메인에 대한 이름 서버를 요청한 후, 해석기는 현재 이름 서버를 얻고 4단계: TTL 설정 낮춤에서 지정한 새 TTL도 얻게 됩니다.

7단계: Route 53 이름 서버를 사용하도록 NS 레코드 업데이트

도메인의 DNS 서비스로 Amazon Route 53 사용을 시작하려면 상위 영역인 등록 기관에서 제공한 방법을 사용하여 NS 레코드의 현재 이름 서버를 Route 53 이름 서버로 바꿉니다.

> **Note**
>
> Route 53 이름 서버를 사용하도록 현재 DNS 서비스 공급자로 NS 레코드를 업데이트하면 도메인의 DNS 구성이 업데이트됩니다. (이런 업데이트는 마이그레이션하는 DNS 서비스로 설정을 업데이트한다는 점을 제외하면 도메인의 Route 53 호스팅 영역에 있는 NS 레코드를 업데이트하는 것과 비슷합니다.)

상위 영역인 등록 기관에서 NS 레코드를 업데이트하여 Route 53 이름 서버를 사용하려면

1. Route 53 콘솔에서 호스팅 영역에 대한 이름 서버를 가져옵니다.
   a. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
   b. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
   c. 호스팅 영역 페이지에서 해당 호스팅 영역의 이름을 선택합니다.
   d. 호스팅 영역 세부 정보 섹션에 있는 이름 서버에 대해 나열된 4개의 이름을 기록합니다.
2. 도메인에 대해 현재 DNS 서비스에서 제공되는 방법을 사용하여 호스팅 영역에 대한 NS 레코드를 업데이트하십시오. 도메인이 Route 53에 등록된 경우 도메인의 글루 레코드 및 이름 서버 추가 또는 변경 섹션을 참조하세요. 이 프로세스는 현재 DNS 서비스를 통해 이름 서버를 삭제할 수 있는지에 따라 달라집니다.

   이름 서버를 삭제할 수 있는 경우

- 호스팅 영역에 대한 NS 레코드에 현재 이름 서버의 이름을 기록해 두십시오. 현재 DNS 구성으로 되돌릴 필요가 있는 경우 이들 서버는 개발자가 지정하는 서버입니다.
- NS 레코드에서 현재 이름 서버를 삭제하십시오.
- NS 레코드를 이 절차의 1단계에서 확인한 Route 53 이름 서버 4개 모두의 이름으로 업데이트하세요.

> **Note**
>
> 마치면 NS 레코드에 있는 이름 서버만 4개의 Route 53 이름 서버가 됩니다.

이름 서버를 삭제할 수 없는 경우

- 사용자 지정 이름 서버를 사용하려면 이 옵션을 선택하십시오.
- 이 절차의 1단계에서 확인한 4개의 Route 53 이름 서버를 모두 추가하세요.

8단계: 도메인의 트래픽 모니터링

웹 사이트 또는 애플리케이션 트래픽과 이메일을 포함하여, 도메인의 트래픽을 모니터링합니다.

- 트래픽이 느리거나 중지된 경우 - 이전 DNS 서비스에서 제공하는 방법을 사용하여 도메인의 이름 서버를 이전 이름 서버로 다시 변경합니다. 이는 상위 영역인 등록 기관에서 NS 레코드를 업데이트하여 Route 53 이름 서버를 사용하려면의 2단계에서 기록해 둔 이름 서버입니다. 그런 다음 문제를 알아냅니다.
- 트래픽이 영향을 받지 않는 경우 - 9단계: NS 레코드의 TTL을 더 높은 값으로 다시 변경으로 계속 진행합니다.

9단계: NS 레코드의 TTL을 더 높은 값으로 다시 변경

도메인의 Amazon Route 53 호스팅 영역에서 NS 레코드의 TTL을 더 일반적인 값으로 변경합니다(예: 172,800초(2일)). 그러면 종종 그랬듯이 DNS 해석기가 도메인의 이름 서버에 대한 쿼리를 보내기를 기다릴 필요가 없으므로 사용자 입장에서는 지연 시간이 짧아지는 효과가 있습니다.

Route 53 호스팅 영역에 있는 NS 레코드의 TTL을 변경하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.

2. 탐색 창에서 [Hosted Zones]를 선택합니다.
3. 호스팅 영역의 이름을 선택합니다.
4. 호스팅 영역에 대한 레코드 목록에서 NS 레코드를 선택합니다.
5. 편집을 선택합니다.
6. [TTL (Seconds)]을 DNS 해석기가 도메인의 이름 서버의 이름을 캐시하도록 할 시간(초)으로 변경합니다. 172,800초의 값을 권장합니다.
7. Save changes(변경 사항 저장)를 선택합니다.

10단계: 도메인 등록을 Amazon Route 53로 이전

도메인의 DNS 서비스를 Amazon Route 53로 이전했으므로, 도메인의 등록을 Route 53에 선택 사항으로 이전할 수 있습니다. 자세한 내용은 도메인 등록을 Amazon Route 53으로 이전하기 단원을 참조하십시오.

11단계: DNSSEC 서명 다시 사용(필요한 경우)

도메인의 DNS 서비스를 Amazon Route 53로 이전했으므로 DNSSEC 서명을 다시 사용할 수 있습니다.

DNSSEC 서명 활성화 절차는 다음 두 단계로 구성됩니다.

- 1단계: Route 53에 DNSSEC 서명을 활성화하고 Route 53에 AWS Key Management Service ()의 고객 관리형 키를 기반으로 키 서명 키(KSK)를 생성하도록 요청합니다AWS KMS.
- 2단계: DNS 응답이 신뢰할 수 있는 암호화 서명으로 인증될 수 있도록 상위 영역에 DS(Delegation Signer) 레코드를 추가하여 호스팅 영역에 대한 신뢰 체인을 만듭니다.

  지침은 DNSSEC 서명 활성화 및 신뢰 체인 설정 단원을 참조하십시오.

Route 53를 비활성 도메인에 대한 DNS 서비스로 설정

트래픽이 전혀 발생하지 않는 도메인에 대해 DNS 서비스를 Amazon Route 53로 마이그레이션하려는 경우 이 섹션의 절차를 수행하세요.

주제

- 1단계: 현재 DNS 서비스 공급자(비활성 도메인)로부터 현재 DNS 구성 가져오기
- 2단계: 호스팅 영역 생성(비활성 도메인)

- 3단계: 레코드 생성(비활성 도메인)
- 4단계: 도메인 등록을 업데이트하여 Amazon Route 53 이름 서버 사용(비활성 도메인)

1단계: 현재 DNS 서비스 공급자(비활성 도메인)로부터 현재 DNS 구성 가져오기

다른 공급자로부터 Route 53로 DNS 서비스를 마이그레이션할 때 Route 53에서 현재 DNS 구성을 재현합니다. Route 53에서 도메인과 이름이 같은 호스팅 영역을 생성하고 호스팅 영역에 레코드를 생성합니다. 각각의 레코드는 지정된 도메인 또는 하위 도메인 이름에 대해 트래픽을 라우팅할 방법을 나타냅니다. 예를 들어, 웹 브라우저에 도메인 이름을 입력하는 경우 그 트래픽이 데이터 센터의 웹 서버, Amazon EC2 인스턴스, CloudFront 배포 또는 다른 위치로 라우팅되도록 하고 싶습니까?

사용하는 프로세스는 현재 DNS 구성의 복잡성에 따라 다릅니다.

- 현재 DNS 구성이 간단한 경우 - 단지 몇몇 하위 도메인에 대해서만 인터넷 트래픽을 소수의 리소스(예: 웹 서버 또는 Amazon S3 버킷)로 라우팅하는 경우에는 Route 53 콘솔에서 몇 개의 레코드를 수동으로 생성할 수 있습니다.
- 현재 DNS 구성이 더 복잡하고 현재 구성을 재현하기만 하려는 경우 - 현재 DNS 서비스 공급자로부터 영역 파일을 받아 Route 53로 가져올 수 있는 경우 마이그레이션을 단순화할 수 있습니다. (모든 DNS 서비스 공급자가 영역 파일을 제공하는 것은 아닙니다.) 영역 파일을 가져올 때 Route 53는 호스팅 영역에 해당 레코드를 생성하여 기존 구성을 자동으로 재현합니다.

  현재 DNS 서비스 공급자에게 영역 파일 또는 레코드 목록을 얻는 방법에 대해 고객 지원을 요청해 보십시오. 필요한 영역 파일 형식에 대한 자세한 내용은 영역 파일을 가져와 레코드 생성 단원을 참조하십시오.
- 현재 DNS 구성이 더 복잡하고 Route 53 라우팅 기능에 관심이 있는 경우 - 다음 문서를 검토하여 다른 DNS 서비스 공급자는 제공하지 않는 Route 53 기능이 필요한지 확인하세요. 그러한 기능을 사용하고 싶으면 레코드를 수동으로 생성하거나 영역 파일을 가져온 다음에 레코드를 생성하거나 업데이트할 수 있습니다.
  - 별칭 또는 비 별칭 레코드 선택 에서는 CloudFront 배포 및 Amazon S3 버킷과 같은 일부 AWS 리소스로 트래픽을 무료로 라우팅하는 Route 53 별칭 레코드의 이점을 설명합니다. Amazon S3
  - 라우팅 정책 선택 섹션에서는 예를 들어 사용자의 위치를 기반으로 하는 라우팅, 사용자와 리소스 사이의 지연 시간을 기반으로 하는 라우팅, 리소스 상태가 양호한지 여부를 기반으로 하는 라우팅, 개발자 자신이 지정하는 가중치를 기반으로 하는 리소스에 대한 라우팅과 같은 Route 53 라우팅 옵션에 대해 설명합니다.

> **Note**
>
> 별칭 레코드와 복잡한 라우팅 정책을 이용하기 위해 영역 파일을 가져온 후 구성을 변경할 수도 있습니다.

영역 파일을 가져올 수 없거나 Route 53에 레코드를 수동으로 생성하려는 경우, 마이그레이션할 수 있는 레코드는 다음과 같은 레코드를 포함합니다.

- A(주소) 레코드 - 도메인 이름 또는 하위 도메인 이름을 해당 리소스의 IPv4 주소(예: 192.0.2.3)와 연결
- AAAA(주소) 레코드 - 도메인 이름 또는 하위 도메인 이름을 해당 리소스의 IPv6 주소(예: 2001:0db8:85a3:0000:0000:abcd:0001:2345)와 연결
- 메일 서버(MX) 레코드 - 트래픽을 메일 서버로 라우팅
- CNAME 레코드 - 한 도메인 이름(example.net)의 트래픽을 다른 도메인 이름(example.com)으로 다시 라우팅
- 기타 지원되는 DNS 레코드 유형에 대한 레코드 - 지원되는 레코드 유형의 목록은 지원되는 DNS 레코드 유형 섹션을 참조하세요.

2단계: 호스팅 영역 생성(비활성 도메인)

도메인에 대한 트래픽을 라우팅할 방법을 Amazon Route 53에 알려주려면 도메인과 이름이 같은 호스팅 영역을 생성한 다음 호스팅 영역에 레코드를 생성합니다.

> **Important**
>
> 관리자 권한이 있는 도메인만 호스팅 영역을 생성할 수 있습니다. 일반적으로 도메인을 소유하고 있다는 뜻이지만 도메인 등록자용 애플리케이션을 개발하는 경우도 해당될 수 있습니다.

호스팅 영역을 생성하면 Route 53에서 해당 영역에 대한 NS(이름 서버) 레코드 및 SOA(권한 시작) 레코드를 자동으로 생성합니다. NS 레코드는 Route 53가 호스팅 영역과 연결된 4개의 이름 서버를 식별합니다. Route 53를 도메인을 위한 DNS 서비스로 설정하려면 도메인에서 이 4개의 이름 서버를 사용하도록 등록을 업데이트합니다.

> **Important**
>
> NS(이름 서버) 또는 SOA(권한 시작) 레코드를 추가로 생성하지 말고, 기존 NS 및 SOA 레코드를 삭제하지 마십시오.

호스팅 영역 생성

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. Route 53를 처음 사용하는 경우 시작하기(Get started)를 선택합니다.

   Route 53를 이미 사용하고 있는 경우 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
3. 호스팅 영역 생성(Create hosted zone)을 선택합니다.
4. 호스팅 영역 생성(Create hosted zones) 창에서 도메인 이름과 메모(선택 사항)를 입력합니다. 라벨 위에 마우스 포인트를 대면 도움말이 표시되어 설정에 관한 자세한 내용을 볼 수 있습니다.

   a-z, 0-9, -(하이픈) 이외의 문자를 지정하는 방법과 국제 도메인 이름을 지정하는 방법은 다음(DNS 도메인 이름 형식)을 참조하십시오.
5. 레코드 유형(Record type)의 경우 퍼블릭 호스팅 영역(Public hosted zone)의 기본값을 허용합니다.
6. 호스팅 영역 생성(Create hosted zone)을 선택합니다.

3단계: 레코드 생성(비활성 도메인)

호스팅 영역을 생성한 후 도메인(example.com) 또는 하위 도메인(www.example.com)에 대한 트래픽을 라우팅하려는 위치를 정의하는 레코드를 호스팅 영역에 생성합니다. 예를 들어, example.com 및 www.example.com에 대한 트래픽을 Amazon EC2 인스턴스의 웹 서버로 라우팅하려는 경우 example.com과 www.example.com으로 명명된 레코드를 하나씩 만듭니다. 각 레코드에 EC2 인스턴스에 대한 IP 주소를 지정합니다.

다양한 방법으로 레코드를 생성할 수 있습니다.

영역 파일 가져오기

이 방법은 1단계: 현재 DNS 서비스 공급자(비활성 도메인)로부터 현재 DNS 구성 가져오기에서 현재 DNS 서비스를 통해 영역 파일을 받는 경우 가장 쉬운 방법입니다. Amazon Route 53에서는 별칭 레코드를 생성하거나 가중치 기반 또는 장애 조치 같은 특별한 라우팅 유형을 사용할 시점을 예

측할 수 없습니다. 따라서 영역 파일을 가져오는 경우 Route 53는 간단한 라우팅 정책을 사용하여 표준 DNS 레코드를 생성합니다.

자세한 내용은 영역 파일을 가져와 레코드 생성 단원을 참조하십시오.

콘솔에서 레코드 개별 생성

영역 파일을 가져오지 않고 단지 시작하기 위해 Simple의 라우팅 정책으로 몇 개의 레코드만 생성하려는 경우 Route 53 콘솔에서 레코드를 생성할 수 있습니다. 별칭 레코드와 그 밖의 레코드를 모두 생성할 수 있습니다.

자세한 정보는 다음의 주제를 참조하세요.

- 라우팅 정책 선택
- 별칭 또는 비 별칭 레코드 선택
- Amazon Route 53 콘솔을 사용하여 레코드 생성

프로그래밍 방식으로 레코드 생성

AWS SDKs, AWS CLI또는 중 하나를 사용하여 레코드를 생성할 수 있습니다 AWS Tools for Windows PowerShell. 자세한 내용은 AWS 설명서를 참조하세요.

SDK를 제공하지 AWS 않는 프로그래밍 언어를 사용하는 경우 Route 53 API를 사용할 수도 있습니다. 자세한 내용은 Amazon Route 53 API Reference를 확인하십시오.

4단계: 도메인 등록을 업데이트하여 Amazon Route 53 이름 서버 사용(비활성 도메인)

도메인에 대한 레코드 생성을 완료하면 도메인에 대한 DNS 서비스를 Amazon Route 53로 변경할 수 있습니다. 도메인 등록자로 설정을 업데이트하려면 다음 절차를 수행하십시오.

도메인의 이름 서버 업데이트 방법

1. Route 53 콘솔에서 Route 53 호스팅 영역에 대한 이름 서버를 가져옵니다.

   a. https://console.aws.amazon.com/route53/에서 Route 53 콘솔을 엽니다.

   b. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.

   c. 호스팅 영역(Hosted zones) 페이지에서 호스팅 영역의 (이름 대신) 라디오 버튼을 선택한 다음 세부 정보 보기(View details)를 선택합니다.

   d. 호스팅 영역에 대한 세부 정보 페이지에서 호스팅 영역 세부 정보(Hosted zone details)를 선택합니다.

e. 이름 서버(Name servers)에 나열된 서버 4개의 이름을 기록합니다.

2. 도메인의 등록자가 제공한 방법을 사용하여, 이 절차의 2단계에서 받은 Route 53 이름 서버 4개를 사용하도록 도메인의 이름 서버를 변경합니다.

   도메인이 Route 53에 등록되어 있으면 도메인의 글루 레코드 및 이름 서버 추가 또는 변경 섹션을 참조하세요.

새 도메인에 대한 DNS 라우팅 구성

Route 53에서 구매한 새 도메인

Route 53에 도메인을 등록하면 Route 53가 자동으로 해당 도메인의 DNS 서비스가 됩니다. Route 53는 도메인과 동일한 이름의 호스팅 영역을 생성하고, 호스팅 영역에 4개의 이름 서버를 할당한 다음 도메인이 이 이름 서버를 사용하도록 업데이트합니다.

다른 등록 대행자에서 구매한 새 도메인

예를 들어 Route 53에서 최상위 도메인(TLD)을 제공하지 않기 때문에 다른 등록 대행자에서 도메인을 구매하는 경우에도 Route 53을 사용하여 DNS 라우팅을 관리할 수 있습니다. 자세한 내용은 Amazon Route 53에 등록할 수 있는 도메인 단원을 참조하십시오.

다음 지침에 따라 퍼블릭 호스팅 영역을 생성한 다음 등록 대행자로 생성된 이름 서버를 사용합니다.

비Route 53 도메인에 대한 호스팅 영역을 생성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역을 선택한 후 호스팅 영역 생성을 선택합니다.
3. 이름에 호스팅 영역을 만들려는 도메인의 이름을 입력합니다. 예를 들어 선택적 설명`example.com`인를 입력하고 퍼블릭 호스팅 영역을 선택한 다음 호스팅 영역 생성을 선택합니다.
4. 호스팅 영역을 생성한 후 생성된 네 개의 이름 서버(NS) 레코드를 기록해 둡니다. 각는 "ns-"로 시작합니다.

   도메인 등록 대행자에서 위에서 이름 서버를 입력하여 도메인 관리를 Route 53 호스팅 영역에 위임합니다.

DNS 트래픽 라우팅

Route 53가 도메인에 대한 인터넷 트래픽을 라우팅하는 방법을 지정하려면 호스팅 영역에 레코드를 생성합니다. 예를 들어, Amazon EC2 인스턴스에서 실행 중인 웹 서버로 example.com에 대한 요청을 라우팅하고자 하는 경우 example.com 호스팅 영역에서 레코드를 생성하고, EC2 인스턴스에 대한 탄력적 IP 주소를 지정합니다. 자세한 정보는 다음의 주제를 참조하세요.

- 호스팅 영역에서 레코드를 생성하는 방법에 대한 자세한 내용은 레코드 작업 섹션을 참조하세요.
- 트래픽을 선택한 AWS 리소스로 라우팅하는 방법에 대한 자세한 내용은 섹션을 참조하세요AWS 리소스로 인터넷 트래픽 라우팅.
- DNS 작동 방식에 대한 자세한 내용은 웹 사이트 또는 웹 애플리케이션으로 인터넷 트래픽을 라우팅하는 방식 단원을 참조하십시오.
- DNS 리포지토리를 확인하려면 섹션을 참조하세요Route 53에서 DNS 응답 확인.

해당 리소스로 트래픽 라우팅

예를 들어 사용자가 웹 브라우저에 해당 도메인 이름을 입력하여 웹 사이트 또는 웹 애플리케이션을 요청하면, Amazon Route 53에서 사용자를 해당 리소스(Amazon S3 버킷 또는 데이터 센터의 웹 서버 등)로 라우팅하도록 도와줍니다. 트래픽을 해당 리소스로 라우팅하도록 Route 53를 구성하려면 다음을 수행하세요.

1. 호스팅 영역 생성. 퍼블릭 호스팅 영역 또는 프라이빗 호스팅 영역을 만들 수 있습니다.

   퍼블릭 호스팅 영역

   예를 들어 인트라넷 트래픽을 해당 리소스로 라우팅하려면 퍼블릭 호스팅 영역을 만들어서, EC2 인스턴스에서 호스팅하는 회사 웹 사이트를 고객들이 볼 수 있게 합니다. 자세한 내용은 퍼블릭 호스팅 영역 작업 섹션을 참조하세요.

   프라이빗 호스팅 영역

   Amazon VPC 내에서 트래픽을 라우팅하려면 프라이빗 호스팅 영역을 만듭니다. 자세한 내용은 프라이빗 호스팅 영역 사용 섹션을 참조하세요.
2. 호스팅 영역에 레코드를 생성합니다. 레코드는 각 도메인 또는 하위 도메인 이름에 대해 트래픽을 라우팅할 위치를 정의합니다. 예를 들어 www.example.com에 대한 트래픽을 해당 데이터 센터의 웹 서버로 라우팅하려면, 일반적으로 example.com 호스팅 영역에 www.example.com 레코드를 생성합니다.

   자세한 정보는 다음의 주제를 참조하세요.

   - 레코드 작업

하위 도메인에 대한 트래픽 라우팅

트래픽을 하위 도메인의 리소스(예: acme.example.com 또는 zenith.example.com)로 라우팅하려는 경우 두 가지 방법이 있습니다.

도메인의 호스팅 영역에 레코드 생성

일반적으로, 하위 도메인에 대한 트래픽을 라우팅하려면 도메인과 이름이 동일한 호스팅 영역에 레코드를 생성합니다. 예를 들어 acme.example.com에 대한 인터넷 트래픽을 해당 데이터 센터의 웹 서버로 라우팅하려면, example.com 호스팅 영역에 acme.example.com이라는 레코드를 생성합니다. 자세한 내용은 레코드 작업 주제 및 해당 하위 주제를 참조하십시오.

하위 도메인에 대한 호스팅 영역을 만들고, 이 새로운 호스팅 영역에 레코드 생성

하위 도메인에 대한 호스팅 영역을 생성할 수도 있습니다. 별도의 호스팅 영역을 이용하여 하위 도메인의 인터넷 트래픽을 라우팅하는 것을 "호스팅 영역에 대한 하위 도메인의 책임 위임" 또는 "다른 이름 서버에 하위 도메인 위임"이라고 하거나 이와 비슷한 용어의 조합으로 부르기도 합니다. 여기서는 작동 방법에 대해 간략하게 살펴봅니다.

1. 트래픽을 라우팅할 하위 도메인과 이름이 같은 호스팅 영역(예: acme.example.com)을 생성합니다.
2. 이 새로운 호스팅 영역에, 해당 하위 도메인(acme.example.com) 및 그 하위 도메인(예: backend.acme.example.com)에 대한 트래픽을 라우팅하는 방법을 정의하는 레코드를 생성합니다.
3. 새 호스팅 영역을 생성할 때 Route 53가 새 호스팅 영역에 할당한 이름 서버를 가져옵니다.
4. 도메인(example.com)의 호스팅 영역에 새 NS 레코드를 생성하고 3단계에서 얻은 이름 서버 4개를 지정합니다.

별도 호스팅 영역을 사용하여 하위 도메인에 대한 트래픽을 라우팅할 때는 IAM 권한을 사용하여 하위 도메인의 호스팅 영역에 대한 액세스를 제한할 수 있습니다. 서로 다른 그룹에서 관리하는 하위 도메인이 여러 개 있는 경우, 각 하위 도메인에 대해 하나의 호스팅 영역을 만들면 도메인의 호스팅 영역에 있는 레코드를 액세스해야 하는 사용자의 수를 현저히 줄일 수 있습니다.

하위 도메인에 별도 호스팅 영역을 사용하면 그 도메인과 하위 도메인에 다른 DNS 서비스를 사용할 수 있습니다. 자세한 내용은 상위 도메인을 마이그레이션하지 않고 Amazon Route 53를 하위 도메인에 대한 DNS 서비스로 사용 섹션을 참조하세요.

이 구성은 각 DNS 해석의 첫 DNS 쿼리에 대해 다소 성능을 높이는 효과가 있습니다. 해석기는 루트 도메인의 호스팅 영역으로부터 정보를 받은 후, 하위 도메인의 호스팅 영역으로부터 정보를 받아야 합니다. 해석기는 하위 도메인에 대한 첫 번째 DNS 쿼리 후에 이 정보를 캐시에 저장하므로 TTL이 만료되어 다른 클라이언트가 해당 해석기로부터 하위 도메인을 요청할 때까지 정보를 다시 받을 필요가 없습니다. 자세한 내용은 Amazon Route 53 레코드를 생성 또는 편집할 때 지정하는 값 섹션의 TTL(초) 섹션을 참조하세요.

주제

- 다른 호스팅 영역을 만들어 하위 도메인에 대한 트래픽 라우팅
- 하위 도메인의 추가 수준에 대한 트래픽 라우팅

다른 호스팅 영역을 만들어 하위 도메인에 대한 트래픽 라우팅

하위 도메인에 대한 트래픽을 라우팅하는 한 가지 방법은 하위 도메인에 대한 호스팅 영역을 만든 후, 이 새로운 호스팅 영역에 하위 도메인에 대한 레코드를 생성하는 것입니다. (가장 일반적인 방법은 해당 도메인의 호스팅 영역에 하위 도메인에 대한 레코드를 생성하는 것입니다.)

> **Note**
>
> 여기에서 Route 53에서 하위 도메인 호스팅 영역을 생성하고 위임하는 프로세스를 설명하는 동안 다른 이름 서버에서 DNS 영역을 생성하고 마찬가지로 해당 이름 서버에 책임을 위임하는 이름 서버(NS) 레코드를 생성할 수도 있습니다.

다음은 이 프로세스를 요약한 것입니다.

1. 하위 도메인에 대한 호스팅 영역을 생성합니다. 자세한 내용은 하위 도메인에 대한 호스팅 영역 새로 만들기 섹션을 참조하세요.
2. 하위 도메인에 대한 호스팅 영역에 레코드를 추가합니다. 하위 도메인의 호스팅 영역에 속한 레코드가 도메인의 호스팅 영역에 하나라도 포함된 경우, 하위 도메인의 호스팅 영역에 그 레코드를 복제합니다. 자세한 내용은 하위 도메인에 대한 호스팅 영역에 레코드 생성 섹션을 참조하세요.
3. 해당 도메인의 호스팅 영역에 하위 도메인에 대한 NS 레코드를 생성하면, 하위 도메인에 대한 책임을 새로운 호스팅 영역의 이름 서버에 위임합니다. 하위 도메인의 호스팅 영역에 속한 레코드가 도메인의 호스팅 영역에 하나라도 포함된 경우, 도메인의 호스팅 영역에서 그 레코드를 삭제합니다. (2단계에서 하위 도메인의 호스팅 영역에 사본을 생성했습니다.) 자세한 내용은 도메인의 호스팅 영역 업데이트 섹션을 참조하세요.

하위 도메인에 대한 호스팅 영역 새로 만들기

Route 53 콘솔을 사용하여 하위 도메인에 대한 호스팅 영역을 만들려면 다음 절차를 수행합니다.

하위 도메인에 대한 호스팅 영역을 만들려면(콘솔)

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. Route 53를 처음 사용하는 경우 시작하기(Get started)를 선택합니다.

   Route 53를 이미 사용하고 있는 경우 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
3. 호스팅 영역 생성(Create hosted zone)을 선택합니다.
4. 오른쪽 창에 하위 도메인 이름(예: acme.example.com)을 입력합니다. 선택적으로 설명을 입력할 수도 있습니다.

   a-z, 0-9, -(하이픈) 이외의 문자를 지정하는 방법과 국제 도메인 이름을 지정하는 방법은 다음(DNS 도메인 이름 형식)을 참조하십시오.
5. 유형(Type)의 경우 퍼블릭 호스팅 영역(Public hosted zone)의 기본값을 허용합니다.
6. 오른쪽 창 하단에서 호스팅 영역 생성(Create hosted zone)을 선택합니다.

하위 도메인에 대한 호스팅 영역에 레코드 생성

Route 53가 하위 도메인(acme.example.com)과 그 하위 도메인(backend.acme.example.com)에 대한 트래픽을 라우팅하는 방법을 정의하려면 하위 도메인의 호스팅 영역에 레코드를 생성합니다.

하위 도메인의 호스팅 영역에 레코드를 생성하는 내용에 대해서는 다음을 참고하십시오.

- 하위 도메인의 호스팅 영역에 NS(이름 서버) 또는 SOA(권한 시작) 레코드를 추가로 생성하지 말고, 기존 NS 및 SOA 레코드를 삭제하지 마십시오.
- 하위 도메인의 모든 레코드를 하위 도메인의 호스팅 영역에 생성합니다. 예를 들어, example.com 과 acme.example.com 도메인의 호스팅 영역이 있다면 acme.example.com 하위 도메인의 모든 레코드를 acme.example.com 호스팅 영역에 생성합니다. 여기에는 backend.acme.example.com 및 beta.backend.acme.example.com 같은 레코드가 포함됩니다.
- 하위 도메인(acme.example.com)의 호스팅 영역에 속한 레코드가 도메인(example.com)의 호스팅 영역에 포함된 경우, 하위 도메인의 호스팅 영역에 그 레코드를 복제합니다. 프로세스의 마지막 단계에서 중복 레코드를 도메인의 호스팅 영역에서 나중에 삭제합니다.

> **Important**
>
> 도메인의 호스팅 영역과 하위 도메인의 호스팅 영역 양쪽에 하위 도메인의 레코드가 있는 경우 DNS 동작에 일관성이 없어집니다. 동작을 좌우하는 것은 DNS 해석기가 캐시한 이름 서버, 도메인 호스팅 영역(example.com)에 대한 이름 서버, 하위 도메인 호스팅 영역(acme.example.com)에 대한 이름 서버입니다. 레코드가 존재하되 DNS 해석기가 쿼리를 제출하는 호스팅 영역에 있는 것이 아닌 경우, Route 53은 NXDOMAIN(존재하지 않는 도메인)을 반환합니다.

자세한 내용은 레코드 작업 섹션을 참조하세요.

도메인의 호스팅 영역 업데이트

호스팅 영역을 생성하면 Route 53에서 호스팅 영역에 4개의 이름 서버를 자동으로 할당합니다. 호스팅 영역의 NS 레코드는 도메인 또는 하위 도메인에 대한 DNS 쿼리에 응답하는 이름 서버를 식별합니다. 하위 도메인의 호스팅 영역에 있는 레코드를 사용하여 인터넷 트래픽 라우팅을 시작하려면, 도메인(example.com)의 호스팅 영역에 NS 레코드를 새로 생성하고, 이 레코드에 하위 도메인(acme.example.com) 이름을 지정합니다. NS 레코드 값으로는 하위 도메인의 호스팅 영역에서 이름 서버의 이름을 지정합니다.

다음은 Route 53가 하위 도메인(acme.example.com) 또는 그 하위 도메인 중 하나에 대해 DNS Resolver로부터 DNS 쿼리를 수신하면 어떻게 되는지 보여줍니다.

1. Route 53가 도메인(example.com)에 대한 호스팅 영역에서 하위 도메인(acme.example.com)에 대한 NS 레코드를 찾습니다.
2. Route 53는 example.com 도메인의 호스팅 영역에 있는 acme.example.com NS 레코드에서 이름 서버를 가져와 이러한 이름 서버를 DNS Resolver에 반환합니다.
3. 해석기가 acme.example.com에 대한 쿼리를 acme.example.com 호스팅 영역에 대한 이름 서버로 다시 제출합니다.
4. Route 53이 acme.example.com 호스팅 영역에 있는 레코드를 사용하여 쿼리에 응답합니다.

Route 53가 하위 도메인의 호스팅 영역을 사용하여 하위 도메인에 대한 트래픽을 라우팅하도록 구성하고, 도메인의 호스팅 영역에서 중복 레코드를 모두 삭제하려면 다음 절차를 수행합니다.

하위 도메인(콘솔)의 호스팅 영역을 사용하도록 Route 53를 구성하려면

1. Route 53 콘솔에서 하위 도메인에 대한 호스팅 영역의 이름 서버를 가져옵니다.
   a. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
   b. 호스팅 영역(Hosted zones) 페이지에서 하위 도메인의 호스팅 영역의 이름을 선택합니다.
   c. 오른쪽 창에서 호스팅 영역 세부 사항(Hosted zones details) 섹션의 이름 서버(Name servers)에 나열된 4개 서버의 이름을 복사합니다.
2. 하위 도메인이 아니라 도메인(example.com)의 호스팅 영역 이름을 선택합니다.
3. 레코드 세트 생성을 선택합니다.
4. 단순 라우팅(Simple routing)을 선택하고 다음(Next)을 선택합니다.
5. Define simple record(단순 레코드 정의)를 선택합니다.
6. 다음 값을 지정하세요.

   명칭

   하위 도메인 이름을 입력합니다.

   값/트래픽 라우팅 대상

   IP 주소 또는 레코드 유형에 따라 다른 값(IP address or another value depending on the record type)을 선택하고 1단계에서 복사한 이름 서버의 이름을 붙여넣습니다.

   레코드 유형

   NS - 호스팅 영역의 이름 서버(NS – Name servers for a hosted zone)를 선택합니다.

   TTL(초)

   NS 레코드에 대한 보다 일반적인 값(예: 172800초)으로 변경합니다.
7. 단순 레코드 정의(Define simple record)를 선택하고 레코드 생성(Create records)을 선택합니다.
8. 하위 도메인의 호스팅 영역에 생성한 레코드가 도메인의 호스팅 영역에 하나라도 포함된 경우, 도메인의 호스팅 영역에서 그 레코드를 삭제합니다. 자세한 내용은 레코드 삭제 섹션을 참조하세요.

   작업이 끝나면 하위 도메인의 모든 레코드가 하위 도메인의 호스팅 영역에 위치하게 됩니다.

하위 도메인의 추가 수준에 대한 트래픽 라우팅

하위 도메인의 하위 도메인(예: backend.acme.example.com)에 대한 트래픽은 하위 도메인(예: acme.example.com)에 대한 트래픽을 라우팅하는 것과 동일한 방법으로 라우팅합니다. 도메인의 호스

팅 영역에 레코드를 생성하거나, 하위 수준 하위 도메인의 호스팅 영역을 생성한 후 이 새로운 호스팅 영역에 레코드를 생성합니다.

낮은 수준의 하위 도메인을 위한 호스팅 영역을 별개로 생성하고자 한다면, 도메인 이름에서 한 수준 옆에 있는 하위 도메인의 호스팅 영역에 하위 수준 하위 도메인에 대한 NS 레코드를 생성합니다. 트래픽이 정확하게 리소스로 라우팅이 되도록 도와줍니다. 예를 들어 다음 하위 도메인에 대한 트래픽을 라우팅한다고 가정하겠습니다.

- subdomain1.example.com
- subdomain2.subdomain1.example.com

다른 호스팅 영역을 사용하여 subdomain2.subdomain1.example.com에 대한 트래픽을 라우팅하려면 다음과 같이 합니다.

1. subdomain2.subdomain1.example.com이라는 호스팅 영역을 만듭니다.
2. subdomain2.subdomain1.example.com hosted 호스팅 영역에 레코드를 생성합니다. 자세한 내용은 하위 도메인에 대한 호스팅 영역에 레코드 생성 섹션을 참조하세요.
3. subdomain2.subdomain1.example.com 호스팅 영역의 이름 서버 이름을 복사합니다.
4. subdomain1.example.com 호스팅 영역에 subdomain2.subdomain1.example.com이라는 NS 레코드를 생성하고, subdomain2.subdomain1.example.com 호스팅 영역의 이름 서버 이름을 붙여 넣습니다.

   또한 subdomain1.example.com에서 중복 레코드를 모두 삭제합니다. 자세한 내용은 도메인의 호스팅 영역 업데이트 섹션을 참조하세요.

   이 NS 레코드를 생성하면 Route 53가 subdomain2.subdomain1.example.com 호스팅 영역을 사용하여 subdomain2.subdomain1.example.com 하위 도메인에 대한 트래픽을 라우팅합니다.

호스팅 영역 작업

호스팅 영역이란 레코드의 컨테이너이며, 레코드에는 특정 도메인(예: example.com)과 그 하위 도메인(acme.example.com, zenith.example.com)의 트래픽을 라우팅하는 방식에 대한 정보가 포함됩니다. 호스팅 영역과 해당 도메인의 이름은 동일합니다. 호스팅 영역의 유형은 두 가지입니다.

- 퍼블릭 호스팅 영역은 인터넷에서 트래픽을 라우팅하고자 하는 방법을 지정하는 레코드를 포함합니다. 자세한 내용은 퍼블릭 호스팅 영역 작업 섹션을 참조하세요.

- 프라이빗 호스팅 영역은 Amazon VPC에서 트래픽을 라우팅하고자 하는 방법을 지정하는 레코드를 포함합니다. 자세한 내용은 프라이빗 호스팅 영역 사용 단원을 참조하십시오.

퍼블릭 호스팅 영역 작업

퍼블릭 호스팅 영역이란 특정 도메인(예: example.com)과 그 하위 도메인(acme.example.com, zenith.example.com)의 트래픽을 인터넷에서 라우팅하는 방식에 대한 정보를 담고 있는 컨테이너입니다. 다음 두 가지 방법 중 하나로 퍼블릭 호스팅 영역을 얻습니다.

- Route 53에 도메인을 등록하면 호스팅 영역이 자동으로 생성됩니다.
- 기존 도메인에 대한 DNS 서비스를 Route 53로 전송하는 경우 도메인에 대한 호스팅 영역 생성부터 시작합니다. 자세한 내용은 Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정 섹션을 참조하세요.

두 가지 경우 모두 호스팅 영역에 레코드를 생성하여 도메인 및 하위 도메인에 대한 트래픽의 라우팅 방법을 지정합니다. 예를 들어, 레코드를 생성하여 www.example.com에 대한 트래픽을 CloudFront 배포 또는 데이터 센터의 웹 서버로 라우팅할 수 있습니다. 레코드에 대한 자세한 내용은 레코드 작업 단원을 참조하십시오.

이 주제에서는 Amazon Route 53 콘솔을 사용하여 퍼블릭 호스팅 영역을 생성, 나열 및 삭제하는 방법을 살펴봅니다.

> **Note**
>
> Route 53 프라이빗 호스팅 영역을 사용하여 Amazon VPC 서비스에서 생성한 하나 이상의 VPC 내의 트래픽을 라우팅할 수도 있습니다. 자세한 내용은 프라이빗 호스팅 영역 사용 섹션을 참조하세요.

주제

- 퍼블릭 호스팅 영역 삭제
- Route 53에서 DNS 응답 확인
- 화이트 레이블 이름 서버 구성
- Amazon Route 53에서 퍼블릭 호스팅 영역에 대해 생성하는 NS 및 SOA 레코드

퍼블릭 호스팅 영역 작업 시 고려 사항

퍼블릭 호스팅 영역 작업 시 다음을 고려하십시오.

NS 및 SOA 레코드

호스팅 영역을 생성하면 Amazon Route 53에서 해당 영역에 대한 NS(이름 서버) 레코드 및 SOA(권한 시작) 레코드를 자동으로 생성합니다. NS 레코드는 DNS 쿼리가 Route 53 이름 서버에 라우팅되도록 등록 기관 또는 DNS 서비스에 부여하는 4개의 이름 서버를 식별합니다. NS 및 SOA 레코드에 관한 자세한 내용은 Amazon Route 53에서 퍼블릭 호스팅 영역에 대해 생성하는 NS 및 SOA 레코드 섹션을 참조하세요.

동일한 이름을 보유한 여러 개의 호스팅 영역

이름이 동일한 2개 이상의 호스팅 영역을 생성하고 각 호스팅 영역에 서로 다른 레코드를 추가할 수 있습니다. Route 53는 호스팅 영역마다 4개의 이름 서버를 할당하고 해당 이름 서버는 서로 각각 다릅니다. 등록 기관의 이름 서버 레코드를 업데이트하는 경우에는 올바른 호스팅 영역, 즉 도메인에 대한 쿼리에 응답할 때 Route 53에서 사용하기를 원하는 레코드를 포함하는 호스팅 영역에 대한 Route 53 이름 서버를 주의하여 사용하세요. Route 53는 이름이 같은 다른 호스팅 영역의 레코드에 대한 값을 반환하지 않습니다.

재사용 가능한 위임 세트

기본적으로 Route 53는 생성하는 각 호스팅 영역에 고유한 4개의 이름 서버 세트(합쳐서 위임 세트라고 함)를 할당합니다. 다수의 호스팅 영역을 생성하려는 경우, 재사용 가능한 위임 세트를 프로그래밍 방식으로 생성할 수 있습니다. (재사용 가능한 위임 세트는 Route 53 콘솔에서 이용할 수 없습니다.) 그런 다음 프로그래밍 방식으로 호스팅 영역을 생성하고 각 호스팅 영역에 재사용 가능한 동일한 위임 세트, 즉 동일한 4개의 이름 서버를 할당할 수 있습니다.

재사용 가능한 위임 세트는 Route 53로의 DNS 서비스 마이그레이션을 간소화합니다. Route 53를 DNS 서비스로 사용하기를 원하는 모든 도메인에 대해 동일한 4개의 이름 서버를 사용하도록 도메인 이름 등록자에게 지시할 수 있기 때문입니다. 자세한 내용은 Amazon Route 53 API 참조의 CreateReusableDelegationSet를 참조하세요.

퍼블릭 호스팅 영역 생성

퍼블릭 호스팅 영역이란 특정 도메인(예: example.com)과 그 하위 도메인(acme.example.com, zenith.example.com)의 트래픽을 인터넷에서 라우팅하는 방식에 대한 정보를 담고 있는 컨테이너입니다. 호스팅 영역을 생성한 이후 레코드를 생성하여 도메인 및 하위 도메인에 대한 트래픽의 라우팅 방법을 지정합니다.

> **Important**
>
> 관리자 권한이 있는 도메인만 호스팅 영역을 생성할 수 있습니다. 일반적으로 도메인을 소유하고 있다는 뜻이지만 도메인 등록자용 애플리케이션을 개발하는 경우도 해당될 수 있습니다.

Route 53 콘솔을 사용하여 퍼블릭 호스팅 영역을 생성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. Route 53를 처음 사용하는 경우 DNS 관리(DNS management)에서 시작하기(Get started)를 선택합니다.

   Route 53를 이미 사용하고 있는 경우 탐색 창에서 Hosted Zones(호스팅 영역)를 선택합니다.
3. 호스팅 영역 생성(Create hosted zone)을 선택합니다.
4. Create Hosted Zone(호스팅 영역 생성) 창에서 트래픽을 라우팅하고자 하는 도메인의 이름을 입력합니다. 선택적으로 설명을 입력할 수도 있습니다.

   a-z, 0-9, -(하이픈) 이외의 문자를 지정하는 방법과 국제 도메인 이름을 지정하는 방법은 다음(DNS 도메인 이름 형식)을 참조하십시오.
5. [Type]에는 [Public Hosted Zone]의 기본값을 수락합니다.
6. 생성(Create)을 선택합니다.
7. 도메인과 하위 도메인의 트래픽을 라우팅할 방법을 지정하는 레코드를 생성합니다. 자세한 내용은 레코드 작업 섹션을 참조하세요.
8. 새로운 호스팅 영역을 레코드를 사용하여 도메인에 대한 트래픽을 라우팅하려면 해당 항목을 참조하십시오.

   - 다른 도메인 등록 기관에 등록된 도메인에 대해 Route 53를 DNS 서비스로 사용하려면 Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정 섹션을 참조하세요.

- 도메인이 Route 53에 등록되어 있으면 도메인의 글루 레코드 및 이름 서버 추가 또는 변경 섹션을 참조하세요.

퍼블릭 호스팅 영역에 대한 이름 서버 가져오기

도메인 등록을 위한 DNS 서비스를 변경하려는 경우 퍼블릭 호스팅 영역의 이름 서버를 가져옵니다. DNS 서비스를 변경하는 방법에 대한 자세한 내용은 Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정 단원을 참조하십시오.

> **Note**
>
> 일부 등록자는 IP 주소를 사용하는 이름 서버만 지정하도록 허용하며, 정규화된 도메인 이름을 지정하는 것은 허용하지 않습니다. 등록자가 IP 주소를 사용하도록 요구하는 경우, dig 유틸리티(Mac, Unix 또는 Linux의 경우) 또는 nslookup 유틸리티(Windows의 경우)를 사용하여 이름 서버의 IP 주소를 가져올 수 있습니다. Amazon은 이름 서버의 IP 주소를 거의 변경하지 않으며, IP 주소를 변경해야 하는 경우 미리 알려 드립니다.

Route 53 콘솔을 사용하여 호스팅 영역에 대한 이름 서버를 가져오려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted Zones)을 클릭합니다.
3. 호스팅 영역(Hosted zones) 페이지에서 호스팅 영역의 (이름 대신) 라디오 버튼을 선택한 다음 세부 정보 보기(View details)를 선택합니다.
4. 호스팅 영역에 대한 세부 정보 페이지에서 호스팅 영역 세부 정보(Hosted zone details)를 선택합니다.
5. 이름 서버(Name servers)에 나열된 서버 4개의 이름을 기록합니다.

퍼블릭 호스팅 영역 나열

Amazon Route 53 콘솔을 사용하여 현재 AWS 계정으로 생성한 모든 호스팅 영역을 나열할 수 있습니다. Route 53 API를 사용하여 호스팅 영역을 나열하는 방법에 대한 자세한 내용은 Amazon Route 53 API 참조의 ListHostedZones를 참조하세요.

Route 53 콘솔을 사용하여 AWS 계정과 연결된 퍼블릭 호스팅 영역을 나열하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다. 페이지에는 현재 로그인한 AWS 계정과 연결된 호스팅 영역 목록이 표시됩니다.
3. 호스팅 영역을 필터링하려면 테이블 상단에 있는 검색 창을 사용합니다.

   일부 동작은 호스팅 영역에 최대 2,000개 또는 2,000개 이상의 레코드를 포함하는지 여부에 따라 다릅니다.

   호스팅 영역이 최대 2,000개인 경우

   - 특정 값을 보유한 레코드를 표시하려면 검색 창을 클릭하고 드롭다운 목록에서 속성을 선택한 다음 값을 입력합니다. 검색 창에 직접 값을 입력하고 Enter 키를 누를 수도 있습니다. 예를 들어, 이름이 **abc**로 시작하는 호스팅 영역을 표시하려면 검색 창에 해당 값을 입력하고 Enter 키를 누릅니다.
   - 호스팅 영역 유형이 동일한 호스팅 영역만 표시하려면 드롭다운 목록에서 해당 유형을 선택하고 그 유형을 입력합니다.

   호스팅 영역이 2,000개 이상인 경우

   - 정확한 도메인 이름, 모든 속성 및 유형을 기반으로 속성을 검색할 수 있습니다.
   - 정확한 도메인 이름을 사용하여 검색하면 더 빠른 검색 결과를 얻을 수 있습니다.

퍼블릭 호스팅 영역에서 DNS 쿼리 지표 보기

지정된 퍼블릭 호스팅 영역이나 퍼블릭 호스팅 영역의 조합에서 Route 53가 응답하고 있는 총 DNS 쿼리의 수를 볼 수 있습니다. 지표가 CloudWatch에 표시되면 그래프를 보고 확인하고 싶은 기간을 선택한 다음, 기타 다양한 방법으로 지표를 사용자 정의할 수 있습니다. 또한 지정된 기간의 DNS 쿼리 수가 지정된 수준을 넘거나 수준에 미달될 때 사용자에게 알리기 위한 경보를 생성하고 알림을 구성할 수 있습니다.

> **Note**
>
> Route 53는 모든 퍼블릭 호스팅 영역에서 CloudWatch에 DNS 쿼리 수를 자동으로 전송하기 때문에 쿼리 지표를 보기 위해 아무것도 사전에 구성할 필요가 없습니다. DNS 쿼리 지표에 대한 요금은 없습니다.

어떤 DNS 쿼리가 계산됩니까?

지표에는 DNS 해석기가 Route 53로 전달하는 쿼리만 포함되어 있습니다. DNS 해석기가 쿼리(예: example.com의 로드 밸런서에 대한 IP 주소)에 대한 응답을 이미 캐시한 경우 해석기는 해당 레코드에 대한 TTL이 만료될 때까지 쿼리를 Route 53로 전달하지 않고 캐시된 응답을 계속 반환합니다.

도메인 이름(example.com) 또는 하위 도메인 이름(www.example.com)에 대해 제출된 DNS 쿼리 수, 사용자가 사용하고 있는 해석기 및 레코드에 대한 TTL에 따라 DNS 쿼리 지표에는 DNS 해석기에 제출된 수 천 개의 쿼리 중 한 개의 쿼리에 대한 정보만 포함될 수 있습니다. DNS 작업 방법에 대한 자세한 내용은 Amazon Route 53가 도메인의 트래픽을 라우팅하는 방법 섹션을 참조하세요.

호스팅 영역에 대한 쿼리 지표가 언제 CloudWatch에 나타나기 시작합니까?

호스팅 영역을 생성한 후 CloudWatch에 호스팅 영역이 나타나기까지는 최대 몇 시간이 걸립니다. 또한 표시할 데이터가 있도록 호스팅 영역의 레코드에 대한 DNS 쿼리를 제출해야 합니다.

지표는 미국 동부(버지니아 북부)에서만 사용 가능

콘솔의 지표를 가져오려면 해당 리전을 미국 동부(버지니아 북부)로 선택해야 합니다. AWS CLI를 사용하여 지표를 가져오려면 AWS 리전을 지정하지 않은 상태로 두거나 리전`us-east-1`으로를 지정해야 합니다. 다른 리전을 선택한 경우에는 Route 53 지표를 사용할 수 없습니다.

DNS 쿼리의 CloudWatch 지표 및 측정기준

DNS 쿼리의 CloudWatch 지표 및 측정기준에 대한 자세한 내용은 Amazon CloudWatch를 사용하여 호스팅 영역 모니터링 섹션을 참조하세요. CloudWatch 지표에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 Amazon CloudWatch 지표 사용을 참조하세요.

DNS 쿼리에 대한 세부 데이터 얻기

다음 값을 포함하여 Route 53가 응답하는 각 DNS 쿼리에 대한 세부 정보를 가져오려면 다음과 같이 쿼리 로깅을 구성할 수 있습니다.

- 요청된 도메인 또는 하위 도메인
- 요청의 날짜 및 시간
- DNS 레코드 유형(예: A 또는 AAAA)

- DNS 쿼리에 응답한 Route 53 엣지 로케이션
- DNS 응답 코드(예: `NoError` 또는 `ServFail`)

자세한 내용은 퍼블릭 DNS 쿼리 로깅 섹션을 참조하세요.

DNS 쿼리 지표를 가져오는 방법

사용자가 호스팅 영역을 생성하는 즉시 Amazon Route 53는 지표 및 측정기준을 1분마다 CloudWatch에 전송하기 시작합니다. 다음 절차를 사용하여 CloudWatch 콘솔에서 지표를 보거나 AWS Command Line Interface ()를 사용하여 지표를 볼 수 있습니다AWS CLI.

주제

- CloudWatch 콘솔에서 퍼블릭 호스팅 영역의 DNS 쿼리 지표 확인
- 를 사용하여 DNS 쿼리 지표 가져오기 AWS CLI

CloudWatch 콘솔에서 퍼블릭 호스팅 영역의 DNS 쿼리 지표 확인

CloudWatch 콘솔에서 퍼블릭 호스팅 영역의 DNS 쿼리 지표를 확인하려면 다음 절차를 수행합니다.

CloudWatch 콘솔에서 퍼블릭 호스팅 영역의 DNS 쿼리 지표를 확인하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudwatch/ CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 지표(Metrics)를 선택합니다.
3. 콘솔의 오른쪽 상단 모서리에 있는 AWS 리전 목록에서 미국 동부(버지니아 북부)를 선택합니다. 다른 AWS 리전을 선택하면 Route 53 지표를 사용할 수 없습니다.
4. 모든 지표(All metrics) 탭에서 [Route 53]을 선택합니다.
5. Hosted Zone Metrics(호스팅 영역 지표)를 선택합니다.
6. 지표 이름이 DNSQueries인 하나 이상의 호스팅 영역에 대해 확인란을 클릭합니다.
7. 그래프로 표시된 지표 탭에서 원하는 형식으로 지표를 볼 수 있도록 해당 값을 변경합니다.

   통계에서 합계 또는 SampleCount를 선택합니다. 두 통계 모두 동일한 값을 표시합니다.

를 사용하여 DNS 쿼리 지표 가져오기 AWS CLI

를 사용하여 DNS 쿼리 지표를 가져오려면 get-metric-data 명령을 AWS CLI사용합니다. 다음 사항에 유의하세요.

- 별도의 JSON 파일에서 명령의 대부분 값을 지정합니다. 자세한 내용은 get-metric-data를 참조하십시오.
- 명령은 JSON 파일에서 Period에 대해 지정한 시간 간격마다 하나의 값을 반환합니다. Period는 초 단위이므로 5분의 기간을 지정하고 Period에 대해 60을 지정하면 5개의 값을 얻게 됩니다. 5분의 기간을 지정하고 Period에 대해 300를 지정하면 한 개의 값을 얻게 됩니다.
- JSON 파일에서 Id에 대해 어떤 값이든 지정할 수 있습니다.
- AWS 리전을 지정하지 않은 상태로 두거나 리전us-east-1으로를 지정합니다. 다른 리전을 선택한 경우에는 Route 53 지표를 사용할 수 없습니다. 자세한 내용은 AWS Command Line Interface 사용 설명서의 AWS CLI 구성을 참조하세요.

다음은 2019년 5월 1일 4:01에서 4:07 사이의 5분 동안 DNS 쿼리 지표를 가져오는 데 사용하는 AWS CLI 명령입니다. metric-data-queries 파라미터는 이러한 명령을 따르는 샘플 JSON 파일을 참조합니다.

```
aws cloudwatch get-metric-data --metric-data-queries file://./metric.json --start-time
 2019-05-01T04:01:00Z --end-time 2019-05-01T04:07:00Z
```

아래에 JSON 파일 샘플이 나와 있습니다.

```
[
    {
        "Id": "my_dns_queries_id",
        "MetricStat": {
            "Metric": {
                "Namespace": "AWS/Route53",
                "MetricName": "DNSQueries",
                "Dimensions": [
                    {
                        "Name": "HostedZoneId",
                        "Value": "Z1D633PJN98FT9"
                    }
                ]
            },
            "Period": 60,
            "Stat": "Sum"
        },
        "ReturnData": true
    }
]
```

아래는 이 명령에서 나온 출력값입니다. 다음 사항에 유의하세요.

- 명령의 시작 시간과 종료 시간은 2019-05-01T04:01:00Z에서 2019-05-01T04:07:00Z까지 7분의 기간에 적용됩니다.
- 반환 값은 단 6개입니다. 이 기간 동안에는 DNS 쿼리가 없었기 때문에 2019-05-01T04:05:00Z에 대한 값은 없습니다.
- JSON 파일에서 지정된 Period의 값은 60(초)이므로 1분의 간격을 두고 값들이 보고됩니다.


```
{
    "MetricDataResults": [
        {
            "Id": "my_dns_queries_id",
            "StatusCode": "Complete",
            "Label": "DNSQueries",
            "Values": [
                101.0,
                115.0,
                103.0,
                127.0,
                111.0,
                120.0
            ],
            "Timestamps": [
                "2019-05-01T04:07:00Z",
                "2019-05-01T04:06:00Z",
                "2019-05-01T04:04:00Z",
                "2019-05-01T04:03:00Z",
                "2019-05-01T04:02:00Z",
                "2019-05-01T04:01:00Z"
            ]
        }
    ]
}
```


퍼블릭 호스팅 영역 삭제

이 섹션에서는 Amazon Route 53 콘솔을 사용하여 퍼블릭 호스팅 영역을 삭제하는 방법을 설명합니다.

기본 SOA 및 NS 레코드 이외의 레코드가 없는 경우에만 호스팅 영역을 삭제할 수 있습니다. 호스팅 영역에 다른 레코드가 포함되어 있는 경우, 호스팅 영역을 삭제하기 전에 이를 삭제해야 합니다. 이를 통해 레코드를 포함하고 있는 호스팅 영역을 실수로 삭제하는 일을 방지할 수 있습니다.

주제

- 사용 중인 도메인으로의 트래픽 라우팅 방지
- 다른 서비스에서 생성한 퍼블릭 호스팅 영역 삭제
- Route 53 콘솔을 사용하여 퍼블릭 호스팅 영역 삭제

사용 중인 도메인으로의 트래픽 라우팅 방지

도메인 등록을 유지하는 동시에 웹 사이트 또는 웹 애플리케이션으로 인터넷 트래픽이 라우팅되는 것을 중지하고자 한다면 호스팅 영역을 삭제하는 대신 호스팅된 영역에서 레코드를 삭제하는 것이 좋습니다.

> **Important**
>
> 호스팅 영역을 삭제하면 호스팅 영역의 삭제를 취소할 수 없습니다. 새 호스팅 영역을 만들고 도메인 등록을 위한 이름 서버를 업데이트해야 합니다. 도메인 등록은 효력이 발생하려면 최대 48 시간이 걸립니다. 또한, 호스팅 영역을 삭제하면 귀하의 도메인을 사용하여 다른 사람이 도메인과 라우팅 트래픽을 이들 리소스로 가로챌 수 있습니다.
>
> 하위 도메인에 대한 책임을 호스팅 영역으로 위임하고 하위 호스팅 영역을 삭제하려면 하위 호스팅 영역과 이름이 같은 NS 레코드를 삭제하여 상위 호스팅 영역도 업데이트해야 합니다. 예를 들어 호스팅 영역 acme.example.com을 삭제하려면 example.com 호스팅 영역에서 NS 레코드 acme.example.com도 삭제해야 합니다. 먼저 NS 레코드를 삭제하고 NS 레코드의 TTL이 지속될 때까지 기다린 후 하위 호스팅 영역을 삭제하는 것이 좋습니다. 이렇게 하면 DNS 해석기가 하위 호스팅 영역의 이름 서버를 계속 캐시하는 기간 동안 다른 누군가가 하위 호스팅 영역을 가로챌 수 없습니다.

호스팅 영역의 요금을 매달 부담하지 않으려면 무료 DNS 서비스로 도메인의 DNS 서비스를 이전할 수 있습니다. DNS 서비스를 이전할 경우, 도메인 등록을 위해 이름 서버를 업데이트해야 합니다. 도메인이 Route 53에 등록된 경우 Route 53 이름 서버를 새로운 DNS 서비스의 이름 서버로 바꾸는 방법에 대한 자세한 내용은 도메인의 글루 레코드 및 이름 서버 추가 또는 변경 섹션을 참조하세요. 도메인이 다른 등록 대행자에 등록되어 있는 경우 등록 대행자가 제공한 방법을 사용하여 도메인 등록에 대한 이름 서버를 업데이트하십시오. 자세한 내용은 인터넷에서 "무료 DNS 서비스"를 검색하여 참조하십시오.

다른 서비스에서 생성한 퍼블릭 호스팅 영역 삭제

호스팅 영역이 다른 서비스에서 생성된 경우 Route 53 콘솔을 사용하여 삭제할 수 없습니다. 대신 다른 서비스에 대한 해당 프로세스를 사용해야 합니다.

- AWS Cloud Map - 퍼블릭 DNS 네임스페이스를 생성할 때 AWS Cloud Map 생성한 호스팅 영역을 삭제하려면 네임스페이스를 삭제합니다.는 호스팅 영역을 자동으로 AWS Cloud Map 삭제합니다. 자세한 내용은 AWS Cloud Map 개발자 안내서의 네임스페이스 삭제를 참조하세요.
- Amazon Elastic Container Service(Amazon ECS) 서비스 검색 – 서비스 검색을 사용하여 서비스를 만들 때 Amazon ECS에서 생성한 퍼블릭 호스팅 영역을 삭제하려면 네임스페이스를 사용하는 Amazon ECS 서비스를 삭제하고 해당 네임스페이스를 삭제하세요. 자세한 내용은 Amazon Elastic Container Service 개발자 안내서의 서비스 삭제를 참조하세요.

Route 53 콘솔을 사용하여 퍼블릭 호스팅 영역 삭제

Route 53 콘솔을 사용하여 퍼블릭 호스팅 영역을 삭제하려면 다음 절차를 수행하세요.

Route 53 콘솔을 사용하여 퍼블릭 호스팅 영역을 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택하고 삭제하려는 호스팅 영역에 강조 표시된 링크를 선택합니다.
3. 삭제할 호스팅 영역에 NS 및 SOA 레코드만 포함되어 있는지 확인합니다. 다른 레코드가 있는 경우 삭제합니다. DNSSEC 서명도 사용하지 않아야 합니다.

    - 호스팅 영역 세부 정보 페이지의 레코드(Records) 목록에 유형(Type) 열의 값이 NS 또는 SOA 이외의 레코드가 포함되어 있는 경우, 해당 행을 선택한 다음 삭제(Delete)를 선택합니다.

      연속된 여러 레코드를 선택하려면 첫 번째 행을 선택한 다음, [Shift] 키를 누른 상태에서 마지막 행을 선택합니다. 비연속적인 여러 레코드를 선택하려면 첫 번째 행을 선택한 다음, [Ctrl] 키를 누른 상태에서 나머지 행을 선택합니다.

      > **Note**
      >
      > 호스팅 영역의 하위 도메인에 대한 NS 레코드를 생성한 경우, 해당 레코드 역시 삭제합니다.

4. 호스팅 영역(Hosted zones) 페이지로 돌아가서 삭제하려는 호스팅 영역의 행을 선택합니다.
5. Delete(삭제)를 선택합니다.
6. 확인 키를 입력하고 삭제(Delete)를 선택합니다.
7. 도메인을 인터넷에서 사용 불가능하게 만들려면 DNS 서비스를 무료 DNS 서비스로 이전한 후 Route 53 호스팅 영역을 삭제하세요. 이렇게 하면 이후의 DNS 쿼리가 잘못 라우팅되지 않도록 할 수 있습니다.

   도메인이 Route 53에 등록된 경우 Route 53 이름 서버를 새로운 DNS 서비스의 이름 서버로 바꾸는 방법에 대한 자세한 내용은 도메인의 글루 레코드 및 이름 서버 추가 또는 변경 섹션을 참조하세요. 도메인이 다른 등록 대행자에 등록되어 있는 경우 등록 대행자가 제공한 방법을 사용하여 도메인에 대한 이름 서버를 변경하십시오.

   > **Note**
   >
   > 하위 도메인(acme.example.com)의 호스팅 영역을 삭제하는 경우에는 도메인(example.com)의 이름 서버를 변경할 필요가 없습니다.

Route 53에서 DNS 응답 확인

도메인에 대해 Amazon Route 53 호스팅 영역을 생성한 경우 콘솔에서 DNS 확인 도구를 사용하여 DNS 서비스로 Route 53를 사용하도록 도메인을 구성하면 Route 53가 어떻게 DNS 쿼리에 응답하는지 확인할 수 있습니다. 또한 지리 위치, 지리 근접성 및 지연 시간 레코드에 대해 특정 DNS 해석기 및/또는 클라이언트 IP 주소에서 쿼리를 시뮬레이션하여 Route 53에서 반환하는 응답을 확인할 수 있습니다.

> **Important**
>
> 이 도구는 Domain Name System에 쿼리를 제출하지 않으며 호스팅 영역의 레코드 설정을 기반으로 해서만 응답합니다. 이 도구는 호스팅 영역이 현재 도메인의 트래픽을 라우팅하는 데 사용되고 있는지 여부에 관계없이 동일한 정보를 반환합니다.

DNS 확인 도구는 퍼블릭 호스팅 영역에만 사용할 수 있습니다.

> **Note**
>
> DNS 검사 도구는 `dig` 명령의 응답 섹션에서 예상할 수 있는 내용과 유사한 정보를 반환합니다. 따라서 상위 이름 서버를 가리키는 하위 도메인의 이름 서버에 대해 쿼리해도 해당 이름 서버는 반환되지 않습니다.

주제

확인 도구를 사용해 Amazon Route 53가 DNS 쿼리에 응답하는 방식 확인

도구를 사용하여 레코드의 DNS 쿼리에 대한 대응으로 Amazon Route 53가 반환하는 응답을 확인할 수 있습니다.

확인 도구를 사용하여 Route 53가 DNS 쿼리에 응답하는 방식을 확인하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
3. [Hosted Zones] 페이지에서 호스팅 영역의 이름을 선택합니다. 콘솔에 해당 호스팅 영역의 레코드 목록이 표시됩니다.
4. Route 53의 응답 확인(Check response from Route 53) 페이지로 바로 이동하려면 레코드 테스트(Test record)를 선택합니다.
5. 다음 값을 지정하세요.
   - 호스팅 영역의 이름을 제외한 레코드의 이름입니다. 예를 들어, www.example.com을 확인하려면 www를 입력합니다. example.com을 확인하려면 레코드 이름 필드를 비워 둡니다.
   - 확인하려는 레코드의 유형(예: A 또는 CNAME)입니다.
6. [Get Response]를 선택합니다.
7. Route 53에서 반환된 응답(Response returned by Route 53) 섹션에는 다음 값이 포함됩니다.

   DNS 응답 코드

   쿼리가 유효한지 여부를 나타내는 코드입니다. 가장 일반적인 응답 코드는 [NOERROR]이며, 이는 쿼리가 유효한 상태임을 의미합니다. 응답이 유효하지 않은 경우에는 Route 53가 이유

를 설명하는 응답 코드를 반환합니다. 가능한 응답 코드의 목록을 보려면 IANA 웹 사이트에서 DNS RCODES 단원을 참조하십시오.

프로토콜

Amazon Route 53이 쿼리에 응답하는 데 사용한 프로토콜은 [UDP] 또는 [TCP]입니다.

Route 53에서 반환된 응답

Route 53가 웹 애플리케이션에 반환하는 값입니다. 값은 다음 중 하나입니다.

- 별칭이 아닌 레코드의 경우 응답에 레코드에 있는 값이 포함됩니다.
- 이름과 유형이 동일한 여러 레코드의 경우(가중치, 지연 시간, 지리 위치 및 장애 조치 포함) 응답에 요청을 기반으로 적절한 레코드의 값이 포함됩니다.
- 다른 레코드 이외의 AWS 리소스를 참조하는 별칭 레코드의 경우 응답에는 리소스 유형에 따라 AWS 리소스의 IP 주소 또는 도메인 이름이 포함됩니다.
- 다른 레코드를 참조하는 별칭 레코드의 경우 응답에 참조된 레코드의 값이 포함됩니다.

확인 도구를 이용해 특정 IP 주소에서 쿼리 시뮬레이션(지리 위치 및 지연 시간 레코드만 해당)

지연 시간 또는 지리 위치 레코드를 생성한 경우 확인 도구를 사용하여 DNS 해석기 및 클라이언트의 IP 주소에서 쿼리를 시뮬레이션할 수 있습니다.

확인 도구를 사용하여 지정된 IP 주소에서 쿼리를 시뮬레이션하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
3. [Hosted Zones] 페이지에서 호스팅 영역의 이름을 선택합니다. 콘솔에 해당 호스팅 영역의 레코드 목록이 표시됩니다.
4. [Check response from Route 53] 페이지로 바로 이동하려면 [Test record set]를 선택합니다.

   특정 레코드에 대한 [Check response from Route 53] 페이지로 이동하려면 해당 레코드의 확인란을 선택하고 [Test record set]를 선택합니다.
5. 먼저 레코드를 선택하지 않고 레코드 세트 테스트를 선택한 경우, 다음 값을 지정합니다.

   - 호스팅 영역의 이름을 제외한 레코드의 이름입니다. 예를 들어, www.example.com을 확인하려면 www를 입력합니다. example.com을 확인하려면 레코드 이름 필드를 비워 둡니다.
   - 확인하려는 레코드의 유형(예: A 또는 CNAME)입니다.

6. 해당하는 값을 지정합니다.

   해석기 IP 주소

   클라이언트가 요청할 때 사용하는 DNS 해석기의 위치를 시뮬레이션할 IPv4 또는 IPv6 주소를 지정합니다. 이는 지연 시간 및 지리 위치 레코드를 테스트하는 데 유용합니다. 이 값을 생략하면 도구는 AWS 미국 동부(버지니아 북부) 리전(us-east-1)에 있는 DNS 해석기의 IP 주소를 사용합니다.

   EDNS0 클라이언트 서브넷 IP

   해석기가 EDNS0을 지원하는 경우 해당 지리적 위치의 IP 주소로 클라이언트 서브넷 IP 주소를 입력합니다(예: 192.0.2.0 또는 2001:db8:85a3::8a2e:370:7334).

   서브넷 마스크

   [EDNS0 client subnet IP]의 IP 주소를 지정하는 경우 확인 도구가 DNS 쿼리에 포함하도록 원하는 IP 주소의 비트 수를 선택적으로 지정할 수 있습니다. 예를 들어, EDNS0 클라이언트 서브넷 IP(EDNS0 client subnet IP)로 192.0.2.44을 지정하고 서브넷 마스크(Subnet mask)로 24를 지정하는 경우 확인 도구는 192.0.2.0/24의 쿼리를 시뮬레이션합니다. 기본값은 IPv4 주소의 경우 24비트, IPv6 주소의 경우 비트입니다.

7. [Get Response]를 선택합니다.

8. Route 53에서 반환된 응답(Response returned by Route 53) 섹션에는 다음 값이 포함됩니다.

   Route 53에 전송되는 DNS 쿼리

   확인 도구가 Route 53로 전송한 Bind 형식의 쿼리입니다. 이는 웹 애플리케이션에서 쿼리를 보내는 데 사용하는 동일한 형식입니다. 일반적으로 세 가지 값은 레코드의 이름, [IN](인터넷용) 및 레코드의 유형입니다.

   DNS 응답 코드

   쿼리가 유효한지 여부를 나타내는 코드입니다. 가장 일반적인 응답 코드는 [NOERROR]이며, 이는 쿼리가 유효한 상태임을 의미합니다. 응답이 유효하지 않은 경우에는 Route 53가 이유를 설명하는 응답 코드를 반환합니다. 가능한 응답 코드의 목록을 보려면 IANA 웹 사이트에서 DNS RCODES 단원을 참조하십시오.

   프로토콜

   Amazon Route 53이 쿼리에 응답하는 데 사용한 프로토콜은 [UDP] 또는 [TCP]입니다.

Route 53에서 반환된 응답

Route 53가 웹 애플리케이션에 반환하는 값입니다. 값은 다음 중 하나입니다.

- 별칭이 아닌 레코드의 경우 응답에 레코드에 있는 값이 포함됩니다.
- 이름과 유형이 동일한 여러 레코드의 경우(가중치, 지연 시간, 지리 위치 및 장애 조치 포함) 응답에 요청을 기반으로 적절한 레코드의 값이 포함됩니다.
- 다른 레코드 이외의 AWS 리소스를 참조하는 별칭 레코드의 경우 응답에는 리소스 유형에 따라 AWS 리소스의 IP 주소 또는 도메인 이름이 포함됩니다.
- 다른 레코드를 참조하는 별칭 레코드의 경우 응답에 참조된 레코드의 값이 포함됩니다.

화이트 레이블 이름 서버 구성

각 Amazon Route 53 호스팅 영역은 4개의 이름 서버(합쳐서 위임 세트라고 함)와 연결되어 있습니다. 기본적으로 이름 서버에는 ns-2048.awsdns-64.com과 같은 이름이 있습니다. 이름 서버의 도메인 이름이 호스팅 영역의 도메인 이름과 동일하기를 원하는 경우(예: ns1.example.com), 베니티 이름 서버 또는 프라이빗 이름 서버라고도 하는 화이트 레이블 이름 서버를 구성하면 됩니다.

다음 절차에서는 여러 도메인에 재사용할 수 있는 네 개의 화이트 레이블 이름 서버 한 세트를 구성하는 방법을 설명합니다. 예를 들어, example.com, example.org, example.net 도메인을 소유하고 있다고 가정해 봅시다. 이 절차를 통해 example.com에 대한 화이트 레이블 이름 서버를 구성하고 이를 example.org 및 example.net에 재사용할 수 있습니다.

주제

1단계: 재사용 가능한 Route 53 위임 세트 만들기

흰색 레이블 이름 서버는 Route 53 재사용 가능한 위임 세트와 연결됩니다. 호스팅 영역과 재사용 가능한 위임 세트가 동일한 AWS 계정에서 생성된 경우에만 호스팅 영역에 화이트 레이블 이름 서버를 사용할 수 있습니다.

재사용 가능한 위임 세트를 생성하려면 Route 53 API, AWS CLI 또는 AWS SDKs. 자세한 내용은 다음 설명서를 참조하세요.

- Route 53 API - Amazon Route 53 API 참조의 CreateReusableDelegationSet 참조
- AWS CLI - AWS CLI 명령 참조의 create-reusable-delegation-set 참조
- AWS SDKs AWS 참조하세요.

2단계: Amazon Route 53 호스팅 영역을 생성 또는 재생성하고 NS 및 SOA 레코드에 대한 TTL 변경

Amazon Route 53 호스팅 영역 생성 또는 재생성:

- 화이트 레이블 이름 서버를 사용할 도메인의 DNS 서비스로 현재 Route 53를 사용하고 있지 않은 경우 - 호스팅 영역을 생성하고 이전 단계에서 호스팅 영역별로 생성한 재사용 가능한 위임 세트를 지정합니다. 자세한 내용은 Amazon Route 53 API 참조의 CreateHostedZone을 참조하세요.
- 화이트 레이블 이름 서버를 사용할 도메인의 DNS 서비스로 Route 53를 사용하고 있는 경우 - 화이트 레이블 이름 서버를 사용할 호스팅 영역을 다시 생성한 다음, 이전 단계에서 호스팅 영역별로 생성한 재사용 가능한 위임 세트를 지정해야 합니다.

> **Important**
>
> 기존 호스팅 영역과 연결된 이름 서버는 변경할 수 없습니다. 재사용 가능한 위임 세트를 호스팅 영역과 연결하려면 호스팅 영역을 생성해야 합니다.

호스팅 영역을 생성하는 경우, 해당 도메인의 리소스에 액세스를 시도하기 전에 각 호스팅 영역에서 다음 TTL 값을 변경합니다.

- 호스팅 영역에 대한 NS 레코드의 TTL을 60초 이하로 변경합니다.
- 호스팅 영역에 대한 SOA 레코드의 최소 TTL을 60초 이하로 변경합니다. 이는 SOA 레코드의 마지막 값입니다.

등록자에게 실수로 화이트 레이블 이름 서버에 대한 잘못된 IP 주소를 제공하면, 웹 사이트를 사용할 수 없게 되며 문제가 해결된 후에도 TTL 기간 동안은 사용할 수 없습니다. TTL을 낮게 설정하면 웹 사이트를 사용하지 못하는 기간을 단축할 수 있습니다.

호스팅 영역을 생성하고 호스팅 영역의 이름 서버에 대해 재사용 가능한 위임 세트를 지정하는 방법에 대한 자세한 내용은 Amazon Route 53 API 참조의 CreateHostedZone을 참조하세요.

3단계: 호스팅 영역의 레코드 다시 생성

2단계에서 생성한 호스팅 영역에 레코드 생성:

- 도메인의 DNS 서비스를 Amazon Route 53로 마이그레이션하는 경우 - 기존 레코드에 대한 정보를 가져와서 레코드를 생성할 수 있습니다. 자세한 내용은 영역 파일을 가져와 레코드 생성 섹션을 참조하세요.
- 화이트 레이블 이름 서버를 사용할 수 있도록 기존 호스팅 영역을 대체하는 경우 - 새 호스팅 영역에서 현재 호스팅 영역에 나타나는 레코드를 다시 생성합니다. Route 53의 경우 호스팅 영역에서 레코드를 내보낼 방법이 없지만 일부 타사 공급 업체에서는 가능합니다. 그런 다음 Route 53 가져오기 기능으로 라우팅 정책이 단순하며 별칭이 아닌 레코드를 가져올 수 있습니다. 별칭 레코드 또는 라우팅 정책이 단순하지 않은 레코드는 내보냈다가 다시 가져올 수 없습니다.

  Route 53 API를 사용하여 레코드를 만드는 방법에 대한 자세한 내용은 Amazon Route 53 API 참조의 CreateHostedZone을 참조하세요. Route 53 콘솔을 사용하여 레코드를 생성하는 방법에 대한 자세한 내용은 레코드 작업 섹션을 참조하세요.

4단계: IP 주소 받기

재사용 가능한 위임 세트에서 이름 서버의 IPv4 및 IPv6 주소를 가져온 다음, 아래 표에 입력합니다.

재사용 가능한 위임 세트의 이름 서버 이름(예: Ns-2048.awsdns-64.com)	IPv4 및 IPv6 주소	화이트 레이블 이름 서버에 할당할 이름(예: ns1.example.com)
	IPv4: IPv6:	
	IPv4: IPv6:	

재사용 가능한 위임 세트의 이름 서버 이름(예: Ns-2048.awsdns-64.com)	IPv4 및 IPv6 주소	화이트 레이블 이름 서버에 할당할 이름(예: ns1.example.com)
	IPv4: IPv6:	
	IPv4: IPv6:	

예를 들어, 재사용 가능한 위임 세트의 이름 서버 네 개가 다음과 같다고 가정해 봅시다.

- ns-2048.awsdns-64.com
- ns-2049.awsdns-65.net
- ns-2050.awsdns-66.org
- ns-2051.awsdns-67.co.uk

다음은 4개 이름 서버 중 첫 번째의 IP 주소를 가져오기 위해 실행할 Linux 및 Windows 명령입니다.

Linux용 dig 명령

```
% dig A ns-2048.awsdns-64.com +short
192.0.2.117
```

```
% dig AAAA ns-2048.awsdns-64.com +short
2001:db8:85a3::8a2e:370:7334
```

Windows의 경우 nslookup 명령

```
c:\> nslookup ns-2048.awsdns-64.com
Non-authoritative answer:
Name:    ns-2048.awsdns-64.com
Addresses:  2001:db8:85a3::8a2e:370:7334
          192.0.2.117
```

5단계: 화이트 레이블 이름 서버의 레코드 생성

화이트 레이블 이름 서버의 도메인 이름(예: ns1.example.com)과 이름이 동일한 호스팅 영역(예: example.com)에서 8개의 레코드를 생성합니다.

- 각 화이트 레이블 이름 서버당 A 레코드 1개
- 각 화이트 레이블 이름 서버당 AAAA 레코드 1개

> **Important**
>
> 둘 이상의 호스팅 영역에 대해 동일한 화이트 레이블 이름 서버를 사용하는 경우, 다른 호스팅 영역에 대해 이 단계를 수행하지 마십시오.

각 레코드에 대해 다음 값을 지정합니다. 이전 단계에서 입력한 표를 참조하십시오.

라우팅 정책

단순 라우팅(Simple routing)을 지정합니다.

레코드 이름

화이트 레이블 이름 서버 중 하나에 할당할 이름입니다(예: ns1.example.com). 접두사(이 예에서는 ns1)의 경우, 도메인 이름에 유효한 모든 값을 사용할 수 있습니다.

값/트래픽 라우팅 대상

재사용 가능한 위임 세트의 Route 53 이름 서버 중 하나의 IPv4 또는 IPv6 주소입니다.

> **Important**
>
> 화이트 레이블 이름 서버에 대한 레코드를 생성할 때 잘못된 IP 주소를 지정하면, 다음 단계를 수행할 때 인터넷에서 웹 사이트 또는 웹 애플리케이션을 사용할 수 없게 됩니다. IP 주소를 즉시 수정하더라도 TTL 기간 동안에는 웹 사이트 또는 웹 애플리케이션을 사용할 수 없습니다.

레코드 유형

IPv4 주소에 대해 레코드를 생성하는 경우 [A]를 지정합니다.

IPv6 주소에 대해 레코드를 생성하는 경우 [AAAA]를 지정합니다.

TTL(초)

이 값은 DNS 해석기에서 Route 53로 또 다른 DNS 쿼리를 전달하기 전에 이 레코드의 정보를 캐싱하는 시간입니다. 이러한 레코드에 실수로 잘못된 값을 지정하는 경우 신속하게 복구할 수 있도록 초기 값을 60초 이하로 지정하는 것이 좋습니다.

6단계: NS 및 SOA 레코드 업데이트

화이트 레이블 이름 서버를 사용할 호스팅 영역의 SOA 및 NS 레코드를 업데이트합니다. 한 번에 호스팅 영역 한 개와 해당 도메인에 대해 6-8단계를 수행한 다음, 다른 호스팅 영역과 도메인에 대해 이를 반복합니다.

> **Important**
>
> 화이트 레이블 이름 서버(예: ns1.example.com)와 도메인 이름이 동일한 Amazon Route 53 호스팅 영역(예: example.com)부터 시작합니다.

1. Route 53 이름 서버의 이름을 화이트 레벨 이름 서버 중 하나의 이름으로 바꿔서 SOA 레코드를 업데이트합니다.

   예

   Route 53 이름 서버의 이름을

   ```
   ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 60
   ```

   화이트 레벨 이름 서버 중 하나의 이름으로 바꿉니다.

   ```
   ns1.example.com. hostmaster.example.com. 1 7200 900 1209600 60
   ```

   > **Note**
   >
   > 2단계: Amazon Route 53 호스팅 영역을 생성 또는 재생성하고 NS 및 SOA 레코드에 대한 TTL 변경에서 마지막 값인 최소 TTL(Time To Live)을 변경했습니다.

   Route 53 콘솔을 사용하여 레코드를 업데이트하는 방법에 대한 자세한 내용은 레코드 편집 섹션을 참조하세요.

2. NS 레코드에서 도메인에 대한 현재 이름 서버의 이름을 기록해 두고, 필요할 경우 되돌릴 수 있도록 하십시오.
3. NS 레코드를 업데이트합니다. Route 53 이름 서버의 이름을 화이트 레이블 이름 서버 4개의 이름(예: `ns1.example.com`, `ns2.example.com`, `ns3.example.com` 및 `ns4.example.com`)으로 바꿉니다.

7단계: 글루 레코드 생성 및 등록 대행자 이름 서버 변경

등록자가 제공한 방법을 사용하여 다음과 같이 글루 레코드를 생성하고 등록자의 이름 서버를 변경합니다.

1. 글루 레코드를 추가하는 방법:
   - 화이트 레이블 이름 서버와 도메인 이름이 동일한 도메인을 업데이트하는 경우 - 이름 및 IP 주소가 4단계에서 얻은 값과 일치하는 글루 레코드 4개를 생성합니다. 해당 글루 레코드에 화이트 레이블 이름 서버의 IPv4 및 IPv6 주소를 모두 포함시킵니다. 예를 들면 다음과 같습니다.

     ns1.example.com – IP 주소 = 192.0.2.117 및 2001:db8:85a3::8a2e:370:7334

     등록자는 글루 레코드에 대해 다양한 용어를 사용합니다. 이를 새로운 이름 서버 또는 이와 유사한 대상을 등록하는 것으로 볼 수도 있습니다.
   - 또 다른 도메인을 업데이트하는 경우 – Route 53이 DNS 서비스인 경우 먼저 항목의 단계를 완료하고 도메인 이름과 일치하는 글루 레코드를 만들어야 합니다. 그런 다음 이 절차의 2단계로 건너뜁니다.
2. 도메인의 이름 서버를 화이트 레이블 이름 서버의 이름으로 변경합니다.

Amazon Route 53를 DNS 서비스로 사용하는 경우, 도메인의 글루 레코드 및 이름 서버 추가 또는 변경 섹션을 참조하세요.

8단계: 웹 사이트 또는 애플리케이션의 트래픽 모니터링

7단계에서 글루 레코드를 생성하고 이름 서버를 변경한 웹 사이트 또는 애플리케이션의 트래픽을 다음과 같이 모니터링합니다.

- 트래픽이 중지된 경우 - 등록 기관이 제공한 방법을 사용하여 도메인의 이름 서버를 이전 Route 53 이름 서버로 다시 변경합니다. 이는 6b단계에서 기록해 둔 이름 서버입니다. 그런 다음 문제를 알아냅니다.

- 트래픽에 영향이 없는 경우 - 동일한 화이트 레이블 이름 서버를 사용할 나머지 호스팅 영역에 대해 6~8단계를 반복합니다.

9단계: TTL을 원래 값으로 다시 변경

현재 화이트 레이블 이름 서버를 사용 중인 모든 호스팅 영역에 대해 다음 값을 변경합니다.

- 호스팅 영역에 대한 NS 레코드의 TTL을 더 일반적인 NS 레코드 값으로 변경합니다(예: 172800초(2일)).
- 호스팅 영역에 대한 SOA 레코드의 최소 TTL을 더 일반적인 SOA 레코드 값으로 변경합니다(예: 900초). 이는 SOA 레코드의 마지막 값입니다.

10단계: (선택 사항) 리커시브 DNS 서비스에 연락

선택 사항 - Amazon Route 53 지리적 위치 라우팅을 사용하는 경우, EDNS0의 edns-client-subnet 확장을 지원하는 리커시브 DNS 서비스에 연락하여 화이트 레이블 이름 서버의 이름을 알려 주세요. 이를 통해 이러한 DNS 서비스에서 쿼리가 시작된 대략적인 지리적 위치에 기반한 최적의 Route 53 위치로 DNS 쿼리를 계속 라우팅할 수 있습니다.

Amazon Route 53에서 퍼블릭 호스팅 영역에 대해 생성하는 NS 및 SOA 레코드

Amazon Route 53는 생성하는 각 퍼블릭 호스팅 영역에 대해 NS(이름 서버) 레코드 및 SOA(권한 시작) 레코드를 자동으로 생성합니다. 이러한 레코드는 거의 변경할 필요가 없습니다.

주제

NS(이름 서버) 레코드

Amazon Route 53는 호스팅 영역과 이름이 동일한 NS(이름 서버) 레코드를 자동으로 생성하고, 호스팅 영역에 대한 신뢰할 수 있는 이름 서버 네 개를 나열합니다. 드문 경우를 제외하고 이 레코드에서 이름 서버를 추가, 변경 또는 삭제하지 않는 것이 좋습니다.

다음 예는 Route 53 이름 서버의 이름 형식을 보여줍니다(이것은 예시일 뿐이므로 등록자의 이름 서버 레코드를 업데이트할 때 사용하면 안 됩니다).

- ns-2048.awsdns-64.com

- ns-2049.awsdns-65.net
- ns-2050.awsdns-66.org
- ns-2051.awsdns-67.co.uk

호스팅 영역의 이름 서버 목록을 가져오려면:

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted Zones)을 클릭합니다.
3. 호스팅 영역(Hosted zones) 페이지에서 호스팅 영역의 (이름 대신) 라디오 버튼을 선택한 다음 세부 정보 보기(View details)를 선택합니다.
4. 호스팅 영역에 대한 세부 정보 페이지에서 호스팅 영역 세부 정보(Hosted zone details)를 선택합니다.
5. 이름 서버(Name servers)에 나열된 서버 4개의 이름을 기록합니다.

다른 DNS 서비스 공급자에서 Route 53로의 DNS 서비스 마이그레이션에 대한 자세한 내용은 Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정 섹션을 참조하세요.

SOA(권한 시작) 레코드

SOA(권한 시작) 레코드는 도메인에 대한 기본 DNS 정보를 식별합니다. 예:

```
ns-2048.awsdns-64.net. hostmaster.example.com. 1 7200 900 1209600 86400
```

SOA 레코드에는 다음 요소가 포함되어 있습니다.

- SOA 레코드를 생성한 Route 53 이름 서버(예: `ns-2048.awsdns-64.net`)입니다.
- 관리자의 이메일 주소입니다. @ 기호는 마침표로 대체됩니다(예: `hostmaster.example.com`). 기본 값은 모니터링되지 않는 amazon.com 이메일 주소입니다.
- 호스팅 영역에서 레코드를 업데이트할 때마다 선택적으로 증가시킬 수 있는 일련번호입니다. Route 53는 자동으로 숫자를 증가시키지 않습니다. (일련 번호는 부 DNS를 지원하는 DNS 서비스에 사용됩니다.) 이 예시에서 이 값은 `1`입니다.
- 부 DNS 서버에서 주 DNS 서버의 SOA 레코드를 쿼리하여 변경 내용을 확인하기 전에 기다리는 새로 고침 시간(초). 이 예시에서 이 값은 `7200`입니다.
- 부 서버에서 실패한 영역 전송을 재시도하기 전에 기다리는 재시도 간격(초). 일반적으로 재시도 시간은 새로 고침 시간보다 짧습니다. 이 예시에서 이 값은 `900`(15분)입니다.

- 부 서버에서 영역 전송을 완료하기 위해 시도할 수 있는 시간(초). 영역이 성공적으로 전송되기 전에 이 시간이 경과하면 부 서버에서 데이터가 오래되어 신뢰할 수 없다고 간주하여 쿼리에 응답하는 것을 중지합니다. 이 예시에서 이 값은 1209600(2주)입니다.
- 최소 TTL(Time To Live). 이 값은 재귀 해석기에서 다음 응답을 Route 53에서 캐싱해야 하는 시간을 정의하는 데 도움이 됩니다.

  NXDOMAIN

  example.com과 같이 DNS 쿼리에 지정된 이름을 가진 유형의 레코드가 없습니다. zenith.example.com과 같이 DNS 쿼리에 지정된 이름의 하위 레코드도 없습니다.

  NODATA

  DNS 쿼리에 지정된 이름을 가진 레코드가 하나 이상 있지만 이러한 레코드 중 DNS 쿼리에 지정된 유형(예: A)은 없습니다.

  DNS 해석기에서 NXDOMAIN 또는 NODATA 응답을 캐싱하면 이를 음성 캐싱이라고 합니다.

  음성 캐싱의 기간은 다음 값보다 짧습니다.

  - 이 값은 SOA 레코드의 최소 TTL입니다. 이 예에서 이 값은 86400(하루)입니다.
  - SOA 레코드에 대한 TTL의 값입니다. 기본 값은 900초입니다. 이 값의 변경에 대한 자세한 내용은 다음(레코드 편집)을 참조하십시오.

  Route 53에서 NXDOMAIN 또는 NODATA 응답(부정 응답)을 사용하여 DNS 쿼리에 응답하면 표준 쿼리의 요율로 비용이 청구됩니다. (Amazon Route 53 가격에서 “쿼리”를 참조하세요. 부정 응답 비용이 염려되는 경우 한 가지 옵션은 SOA 레코드의 TTL, SOA 레코드의 최소 TTL(이 값) 또는 둘 다 변경하는 것입니다. 전체 호스팅 영역에 대한 부정 응답에 적용되는 이러한 TTL을 늘리면 긍정적인 효과와 부정적인 효과를 모두 가질 수 있습니다.

  - 인터넷의 DNS 해석기에 더 오랜 기간 동안 존재하지 않는 레코드를 캐싱하므로 Route 53에 전달되는 쿼리 수가 감소합니다. 이렇게 하면 DNS 쿼리에 대한 Route 53 요금이 감소합니다.
  - 그러나 유효한 레코드를 잘못 삭제한 후 나중에 다시 생성하면 DNS 해석기에서 더 오랜 기간 동안 부정 응답(이 레코드는 존재하지 않음)을 캐싱합니다. 이렇게 하면 고객 또는 사용자가 acme.example.com의 웹 서버와 같은 해당 리소스에 도달할 수 없는 시간이 길어집니다.

루트 53에서 SOA 레코드를 찾으려면 다음을 수행합니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.

3. 레코드를 보려는 도메인의 링크된 이름을 선택합니다.
4. 레코드(Records) 섹션에서 나열된 모든 레코드를 볼 수 있으며 레코드를 필터링하여 SOA 값을 찾을 수 있습니다.

프라이빗 호스팅 영역 사용

프라이빗 호스팅 영역은 Amazon VPC 서비스로 생성한 하나 이상의 VPC 내에 있는 도메인과 그 하위 도메인에 대하여 Amazon Route 53의 DNS 쿼리 응답 정보가 담긴 컨테이너입니다. 프라이빗 호스팅 영역의 작업 방식은 다음과 같습니다.

1. 프라이빗 호스팅 영역을 생성(예: example.com) 및 호스팅 영역과 연결하려는 VPC를 지정합니다. 호스팅 영역을 생성한 후 더 많은 VPC를 여기에 연결할 수 있습니다.
2. VPC 중에서 도메인 및 하위 도메인 그리고 VPC 간에 대한 Route 53의 DNS 쿼리 응답 방식을 확인하는 호스팅 영역에 레코드를 생성합니다. 예를 들어, 데이터베이스 서버가 프라이빗 호스팅 영역에 연결한 VPC의 EC2 인스턴스에서 실행된다고 가정하겠습니다. A 또는 AAAA 레코드를 생성하고 (예: db.example.com) 데이터베이스 서버의 IP 주소를 지정합니다.

   레코드에 대한 자세한 내용은 레코드 작업 단원을 참조하십시오. 프라이빗 호스팅 영역 사용에 대해 Amazon VPC 요구 사항에 대한 자세한 내용은 Amazon VPC 사용 설명서의 프라이빗 호스팅 영역 사용을 참조하세요.
3. 애플리케이션이 db.example.com에 DNS 쿼리를 제출하면 Route 53가 해당 IP 주소를 반환합니다. 프라이빗 호스팅 영역에서 응답을 받으려면 연결된 VPC 중 하나에서 EC2 인스턴스를 실행 중이거나 하이브리드 설정의 인바운드 엔드포인트가 있어야 합니다. VPC 또는 하이브리드 설정 외부에서 프라이빗 호스팅 영역을 쿼리하려고 하면 인터넷에서 쿼리가 반복적으로 해결됩니다.
4. 애플리케이션은 Route 53에서 얻은 IP 주소를 사용하여 데이터베이스 서버와 연결합니다.

프라이빗 호스팅 영역을 생성할 때 다음 네임 서버가 사용됩니다.

- ns-0.awsdns-00.com
- ns-512.awsdns-00.net
- ns-1024.awsdns-00.org
- ns-1536.awsdns-00.co.uk

DNS 프로토콜을 사용하려면 모든 호스팅 영역에 NS 레코드 세트가 있어야 하기 때문에 이러한 네임 서버가 사용됩니다. 이러한 이름 서버는 예약되어 있으며 Route 53 퍼블릭 호스팅 영역에서 절대 사용

되지 않습니다. 프라이빗 호스팅 영역에 지정된 VPC에 연결된 인바운드 엔드포인트를 사용하여 호스팅 영역에 연결된 VPC의 Route 53 Resolver를 통해서만 해당 영역을 쿼리할 수 있습니다.

네임 서버는 인터넷에 표시되지만 Route 53 Resolver는 네임 서버 주소에 연결하지 않습니다. 또한 인터넷을 통해 이름 서버를 직접 쿼리하는 경우 프라이빗 호스팅 영역 정보가 반환되지 않습니다. 대신 Route 53 Resolver는 쿼리가 VPC와 호스팅 영역 간의 연결을 기반으로 프라이빗 네임스페이스 내에 있음을 감지하고 직접 프라이빗 연결을 사용하여 프라이빗 DNS 서버에 도달합니다.

> **Note**
>
> 원하는 경우 프라이빗 호스팅 영역에서 NS 레코드 세트를 변경할 수 있으며 프라이빗 DNS 확인은 계속 작동합니다. 그렇게 하는 것은 권장되지 않지만, 원한다면 퍼블릭 DNS 서버에서 사용하지 않는 예약된 도메인 이름을 사용해야 합니다.

인터넷에서 도메인에 대한 트래픽을 라우팅하고자 하는 경우 Route 53 퍼블릭 호스팅 영역을 사용합니다. 자세한 내용은 퍼블릭 호스팅 영역 작업 섹션을 참조하세요.

주제

- 프라이빗 호스팅 영역 작업 시 고려 사항
- 프라이빗 호스팅 영역 생성
- 프라이빗 호스팅 영역 나열
- 더 많은 VPC를 프라이빗 호스팅 영역에 연결
- Amazon VPC와 다른 AWS 계정에서 생성한 프라이빗 호스팅 영역 연결
- 프라이빗 호스팅 영역에서 VPC 연결 해제
- 프라이빗 호스팅 영역 삭제
- VPC 권한

프라이빗 호스팅 영역 작업 시 고려 사항

프라이빗 호스팅 영역을 사용하는 경우 다음 고려 사항을 참조하십시오.

- Amazon VPC settings
- Route 53 health checks
- Supported routing policies for records in a private hosted zone

- Split-view DNS
- Public and private hosted zones that have overlapping namespaces
- Private hosted zones that have overlapping namespaces
- Private hosted zones and Route 53 Resolver rules
- Delegating responsibility for a subdomain
- Custom DNS servers
- Required IAM permissions

Amazon VPC 설정

프라이빗 호스팅 영역을 사용하려면 다음과 같은 Amazon VPC 설정을 `true`로 설정해야 합니다.

- `enableDnsHostnames`
- `enableDnsSupport`

자세한 내용은 Amazon VPC 사용 설명서의 VPC에 대한 DNS 속성 보기 및 업데이트를 참조하세요.

Route 53 상태 확인

프라이빗 호스팅 영역에서는 장애 조치, 다중 값 응답, 가중치 적용, 지연 시간, 지리적 위치 및 지리적 근접성 레코드에만 Route 53 상태 확인을 연결할 수 있습니다. 장애 조치 레코드를 이용한 상태 확인 연결에 대한 자세한 내용은 프라이빗 호스팅 영역에서 장애 조치 구성 단원을 참조하십시오.

프라이빗 호스팅 영역의 레코드에 대해 지원되는 라우팅 정책

프라이빗 호스팅 영역에서 레코드를 생성할 때 다음 라우팅 정책을 사용할 수 있습니다.

- 단순 라우팅
- 장애 조치 라우팅
- 다중값 응답 라우팅
- 가중치 기반 라우팅
- 지연 시간 기반 라우팅
- 지리적 라우팅
- 지리 근접 라우팅

다른 라우팅 정책을 이용해 프라이빗 호스팅 영역에서 레코드를 생성하는 것은 지원되지 않습니다.

분할-보기 DNS

Route 53를 사용하여 분할-보기 DNS(분할-수평 DNS)를 구성할 수 있습니다. 분할-보기 DNS에서는 내부 사용(accounting.example.com) 및 퍼블릭 웹사이트(www.example.com) 같은 외부 사용에 있어 동일한 도메인 이름(example.com)을 사용합니다. 내부 및 외부에서 동일한 하위 도메인 이름을 사용하되, 내부 및 외부 사용자에게 서로 다른 콘텐츠를 제공하거나 서로 다른 인증을 요구하고 싶을 수도 있습니다.

분할-보기 DNS를 구성하려면 다음 단계를 수행합니다.

1. 이름이 동일한 퍼블릭 호스팅 영역과 프라이빗 호스팅 영역을 생성합니다 (퍼블릭 호스팅 영역에서 다른 DNS 서비스를 사용하고 있는 경우에도 분할-보기 DNS는 여전히 작동).
2. 하나 이상의 Amazon VPC를 프라이빗 호스팅 영역에 연결합니다. Route 53 Resolver는 프라이빗 호스팅 영역을 사용하여 지정된 VPC에서 DNS 쿼리를 라우팅합니다.
3. 각 호스팅 영역에서 레코드를 생성합니다. 퍼블릭 호스팅 영역의 레코드는 인터넷 트래픽이 라우팅되는 방법을 제어하고, 프라이빗 호스팅 영역의 레코드는 Amazon VPC에서 트래픽이 라우팅되는 방법을 제어합니다.

VPC 및 온프레미스 워크로드 둘 다의 이름을 확인해야 하는 경우 Route 53 Resolver를 사용할 수 있습니다. 자세한 내용은 Amazon Route 53 Resolver란 무엇인가요? 섹션을 참조하세요.

네임스페이스가 겹치는 퍼블릭 및 프라이빗 호스팅 영역

example.com 및 accounting.example.com과 같이 네임스페이스가 겹치는 프라이빗 및 퍼블릭 호스팅 영역이 있는 경우 Resolver에서는 가장 구체적인 일치를 기반으로 트래픽을 라우팅합니다. 모든 프라이빗 호스팅 영역과 연결된 Amazon VPC에서 사용자가 EC2 인스턴스에 로그인할 때 Route 53 Resolver에서 DNS 쿼리를 처리하는 방법은 다음과 같습니다.

1. Resolver는 프라이빗 호스팅 영역의 이름이 요청에 있는 도메인 이름(예: accounting.example.com)과 일치하는지 평가합니다. 일치는 다음 중 하나로 정의됩니다.
   - 동일한 일치
   - 프라이빗 호스팅 영역의 이름이 요청의 도메인 이름의 부모입니다. 예를 들어 요청에 있는 도메인 이름이 다음과 같다고 가정해 봅니다.

     seattle.accounting.example.com

     다음의 호스팅 영역들은 seattle.accounting.example.com의 부모이기 때문에 일치합니다.

     - accounting.example.com
     - example.com

일치하는 프라이빗 호스팅 영역이 없다면 Resolver가 요청을 퍼블릭 DNS 해석기로 전달하고 요청은 정규 DNS 쿼리로 해결됩니다.

2. 요청에 있는 도메인 이름과 일치하는 프라이빗 호스팅 영역 이름이 있는 경우, 호스팅 영역에서 요청의 도메인 이름 및 DNS 유형(예: accounting.example.com의 A 레코드)과 일치하는 레코드를 찾습니다.

> **Note**
>
> 일치하는 프라이빗 호스팅 영역이 있지만 요청의 도메인 이름 및 유형과 일치하는 레코드가 없다면 Resolver는 요청을 퍼블릭 DNS 해석기로 전달하지 않습니다. 그 대신 NXDOMAIN(존재하지 않는 도메인)을 클라이언트로 반환합니다.

네임스페이스가 겹치는 프라이빗 호스팅 영역

example.com 및 accounting.example.com과 같이 네임스페이스가 겹치는 프라이빗 호스팅 영역이 2개 이상 있는 경우 Resolver에서는 가장 구체적인 일치를 기반으로 트래픽을 라우팅합니다.

> **Note**
>
> 동일한 도메인 이름에 대해 네트워크로 트래픽을 라우팅하는 Route 53 Resolver 규칙과 프라이빗 호스팅 영역(example.com)이 있는 경우 Resolver 규칙이 우선합니다. Private hosted zones and Route 53 Resolver rules을 참조하세요.

모든 프라이빗 호스팅 영역과 연결된 Amazon VPC에서 사용자가 EC2 인스턴스에 로그인할 때 해석기에서 DNS 쿼리를 처리하는 방법은 다음과 같습니다.

1. Resolver는 요청에 있는 도메인 이름(예: accounting.example.com)이 프라이빗 호스팅 영역의 이름과 일치하는지 평가합니다.
2. 요청의 도메인 이름과 정확히 일치하는 호스팅 영역이 없는 경우 Resolver는 요청에서 도메인 이름의 상위 이름을 가진 호스팅 영역을 확인합니다. 예를 들어 요청에 있는 도메인 이름이 다음과 같다고 가정해 봅니다.

   ```
   seattle.accounting.example.com
   ```

   다음 호스팅 영역은 `seattle.accounting.example.com`의 상위 영역이므로 일치합니다.

   - `accounting.example.com`
   - `example.com`

Resolver는 example.com보다 구체적인 accounting.example.com을 선택합니다.

3. Resolver는 요청에서 도메인 이름 및 DNS 유형과 일치하는 레코드 (예: seattle.accounting.example.com에 대한 A 레코드)에 대한 accounting.example.com 호스팅 영역을 검색합니다.

   요청에서 도메인 이름 및 유형과 일치하는 레코드가 없으면 Resolver에서는 존재하지 않는 도메인(NXDOMAIN)을 클라이언트에 반환합니다.

프라이빗 호스팅 영역 및 Route 53 Resolver 규칙

동일한 도메인 이름에 대해 네트워크로 트래픽을 라우팅하는 Resolver 규칙과 프라이빗 호스팅 영역(example.com)이 있는 경우 Resolver 규칙이 우선합니다.

예를 들어, 다음과 같은 구성이 있다고 가정합니다.

- example.com이라는 프라이빗 호스팅 영역이 있고 VPC와 연결합니다.
- example.com의 트래픽을 네트워크로 전달하는 Route 53 Resolver 규칙을 생성하고 이 규칙을 동일한 VPC와 연결합니다.

이 구성에서 Resolver 규칙은 프라이빗 호스팅 영역에 우선합니다. DNS 쿼리는 프라이빗 호스팅 영역의 레코드를 기반으로 해결되지 않고 네트워크로 전달됩니다.

하위 도메인에 대한 책임 위임

프라이빗 호스팅 영역에 NS 레코드를 생성하여 하위 도메인에 대한 책임을 위임할 수 없습니다.

사용자 지정 DNS 서버

VPC의 Amazon EC2 인스턴스에 사용자 정의 DNS 서버를 구성한 경우 해당 VPC에 대해 Amazon에서 제공한 DNS 서버의 IP 주소로 프라이빗 DNS 쿼리를 라우팅하도록 DNS 서버를 구성해야 합니다. 이 IP 주소는 기본 VPC 네트워크 범위에 "2를 더한" 주소입니다. 예를 들어, VPC에 대한 CIDR 범위가 10.0.0.0/16인 경우 DNS 서버의 IP 주소는 10.0.0.2입니다.

VPC와 네트워크 간에 DNS 쿼리를 라우팅하려면 Resolver를 사용하면 됩니다. 자세한 내용은 Amazon Route 53 Resolver란 무엇인가요? 섹션을 참조하세요.

필수 IAM 권한

프라이빗 호스팅 영역을 만들려면 Route 53 작업에 대한 권한 외에도 Amazon EC2 작업에 대해 IAM 권한을 부여해야 합니다. 자세한 내용은 서비스 권한 부여 참조에서 Route 53에 사용되는 작업, 리소스 및 조건 키를 참조하세요.

프라이빗 호스팅 영역 생성

프라이빗 호스팅 영역이란 하나 이상의 Amazon Virtual Private Cloud(VPC)에서 호스팅하는 도메인의 레코드를 모아 둔 컨테이너입니다. 도메인(예: example.com)에 대한 호스팅 영역을 생성한 다음 레코드를 생성하여 VPC 내부 및 VPC 간에 트래픽을 라우팅하는 방식을 Amazon Route 53에 지시합니다.

> **Important**
>
> 프라이빗 호스팅 영역을 생성할 때는 VPC와 호스팅 영역을 연결해야 합니다. 이때 호스팅 영역을 생성할 때 사용하는 것과 동일한 계정으로 생성한 VPC를 지정해야 합니다. 호스팅 영역을 생성한 후 다른 AWS 계정을 사용하여 생성한 VPCs 포함하여 추가 VPCs를 해당 영역과 연결할 수 있습니다.
>
> 한 계정에서 생성한 VPC를 다른 계정에서 생성한 프라이빗 호스팅 영역과 연결하려면 먼저 연결 권한을 부여한 다음 프로그래밍 방식으로 연결해야 합니다. 자세한 내용은 Amazon VPC와 다른 AWS 계정에서 생성한 프라이빗 호스팅 영역 연결 섹션을 참조하세요.

Route 53 API를 사용하여 프라이빗 호스팅 영역을 만드는 방법에 대한 자세한 내용은 Amazon Route 53 API 참조를 참조하세요.

Route 53 콘솔을 사용하여 프라이빗 호스팅 영역을 생성하려면

1. Route 53 호스팅 영역과 연결할 각 VPC에 대해 다음과 같은 VPC 설정을 `true`로 변경합니다.

   - `enableDnsHostnames`
   - `enableDnsSupport`

   자세한 내용은 Amazon VPC 사용 설명서의 VPC에 대한 DNS 지원 업데이트를 참조하세요.
2. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
3. Route 53를 처음 사용하는 경우 시작하기(Get started)를 선택합니다.

   Route 53를 이미 사용하고 있는 경우 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
4. 호스팅 영역 생성(Create hosted zone)을 선택합니다.
5. 프라이빗 호스팅 영역 생성(Create private hosted zone) 창에서 도메인 이름과 함께 필요한 설명을 입력합니다.

a-z, 0-9, -(하이픈) 이외의 문자를 지정하는 방법과 국제 도메인 이름을 지정하는 방법은 다음(DNS 도메인 이름 형식)을 참조하십시오.

6. 유형(Type) 목록에서 프라이빗 호스팅 영역(Private hosted zone)을 선택합니다.
7. VPC ID 목록에서 호스팅 영역과 연결할 VPC를 선택합니다.

> **Note**
>
> 콘솔에 다음과 같은 메시지가 표시되면 동일한 VPC 내에서 다른 호스팅 영역과 동일한 네임스페이스를 사용하는 호스팅 영역과 연결하는 것을 의미합니다.
> "충돌하는 도메인이 이미 지정된 VPC 또는 위임 세트와 연결되어 있습니다."
> 예를 들어 호스팅 영역 A와 호스팅 영역 B 둘 다 동일한 도메인 이름(예: `example.com`)을 갖는 경우 두 호스팅 영역을 모두 동일한 VPC와 연결할 수는 없습니다.

8. 호스팅 영역 생성(Create hosted zone)을 선택합니다.

프라이빗 호스팅 영역 나열

Amazon Route 53 콘솔을 사용하여 현재 AWS 계정으로 생성한 모든 호스팅 영역을 나열할 수 있습니다. Route 53 API를 사용하여 호스팅 영역을 나열하는 방법에 대한 자세한 내용은 Amazon Route 53 API 참조의 ListHostedZones를 참조하세요.

AWS 계정과 연결된 호스팅 영역을 나열하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.

   호스팅 영역 페이지에는 현재 AWS 계정을 사용하여 생성된 모든 호스팅 영역의 목록이 자동으로 표시됩니다. [Type] 열의 정보로 호스팅 영역이 프라이빗인지 혹은 퍼블릭인지 알 수 있습니다. 열 머리글을 선택하여 모든 프라이빗 호스팅 영역 및 모든 퍼블릭 호스팅 영역을 그룹화합니다.

더 많은 VPC를 프라이빗 호스팅 영역에 연결

동일한 AWS 계정을 사용하여 호스팅 영역과 VPCs를 생성한 경우 Amazon Route 53 콘솔을 사용하여 더 많은 VPCs를 프라이빗 호스팅 영역과 연결할 수 있습니다.

> **Important**
>
> 한 계정에서 생성한 VPC를 다른 계정에서 생성한 프라이빗 호스팅 영역과 연결하려면 먼저 연결 권한을 부여해야 합니다. 또한 연결 권한을 부여하거나 VPC와 호스팅 영역을 연결하는 경우 AWS 콘솔을 사용할 수 없습니다. 자세한 내용은 Amazon VPC와 다른 AWS 계정에서 생성한 프라이빗 호스팅 영역 연결 섹션을 참조하세요.

Route 53 API를 사용하여 더 많은 VPC를 프라이빗 호스팅 영역에 연결하는 방법에 대한 자세한 내용은 Amazon Route 53 API 참조의 AssociateVPCWithHostedZone을 참조하세요.

Route 53 콘솔을 사용하여 프라이빗 호스팅 영역에 VPC를 추가로 연결하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
3. VPC를 추가로 연결할 프라이빗 호스팅 영역의 라디오 버튼을 선택합니다.
4. 편집을 선택합니다.
5. VPC 추가를 선택합니다.
6. 이 호스팅 영역과 연결할 VPC의 ID 및 리전을 선택합니다.
7. 이 호스팅 영역에 VPC를 더 많이 연결하려면 5단계 및 6단계를 반복합니다.
8. Save changes(변경 사항 저장)를 선택합니다.

Amazon VPC와 다른 AWS 계정에서 생성한 프라이빗 호스팅 영역 연결

한 AWS 계정으로 생성한 VPC를 다른 계정으로 생성한 프라이빗 호스팅 영역과 연결하려면 다음 절차를 수행합니다.

Amazon VPC와 다른 AWS 계정과 생성한 프라이빗 호스팅 영역을 연결하려면

1. 호스팅 영역을 생성한 계정에서 다음 방법 중 한 가지를 사용하여 VPC와 프라이빗 호스팅 영역의 연결 권한을 부여합니다.
   - AWS CLI - AWS CLI 명령 참조의 create-vpc-association-authorization을 참조하세요.
   - AWS SDK 또는 AWS Tools for Windows PowerShell - 설명서 페이지에서 해당 AWS설명서를 참조하세요.

- Amazon Route 53 API - Amazon Route 53 API 참조의 CreateVPCAssociationAuthorization 참조

다음 사항에 유의하세요.

- 한 계정에서 생성한 다수의 VPC를 다른 계정에서 생성한 호스팅 영역과 연결하려면 각 VPC마다 권한 부여 요청을 하나씩 제출해야 합니다.
- 연결 권한을 부여할 때는 호스팅 영역 ID를 지정해야 합니다. 따라서 이미 존재하는 프라이빗 호스팅 영역이어야 합니다.
- VPC와 프라이빗 호스팅 영역의 연결 권한을 부여하거나, 둘을 서로 연결하는 경우 Route 53 콘솔을 사용할 수 없습니다.

2. VPC를 생성한 계정에서 VPC와 호스팅 영역을 연결합니다. 연결 권한 부여와 마찬가지로 AWS SDK, Tools for Windows PowerShell AWS CLI, 또는 Route 53 API를 사용할 수 있습니다. 예를 들어 API를 사용할 경우에는 AssociateVPCWithHostedZone 작업을 사용하십시오.
3. 권장 사항 – VPC와 호스팅 영역을 연결할 수 있는 권한을 삭제합니다. 권한을 삭제하더라도 연결에는 아무런 영향도 미치지 않으며, 오히려 향후 VPC와 호스팅 영역을 다시 연결하는 일을 방지할 수 있습니다. VPC와 호스팅 영역을 다시 연결하려면 이번 절차에서 1 및 2단계를 반복해야 하기 때문입니다.

> **Important**
>
> `ListHostedZonesByVPC`는 VPC가 지정된 호스팅 영역을 반환하고 `GetHostedZone` API는 호스팅 영역에 연결된 VPC를 반환합니다. 이러한 API는 `AssociateVPCWithHostedZone` API에 의해 생성되거나 프라이빗 호스팅 영역이 생성될 때 호스팅 영역과 VPC 연결만 고려합니다. VPC에 대한 호스팅 영역 연결의 전체 목록을 보려면 ListProfileResourceAssociations를 호출합니다.

> **Note**
>
> 생성 가능한 최대 권한 수는 엔터티에 대한 할당량 단원을 참조하십시오.

프라이빗 호스팅 영역에서 VPC 연결 해제

Amazon Route 53 콘솔을 사용하여 프라이빗 호스팅 영역에서 VPC를 연결 해제할 수 있습니다. 이렇게 하면 Route 53가 VPC에서 시작되는 DNS 쿼리에 대해 호스팅 영역의 레코드를 사용하여 트래픽 라우팅을 중지합니다. 예를 들어 example.com 호스팅 영역이 VPC와 연결되어 있는 상태에서 해당 VPC에서 호스팅 영역을 연결 해제하면 Route 53가 example.com 또는 example.com 호스팅 영역의 다른 레코드에 대한 DNS 쿼리 해석을 중지합니다.

> **Note**
>
> 프라이빗 호스팅 영역에서 마지막 VPC의 연결은 해제할 수 없습니다. 해당 VPC의 연결을 해제하려면 먼저 다른 VPC를 호스팅 영역과 연결해야 합니다.

프라이빗 호스팅 영역에서 VPC를 연결 해제하는 방법

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
3. 하나 이상의 VPC를 연결 해제할 프라이빗 호스팅 영역의 라디오 버튼을 선택합니다.
4. 편집을 선택합니다.
5. 이 호스팅 영역에서 연결을 해제할 VPC 옆에 표시된 VPC 제거를 선택합니다.
6. Save changes(변경 사항 저장)를 선택합니다.

프라이빗 호스팅 영역 삭제

이 섹션에서는 Amazon Route 53 콘솔을 사용하여 프라이빗 호스팅 영역을 삭제하는 방법을 설명합니다.

기본 SOA 및 NS 레코드 이외의 레코드가 없는 경우에만 프라이빗 호스팅 영역을 삭제할 수 있습니다. 호스팅 영역에 다른 레코드가 포함되어 있는 경우, 호스팅 영역을 삭제하기 전에 이를 삭제해야 합니다. 이를 통해 레코드를 포함하고 있는 호스팅 영역을 실수로 삭제하는 일을 방지할 수 있습니다.

주제

- 다른 서비스에서 생성한 프라이빗 호스팅 영역 삭제
- Route 53 콘솔을 사용하여 프라이빗 호스팅 영역 삭제

다른 서비스에서 생성한 프라이빗 호스팅 영역 삭제

프라이빗 호스팅 영역이 다른 서비스에서 생성된 경우에는 Route 53 콘솔을 사용하여 삭제할 수 없습니다. 대신 다른 서비스에 대한 해당 프로세스를 사용해야 합니다.

- AWS Cloud Map - 프라이빗 DNS 네임스페이스를 생성할 때 AWS Cloud Map 생성한 호스팅 영역을 삭제하려면 네임스페이스를 삭제합니다.는 호스팅 영역을 자동으로 AWS Cloud Map 삭제합니다. 자세한 내용은 AWS Cloud Map 개발자 안내서의 네임스페이스 삭제를 참조하세요.
- Amazon Elastic Container Service(Amazon ECS) 서비스 검색 – 서비스 검색을 사용하여 서비스를 만들 때 Amazon ECS에서 생성한 퍼블릭 호스팅 영역을 삭제하려면 네임스페이스를 사용하는 Amazon ECS 서비스를 삭제하고 해당 네임스페이스를 삭제하세요. 자세한 내용은 Amazon Elastic Container Service 개발자 안내서의 서비스 삭제를 참조하세요.

Route 53 콘솔을 사용하여 프라이빗 호스팅 영역 삭제

Route 53 콘솔을 사용하여 프라이빗 호스팅 영역을 삭제하려면 다음 절차를 따릅니다.

Route 53 콘솔을 사용하여 프라이빗 호스팅 영역을 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 삭제할 호스팅 영역에 NS 및 SOA 레코드만 포함되어 있는지 확인합니다. 다른 레코드가 있는 경우 다음과 같이 삭제합니다.

   a. 삭제할 호스팅 영역의 이름을 선택합니다.

   b. 레코드(Record) 페이지에서 레코드 목록에 유형(Type) 열의 값이 NS 또는 SOA 이외의 레코드가 포함되어 있는 경우, 해당 행을 선택한 다음 삭제(Delete)를 선택합니다.

      연속된 여러 레코드를 선택하려면 첫 번째 행을 선택한 다음, [Shift] 키를 누른 상태에서 마지막 행을 선택합니다. 비연속적인 여러 레코드를 선택하려면 첫 번째 행을 선택한 다음, [Ctrl] 키를 누른 상태에서 나머지 행을 선택합니다.
3. [Hosted Zones] 페이지에서 삭제할 호스팅 영역의 행을 선택합니다.
4. Delete(삭제)를 선택합니다.
5. 확인 키를 입력하고 삭제(Delete)를 선택합니다.

VPC 권한

VPC 권한은 자격 증명 및 액세스 관리(IAM) 정책 조건을 사용하여 AssociateVPCWithHostedZone, DisassociateVPCFromHostedZone, CreateVPCAssociationAuthorization, DeleteVPCAssociationAuthorization, CreateHostedZone, ListHostedZonesByVPC API를 사용할 때 VPC에 대한 세분화된 권한을 설정할 수 있습니다.

IAM 정책 조건인를 `route53:VPCs`사용하면 다른 AWS 사용자에게 세분화된 관리 권한을 부여할 수 있습니다. 이렇게 하면 호스팅 영역을 연결하거나, 호스팅 영역을 연결 해제하거나, VPC 연결 권한을 생성하거나, VPC 연결 권한을 삭제하거나, 호스팅 영역을 생성하거나, 호스팅 영역을 나열할 수 있는 권한을 다른 사람에게 부여할 수 있습니다.

- 단일 VPC.
- 동일한 리전 내의 모든 VPC.
- 다중 VPC.

VPC 권한에 대한 자세한 내용은 IAM 정책 조건을 사용하여 세분화된 액세스 제어 구현 섹션을 참조하세요.

AWS 사용자를 인증하는 방법은 섹션을 참조ID를 통한 인증하고 Route 53 리소스에 대한 액세스를 제어하는 방법은 섹션을 참조하세요액세스 제어.

호스팅 영역을 다른 AWS 계정으로 마이그레이션

호스팅 영역을 한 AWS 계정에서 다른 계정으로 마이그레이션하려는 경우 이전 호스팅 영역의 레코드를 프로그래밍 방식으로 나열하고 출력을 편집한 다음 편집된 출력을 사용하여 새 호스팅 영역에서 프로그래밍 방식으로 레코드를 생성할 수 있습니다. 다음 사항에 유의하세요.

- 레코드가 몇 개밖에 없는 경우에는 Route 53 콘솔을 사용하여 새 호스팅 영역에 레코드를 생성할 수도 있습니다. 자세한 내용은 Amazon Route 53 콘솔을 사용하여 레코드 생성 단원을 참조하십시오.
- 일부 절차에서는 AWS Command Line Interface ()를 사용합니다AWS CLI. AWS SDKs, Amazon Route 53 API 또는 중 하나를 사용하여 이러한 절차를 수행할 수도 있습니다 AWS Tools for Windows PowerShell. 이 주제에서는 호스팅 영역 수가 적기 AWS CLI 때문에를 사용합니다.
- 이 프로세스를 이용해 기존 호스팅 영역과 이름은 다르지만 같은 레코드를 가진 새 호스팅 영역에 레코드를 생성할 수도 있습니다.
- 트래픽을 트래픽 정책 인스턴스로 라우팅하는 별칭 레코드를 마이그레이션할 수 없습니다.

주제

1단계: 설치 또는 업그레이드 AWS CLI

다운로드, 설치 및 구성에 대한 자세한 내용은 AWS Command Line Interface 사용 설명서를 AWS CLI 참조하세요.

> **Note**
>
> 호스팅 영역을 생성한 계정과 호스팅 영역을 마이그레이션할 대상 계정을 모두 사용 중일 때는 CLI를 사용할 수 있도록 구성하십시오. 자세한 내용은 AWS Command Line Interface 사용 설명서의 구성을 참조하세요.

이미를 사용하고 있는 경우 CLI 명령이 최신 Route 53 기능을 지원하도록 CLI의 최신 버전으로 업그레이드하는 AWS CLI것이 좋습니다.

2단계: 새 호스팅 영역 생성

다음 절차에서는 Route 53 콘솔을 사용하여 마이그레이션하려는 대상 호스팅 영역을 생성하는 방법을 설명합니다.

> **Note**
>
> Route 53는 새 호스팅 영역에 4개의 이름 서버 세트를 새로 할당합니다. 호스팅 영역을 다른 AWS 계정으로 마이그레이션한 후에는 도메인 등록을 업데이트하여 새 호스팅 영역의 이름 서버를 사용해야 합니다. 본 프로세스 후반부에 이 단계에 대해 다시 알려드리겠습니다.

다른 계정을 사용하여 새 호스팅 영역을 생성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.

   호스팅 영역을 마이그레이션하려는 대상 계정에 대해 계정 자격 증명으로 로그인하십시오.
2. 호스팅 영역 생성. 자세한 내용은 퍼블릭 호스팅 영역 생성 섹션을 참조하세요.
3. 호스팅 영역 ID를 기록해 둡니다. 경우에 따라 이 프로세스 후반부에 이 정보가 필요할 것입니다.
4. Route 53 콘솔에서 로그아웃합니다.

3단계: 마이그레이션할 레코드를 포함한 파일 만들기

레코드를 한 호스팅 영역에서 다른 호스팅 영역으로 마이그레이션하려면 마이그레이션할 레코드가 들어 있는 파일을 만들고 편집한 후 그 파일을 사용해 새 호스팅 영역에 레코드를 만드십시오. 다음 절차에 따라 파일을 만드십시오.

마이그레이션할 레코드를 포함한 파일을 만드는 방법

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.

   마이그레이션하려는 호스팅 영역을 생성한 계정에 대해 계정 자격 증명으로 로그인하십시오.
2. 마이그레이션할 호스팅 영역의 호스팅 영역 ID를 다음 절차에 따라 받으십시오.

   a. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.

   b. 마이그레이션하려는 호스팅 영역을 찾습니다. 호스팅 영역이 많은 경우 정확한 도메인 이름(Exact domain name)을 선택하고, 호스팅 영역 이름을 입력하고 Enter를 눌러 목록을 필터링합니다.

   c. [Hosted zone ID] 열의 값을 얻습니다.
3. 다음 명령 실행:

```
aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id > path-to-output-file
```

다음 사항에 유의하세요.

- *hosted-zone-id*의 경우 이 절차의 2단계에서 받은 호스팅 영역의 ID를 지정하십시오.
- *path-to-output-file*의 경우 출력을 저장하고 싶은 디렉터리 경로와 파일 이름을 지정하십시오.
- > 문자를 사용해 지정한 파일로 출력을 보낼 수 있습니다.
- 는 100개가 넘는 레코드가 포함된 호스팅 영역의 페이지 매김을 AWS CLI 자동으로 처리합니다. 자세한 내용은 AWS Command Line Interface 사용 설명서의 AWS 명령줄 인터페이스의 페이지 매김 옵션 사용을 참조하세요.

  다른 프로그래밍 방법을 사용하여 AWS SDKs 중 하나와 같은 레코드를 나열하는 경우 결과 페이지당 최대 100개의 레코드를 얻을 수 있습니다. 호스팅 영역에 100개를 초과하는 레코드가 있을 경우 모든 레코드를 나열하려면 복수의 요청을 제출해야 합니다.
- 6.0 이전 버전의 Windows PowerShell에서 명령을 실행하려면 다음 구문을 사용하십시오.

  ```
  aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id | Out-File path-to-output-file -Encoding utf8
  ```

예를 들어 Windows AWS CLI 컴퓨터에서를 실행하는 경우 다음 명령을 실행할 수 있습니다.

```
aws route53 list-resource-record-sets --hosted-zone-id ZOLDZONE12345 > c:\temp\list-records-ZOLDZONE12345.txt
```

Windows PowerShell 6.0 이전 버전의 Windows AWS CLI 컴퓨터에서를 실행하는 경우 다음 명령을 실행할 수 있습니다.

```
$output = aws route53 list-resource-record-sets --hosted-zone-id <hosted-zone-id>;
 $mypath = <output-path ;
[System.IO.File]::WriteAllLines($mypath,$output)
```

4. 이 출력의 복사본을 만듭니다. 새 호스팅 영역에서 레코드를 생성한 후에는 새 호스팅 영역에서 명령을 실행 AWS CLI `list-resource-record-sets`하고 두 출력을 비교하여 모든 레코드가 생성되었는지 확인하는 것이 좋습니다.

4단계: 마이그레이션하려는 레코드 편집

이전 절차에서 생성한 파일의 형식은 새 호스팅 영역에서 레코드를 생성하는 데 사용하는 `change-resource-record-sets` 명령에 필요한 AWS CLI 형식과 비슷합니다. 다만 파일을 약간 편집해야 합니다. 모든 레코드에 변경 사항 중 몇 가지를 적용해야 합니다. 쓸만한 텍스트 편집기에서 검색 및 바꾸기 기능을 사용하여 변경할 수 있습니다.

3단계: 마이그레이션할 레코드를 포함한 파일 만들기에서 만든 파일의 복사본을 열고 다음과 같이 변경하십시오.

- 출력 내용 맨 위에 있는 첫 두 줄을 삭제하십시오.

```
{
    "ResourceRecordSets": [
```

- NS 및 SOA 레코드와 관련된 줄을 삭제하십시오. 새 호스팅 영역에 이미 해당 레코드가 있습니다.
- 선택 사항 - `Comment` 요소를 추가합니다.
- `Changes` 요소를 추가합니다.
- 각 레코드에 대해 `Action` 및 `ResourceRecordSet` 요소를 추가하십시오.
- JSON 코드를 유효하게 만들려면 필요에 따라 여는 중괄호와 닫는 중괄호(`{ }`)를 추가하십시오.

> **Note**
>
> 중괄호와 대괄호가 알맞은 곳에 있는지 확인하려면 JSON 검사기를 사용할 수 있습니다. 온라인 JSON 검사기를 찾으려면 인터넷에서 "`json validator`"를 검색하십시오.

- 호스팅 영역에 같은 호스팅 영역에 있는 다른 레코드를 참조하는 별칭이 포함되어 있을 경우 다음과 같이 변경하십시오.
  - 호스팅 영역의 ID를 새 호스팅 영역의 ID로 변경하십시오.

> **Important**
>
> 별칭 레코드가 다른 리소스(예: 로드 밸런서)를 가리키는 경우 호스팅 영역 ID를 도메인의 호스팅 영역 ID로 변경하지 마세요. 호스팅 영역 ID를 실수로 변경하는 경우 호스팅 영역 ID를 도메인의 호스팅 영역 ID가 아닌 리소스 자체의 호스팅 영역 ID로 롤백합니다. 해당 호스팅 영역 ID는 리소스가 생성된 AWS 콘솔에 있을 수 있습니다.

- 파일의 맨 아래로 별칭 레코드를 이동합니다. Route 53는 별칭 레코드가 참조하는 레코드를 먼저 생성해야 별칭 레코드를 생성할 수 있습니다.

  > **Important**
  >
  > 하나 이상의 별칭 레코드가 다른 별칭 레코드를 참조하는 경우 별칭 대상인 레코드는 파일에서 참조하는 별칭 레코드 앞에 나와야 합니다. 예를 들어, `alias.example.com`이 `alias.alias.example.com`의 별칭 대상인 경우 `alias.example.com`이 파일에서 먼저 나와야 합니다.

- 트래픽을 트래픽 정책 인스턴스로 라우팅하는 별칭 레코드를 모두 삭제하십시오. 이후에 레코드를 다시 생성할 수 있도록 기록해 두십시오.

- 이 프로세스를 사용하여 다른 이름을 가진 호스팅 영역에 레코드를 생성할 수 있습니다. 출력에 있는 모든 레코드에 대해, Name 요소의 도메인 이름 부분을 새 호스팅 영역의 이름으로 변경하십시오. 예를 들어, example.com 호스팅 영역에 레코드를 나열하고 example.net 호스팅 영역에 레코드를 생성하려는 경우 모든 레코드 이름의 example.com 부분을 example.net으로 변경하십시오.

  시작:

  - `"Name": "example.com."`
  - `"Name": "www.example.com."`

  끝:

  - `"Name": "example.net."`
  - `"Name": "www.example.net."`

다음 예제에서는 example.com에 대한 호스팅 영역을 위한 레코드의 편집된 버전을 보여줍니다. 빨간색 기울임꼴 텍스트가 새로운 내용입니다.

```
{
    "Comment": "string",
    "Changes": [
        {
            "Action": "CREATE",
            "ResourceRecordSet":{
                "ResourceRecords": [
                    {
                        "Value": "192.0.2.4"
                    },
```

```
                    {
                        "Value": "192.0.2.5"
                    },
                    {
                        "Value": "192.0.2.6"
                    }
                ],
                "Type": "A",
                "Name": "route53documentation.com.",
                "TTL": 300
            }
        },
        {
            "Action": "CREATE",
            "ResourceRecordSet":{
                "AliasTarget": {
                    "HostedZoneId": "Z3BJ6K6RIION7M",
                    "EvaluateTargetHealth": false,
                    "DNSName": "s3-website-us-west-2.amazonaws.com."
            },
                "Type": "A",
                "Name": "www.route53documentation.com."
            }
        }
    ]
}
```

5단계: 큰 파일을 여러 작은 파일로 분할

레코드가 많이 있거나 값이 많은 레코드(예: 많은 IP 주소)가 있을 경우 파일을 여러 작은 파일로 분할해야 할 수 있습니다. 다음은 최댓값입니다.

- 각 파일에는 최대 1,000개의 레코드가 포함될 수 있습니다.
- 모든 `Value` 요소에서 값의 최대 총 길이는 32,000바이트입니다.

6단계: 새 호스팅 영역에 레코드 생성

새 호스팅 영역에서 레코드를 생성하려면 다음 AWS CLI 명령을 사용합니다.

```
aws route53 change-resource-record-sets --hosted-zone-id id-of-new-hosted-zone --
change-batch file://path-to-file-that-contains-records
```

예시:

```
aws route53 change-resource-record-sets --hosted-zone-id ZNEWZONE1245 --change-batch
 file://c:/temp/change-records-ZNEWZONE1245.txt
```

트래픽을 트래픽 정책 인스턴스로 라우팅하는 별칭 레코드를 모두 삭제한 경우 Route 53 콘솔을 사용하여 별칭 레코드를 다시 생성하세요. 자세한 내용은 Amazon Route 53 콘솔을 사용하여 레코드 생성 섹션을 참조하세요.

7단계: 기존 호스팅 영역과 새 호스팅 영역의 레코드 비교

새 호스팅 영역에 모든 레코드를 올바로 생성했음을 확인하려면 새 호스팅 영역에 레코드를 나열하고 기존 호스팅 영역의 레코드 목록과 출력 내용을 비교하는 것이 좋습니다. 이렇게 하려면 다음과 같이 합니다.

기존 호스팅 영역과 새 호스팅 영역의 레코드 비교 방법

1. 다음 명령 실행:

   ```
   aws route53 list-resource-record-sets --hosted-zone-id hosted-zone-id --output json
    > path-to-output-file
   ```

   다음 값을 지정하세요.

   - *hosted-zone-id*의 경우 새 호스팅 영역의 ID를 지정하십시오.
   - *path-to-output-file*의 경우 출력을 저장하고 싶은 디렉터리 경로와 파일 이름을 지정하십시오. 3단계: 마이그레이션할 레코드를 포함한 파일 만들기에 사용한 파일 이름과 다른 파일 이름을 사용하십시오. 다른 파일 이름을 사용해야 새 파일이 기존 파일을 덮어쓰지 않습니다.
   - > 문자를 사용해 지정한 파일로 출력을 보낼 수 있습니다.

   예를 들어, Windows 컴퓨터를 사용 중인 경우 다음 명령을 실행할 수도 있습니다.

   ```
   aws route53 list-resource-record-sets --hosted-zone-id ZNEWZONE67890 --output json
    > c:\temp\list-records-ZNEWZONE67890.txt
   ```

2. 출력을 3단계: 마이그레이션할 레코드를 포함한 파일 만들기의 출력과 비교하십시오.

   NS 및 SOA 레코드의 값과 4단계: 마이그레이션하려는 레코드 편집에서 변경한 사항(예: 다른 호스팅 영역 ID 또는 도메인 이름) 외에도 이 두 출력 내용이 같아야 합니다.

3. 새 호스팅 영역의 레코드가 기존 호스팅 영역의 레코드와 일치하지 않을 경우 다음 중 하나를 수행할 수 있습니다.

   - Route 53 콘솔을 사용하여 사소한 사항을 수정하세요. 자세한 내용은 레코드 편집 섹션을 참조하세요.
   - 다수의 레코드가 누락된 경우 누락된 레코드가 포함된 새 텍스트 파일을 만든 다음 6단계: 새 호스팅 영역에 레코드 생성 항목을 반복하십시오.
   - 새 호스팅 영역에서 NS 및 SOA 레코드를 제외한 모든 레코드를 삭제하고 다음 단계를 반복하십시오.
     - 4단계: 마이그레이션하려는 레코드 편집
     - 5단계: 큰 파일을 여러 작은 파일로 분할
     - 6단계: 새 호스팅 영역에 레코드 생성
     - 7단계: 기존 호스팅 영역과 새 호스팅 영역의 레코드 비교

8단계: 도메인 등록을 업데이트하여 새 호스팅 영역을 위한 이름 서버 사용

새 호스팅 영역에서 레코드 생성을 마치면 새 호스팅 영역을 위한 이름 서버를 사용하도록 도메인 등록의 이름 서버를 변경하십시오.

> **Important**
>
> 새 호스팅 영역을 위한 이름 서버를 사용하도록 도메인 등록을 업데이트하지 않으면 Route 53가 계속 기존 호스팅 영역을 사용하여 도메인에 대한 트래픽을 라우팅하게 됩니다. 도메인 등록의 이름 서버를 업데이트하지 않고 기존 호스팅 영역을 삭제하면 인터넷에서 해당 도메인에 접속할 수 없게 됩니다. 도메인 등록의 이름 서버를 업데이트하지 않고 새 호스팅 영역에서 레코드를 추가, 업데이트 또는 삭제할 경우 트래픽이 그러한 변경 사항을 기반으로 라우팅되지 않습니다.

자세한 내용은 Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정 섹션을 참조하세요.

> **Note**
>
> 사용 중인 도메인을 위한 DNS 서비스를 마이그레이션하는 프로세스를 사용하든, 비활성 도메인을 위한 프로세스를 사용하든, 이미 새 호스팅 영역을 생성하고 그 호스팅 영역에 레코드를 생성했으므로 다음 단계를 건너뛸 수 있습니다.

- 1단계: 현재 DNS 서비스 공급자로부터 현재 DNS 구성 가져오기
- 2단계: 호스팅 영역 생성
- 3단계: 레코드 만들기

9단계: DNS 해석기가 새 호스팅 영역을 사용하기 시작할 때까지 기다리기

도메인이 사용 중인 경우(예: 사용자가 도메인 이름을 사용하여 웹 사이트를 검색하거나 웹 애플리케이션에 액세스하는 경우) DNS Resolver가 현재 DNS 서비스 공급자에 의해 제공된 이름 서버의 이름을 캐시했습니다. 몇 분 전에 그 정보를 캐시한 DNS 해석기는 최대 이틀 동안 해당 정보를 저장할 것입니다.

> **Note**
>
> 이전 호스팅 영역에 표시되지 않는 새 호스팅 영역에서 레코드를 만든 경우, 해석기가 새 호스팅 영역의 이름 서버를 사용하기 시작할 때까지 사용자는 새 레코드를 사용하여 리소스에 액세스할 수 없습니다. 예를 들어 인터넷 트래픽을 웹사이트로 라우팅해야 하는 새 호스팅 영역에 test.example.com이라는 레코드를 생성한다고 가정합시다. 이전 호스팅 영역에 레코드가 표시되지 않으면 해석기가 새 호스팅 영역을 사용하기 시작할 때까지 웹 브라우저에 test.example.com을 입력할 수 없습니다.

이전 호스팅 영역을 삭제하기 전에 호스팅 영역을 다른 AWS 계정으로 마이그레이션이 완료되었는지 확인하려면 새 호스팅 영역에 이름 서버를 사용하도록 도메인 등록을 업데이트한 후 2일 동안 기다립니다.

> **Note**
>
> 기본 TTL 값은 172,800초(2일)입니다. 이 값을 더 짧게 변경할 수 있습니다. 자세한 내용은 TTL(초) 단원을 참조하십시오.

이틀 후에 TTL이 만료되고 해석기가 도메인에 대한 이름 서버를 요청한 후, 해석기는 현재 이름 서버를 얻습니다. 또한 Resolver 쿼리 로깅을 활성화하여 새 호스팅 영역에서 쿼리를 모니터링할 수도 있습니다. Resolver 쿼리 로깅 요금에 대한 자세한 내용은 CloudWatch 요금을 참조하세요.

10단계: (선택 사항) 기존 호스팅 영역 삭제

기존 호스팅 영역이 이제는 필요하지 않다고 확신할 때는 이를 선택적으로 삭제할 수 있습니다.

> **Important**
>
> 새 호스팅 영역에 대한 이름 서버를 사용하도록 도메인 등록을 업데이트한 후 적어도 48시간 동안 이전 호스팅 영역이나 해당 호스팅 영역에서 레코드를 삭제하지 마십시오. DNS 해석기가 해당 호스팅 영역의 레코드 사용을 중지하기 전에 이전의 호스팅 영역을 삭제하면, 해석기가 새 호스팅 영역을 사용하기 시작할 때까지 인터넷에서 도메인을 사용할 수 없게 됩니다.

호스팅 영역은 기본 NS 및 SOA 레코드를 제외하고는 비어 있어야 합니다. 기존 호스팅 영역에 많은 레코드가 포함되어 있는 경우 콘솔을 사용하여 레코드를 삭제하려면 시간이 오래 걸릴 수 있습니다. 이때 선택할 수 있는 한 가지 옵션이 다음 단계를 수행하는 방법입니다.

1. 4단계: 마이그레이션하려는 레코드 편집에서 편집된 파일의 다른 복사본을 만드십시오.
2. 파일 복사본에서 모든 레코드에 대해 `"Action": "CREATE"`를 `"Action": "DELETE"`로 변경하십시오.
3. 다음 AWS CLI 명령을 사용하여 레코드를 삭제합니다.

   ```
   aws route53 change-resource-record-sets --hosted-zone-id id-of-old-hosted-zone --
   change-batch file:///path-to-file-that-contains-records
   ```

   > **Important**
   >
   > 호스팅 영역 ID에 대해 지정하는 값이 새 호스팅 영역의 ID가 아니라 기존 호스팅 영역의 ID임을 확인하십시오.

4. 나머지 레코드 전부와 호스팅 영역을 삭제하십시오.

   a. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.

      기존 호스팅 영역을 생성한 계정에 대해 계정 자격 증명으로 로그인하십시오.

   b. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.

c. 기존 호스팅 영역의 이름을 선택하십시오. 호스팅 영역이 많은 경우 정확한 도메인 이름(Exact domain name)을 선택하고, 호스팅 영역 이름을 입력하고 Enter를 눌러 목록을 필터링합니다.

d. 호스팅 영역에 기본 NS 및 SOA 레코드 이외의 레코드(예: 트래픽을 트래픽 정책 인스턴스로 라우팅하는 별칭 레코드)가 포함된 경우, 해당 확인란을 선택하고 삭제(Delete)를 선택합니다.

e. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.

f. 호스팅 영역 목록에서 삭제할 호스팅 영역의 라디오 버튼을 선택하십시오.

g. Delete(삭제)를 선택합니다.

레코드 작업

example.com과 같은 도메인에 대해 호스팅 영역을 생성한 후, 트래픽을 도메인에 라우팅하는 방식을 Domain Name System(DNS)에 알려줄 레코드를 생성합니다.

예를 들어, DNS가 다음 작업을 수행하도록 만드는 레코드를 생성할 수도 있습니다.

- example.com에 대한 인터넷 트래픽을 데이터 센터에 있는 호스트의 IP 주소로 라우팅하기.
- 도메인에 대한 이메일(ichiro@example.com)을 메일 서버(mail.example.com)로 라우팅하기.
- operations.tokyo.example.com이라는 하위 도메인에 대한 트래픽을 다른 호스트의 IP 주소로 라우팅하기.

각 레코드에는 도메인 또는 하위 도메인의 이름, 레코드 유형(예: MX 유형의 레코드는 이메일을 라우팅), 그리고 레코드 유형에 해당되는 다른 정보(MX 레코드의 경우, 1개 이상의 메일 서버의 호스트 이름과 각 서버에 대한 우선 순위)가 담겨 있습니다. 다양한 레코드 유형에 대한 자세한 내용은 지원되는 DNS 레코드 유형 단원을 참조하십시오.

호스팅 영역에 있는 각 레코드의 이름은 반드시 호스팅 영역의 이름으로 끝나야 합니다. 예를 들어, example.com 호스팅 영역은 www.example.com 및 accounting.tokyo.example.com 하위 도메인에 대한 레코드를 포함할 수 있지만 www.example.ca 하위 도메인에 대한 레코드는 포함할 수 없습니다.

> **Note**
>
> 복잡한 라우팅 구성에 대한 레코드를 만들려면 트래픽 흐름 시각적 편집기를 사용하고 구성을 트래픽 정책으로 저장할 수도 있습니다. 그런 다음 동일한 호스팅 영역이나 여러 호스팅 영역의 하나 이상의 도메인 이름(예: example.com) 또는 하위 도메인 이름(예: www.example.com)과 해당 트래픽 정책을 연결할 수 있습니다. 새 구성이 예상대로 수행되지 않을 경우 업데이트

를 롤백할 수도 있습니다. 자세한 내용은 트래픽 흐름을 사용하여 DNS 트래픽 라우팅 단원을 참조하십시오.

Amazon Route 53는 호스팅 영역에 추가하는 레코드에 대해서는 요금을 부과하지 않습니다. 호스팅 영역에 생성할 수 있는 최대 레코드 수에 대한 자세한 내용은 할당량 단원을 참조하십시오.

주제

- 라우팅 정책 선택
- 별칭 또는 비 별칭 레코드 선택
- 지원되는 DNS 레코드 유형
- Amazon Route 53 콘솔을 사용하여 레코드 생성
- 리소스 레코드 세트 권한
- Amazon Route 53 레코드를 생성 또는 편집할 때 지정하는 값
- 영역 파일을 가져와 레코드 생성
- 레코드 편집
- 레코드 삭제
- 레코드 나열

라우팅 정책 선택

레코드를 생성할 때 라우팅 정책을 선택하게 되는데, 이는 Amazon Route 53가 쿼리에 응답하는 방식을 결정합니다.

- 단순 라우팅 정책(Simple routing policy) - 도메인에 대해 특정 기능을 수행하는 하나의 리소스만 있는 경우(예: example.com 웹 사이트의 콘텐츠를 제공하는 하나의 웹 서버)에 사용합니다. 단순 라우팅을 사용하여 프라이빗 호스팅 영역에서 레코드를 생성할 수 있습니다.
- 장애 조치 라우팅 정책(Failover routing policy) - 액티브-패시브 장애 조치를 구성하려는 경우에 사용합니다. 장애 조치 라우팅을 사용하여 프라이빗 호스팅 영역에서 레코드를 생성할 수 있습니다.
- 지리 위치 라우팅 정책(Geolocation routing policy) - 사용자의 위치에 기반하여 트래픽을 라우팅하려는 경우에 사용합니다. 지리적 위치 라우팅을 사용하여 프라이빗 호스팅 영역에서 레코드를 생성할 수 있습니다.

- 지리 근접 라우팅 정책 - 리소스의 위치를 기반으로 트래픽을 라우팅하고 필요에 따라 한 위치의 리소스에서 다른 위치의 리소스로 트래픽을 보내려는 경우에 사용합니다. 지리 근접 라우팅을 사용하여 프라이빗 호스팅 영역에서 레코드를 생성할 수 있습니다.
- 지연 시간 라우팅 정책 - 여러에 리소스가 AWS 리전 있고 트래픽을 최상의 지연 시간을 제공하는 리전으로 라우팅하려는 경우에 사용합니다. 지연 시간 라우팅을 사용하여 프라이빗 호스팅 영역에서 레코드를 생성할 수 있습니다.
- IP 기반 라우팅 정책 - 사용자의 위치에 기반하여 트래픽을 라우팅하고 트래픽이 시작되는 IP 주소가 있는 경우에 사용합니다.
- 다중 응답 라우팅 정책(Multivalue answer routing policy) - Route 53가 DNS 쿼리에 무작위로 선택된 최대 8개의 정상 레코드로 응답하게 하려는 경우에 사용합니다. 다중 값 응답 라우팅을 사용하여 프라이빗 호스팅 영역에서 레코드를 생성할 수 있습니다.
- 가중치 기반 라우팅 정책(Weighted routing policy) - 사용자가 지정하는 비율에 따라 여러 리소스로 트래픽을 라우팅하려는 경우에 사용합니다. 가중치 라우팅을 사용하여 프라이빗 호스팅 영역에서 레코드를 생성할 수 있습니다.

주제

단순 라우팅

단순 라우팅에서는 가중치나 지연 시간 같은 특별한 Route 53 라우팅 없이 표준 DNS 레코드를 구성할 수 있습니다. 단순 라우팅에서는 보통 단일 리소스로 트래픽을 라우팅합니다. 예를 들면 웹 사이트에 대한 웹 서버로 라우팅합니다.

프라이빗 호스팅 영역의 레코드에 단순 라우팅 정책을 사용할 수 있습니다.

Route 53 콘솔에서 단순 라우팅 정책을 선택할 경우 동일한 이름과 유형을 가진 여러 레코드를 만들 수 없지만, 동일 레코드 안에 여러 값(예: 다중 IP 주소)을 지정할 수는 있습니다. (별칭 레코드에 대한 단순 라우팅 정책을 선택하는 경우 현재 호스팅 영역에서 AWS 리소스 하나 또는 레코드 하나만 지정할 수 있습니다.) 한 레코드에 다중 값을 지정한 경우 Route 53가 모든 값을 무작위 순서로 재귀적 해석기로 반환하며, 해석기는 DNS 쿼리를 제출한 클라이언트(웹 브라우저 같은)로 그 값을 반환합니다. 그러면 클라이언트가 값을 하나 선택하고 쿼리를 다시 제출합니다. 간단한 라우팅 정책을 사용하면 여러 IP 주소를 지정할 수 있지만 이러한 IP 주소의 상태는 확인되지 않습니다.

단순 라우팅 정책으로 레코드를 만들 때 지정하는 값에 대한 정보는 다음 주제를 참조하십시오.

- 단순 레코드에 특정한 값
- 단순 별칭 레코드에 특정한 값
- 모든 라우팅 정책에 공통적인 값
- 모든 라우팅 정책의 별칭 레코드에 공통되는 값

장애 조치 라우팅

장애 조치 라우팅은 특정 리소스가 정상일 경우 해당 리소스로 트래픽을 라우팅하고 첫 번째 리소스가 비정상일 경우 다른 리소스로 트래픽을 라우팅합니다. 기본 및 보조 레코드는 웹 사이트로 구성되는 Amazon S3 버킷에서 복잡한 레코드 트리에 이르기까지 그 어느 것에도 트래픽을 라우팅할 수 있습니다. 자세한 내용은 액티브-패시브 장애 조치 단원을 참조하십시오.

프라이빗 호스팅 영역의 레코드에 장애 조치 라우팅 정책을 사용할 수 있습니다.

장애 조치 라우팅 정책으로 레코드를 만들 때 지정하는 값에 대한 정보는 다음 주제를 참조하십시오.

- 장애 조치 레코드에 특정한 값
- 장애 조치 별칭 레코드에 특정한 값
- 모든 라우팅 정책에 공통적인 값
- 모든 라우팅 정책의 별칭 레코드에 공통되는 값

지리적 라우팅

지리적 라우팅을 사용하면 사용자의 지리 위치, 즉 DNS 쿼리가 발생하는 위치를 기반으로 트래픽을 제공하는 리소스를 선택할 수 있습니다. 예를 들어 유럽에서 발생하는 모든 쿼리를 프랑크푸르트 리전에 위치한 Elastic Load Balancing 로드 밸런서로 라우팅할 수 있습니다.

지리적 라우팅을 사용하는 경우, 콘텐츠를 지역화하고 웹 사이트의 일부 또는 전체를 사용자의 언어로 제공할 수 있습니다. 또한 지리적 라우팅을 사용하여 배포권이 있는 위치에서만 콘텐츠를 배포할 수 있도록 제한할 수 있습니다. 또한 예측 가능하고 간편하게 관리할 수 있는 방식으로 엔드포인트 간에 로드를 분산하는 데 사용함으로써, 사용자의 위치가 동일한 엔드포인트에 일관되게 라우팅되도록 할 수도 있습니다.

미국에서는 대륙, 국가 또는 주를 기준으로 지리적 위치를 지정할 수 있습니다. 중복되는 지리 리전에 대해 별도의 레코드를 생성하는 경우(예를 들면, 북미에 하나의 레코드, 캐나다에 하나의 레코드) 우선순위는 가장 작은 지리 지역에 돌아갑니다. 이렇게 하면 한 대륙의 일부 쿼리를 하나의 리소스로 라우팅하고 그 대륙에서 선택된 여러 나라들의 쿼리는 다른 리소스로 라우팅할 수 있습니다. (각 대륙별 국가 목록은 다음(위치)을 참조하십시오).

지리 위치는 IP 주소를 위치에 매핑하는 방식으로 작동합니다. 그러나 일부 IP 주소들은 지리 위치에 매핑되지 않으므로, 7개 대륙 전체를 포괄하는 지리 위치 레코드를 생성한다 해도 Amazon Route 53는 식별할 수 없는 위치에서 온 일부 DNS 쿼리를 수신합니다. 어떤 위치에도 매핑되지 않는 IP 주소로부터 온 쿼리, 그리고 지리 위치 레코드를 생성하지 않은 위치로부터 온 쿼리 모두를 처리하는 기본 레코드를 생성할 수 있습니다. 기본 레코드를 생성하지 않으면, Route 53는 그 위치에서 온 쿼리에 대해 "응답 없음(no answer)"을 반환합니다.

퍼블릭 및 프라이빗 호스팅 영역의 레코드의 지리적 위치 라우팅을 사용할 수 있습니다.

자세한 내용은 Amazon Route 53에서 EDNS0을 사용하여 사용자의 위치를 예측하는 방법 단원을 참조하십시오.

지리적 위치 라우팅 정책으로 레코드를 만들 때 지정하는 값에 대한 정보는 다음 주제를 참조하십시오.

- 지리 위치 레코드에 특정한 값
- 지리 위치 별칭 레코드에 특정한 값
- 모든 라우팅 정책에 공통적인 값
- 모든 라우팅 정책의 별칭 레코드에 공통되는 값

프라이빗 호스팅 영역의 지리적 위치 라우팅

프라이빗 호스팅 영역의 경우 Route 53는 쿼리가 시작된 VPC AWS 리전 의를 기반으로 DNS 쿼리에 응답합니다. 목록은 Amazon EC2 사용 설명서의 리전 및 영역을 AWS 리전참조하세요. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

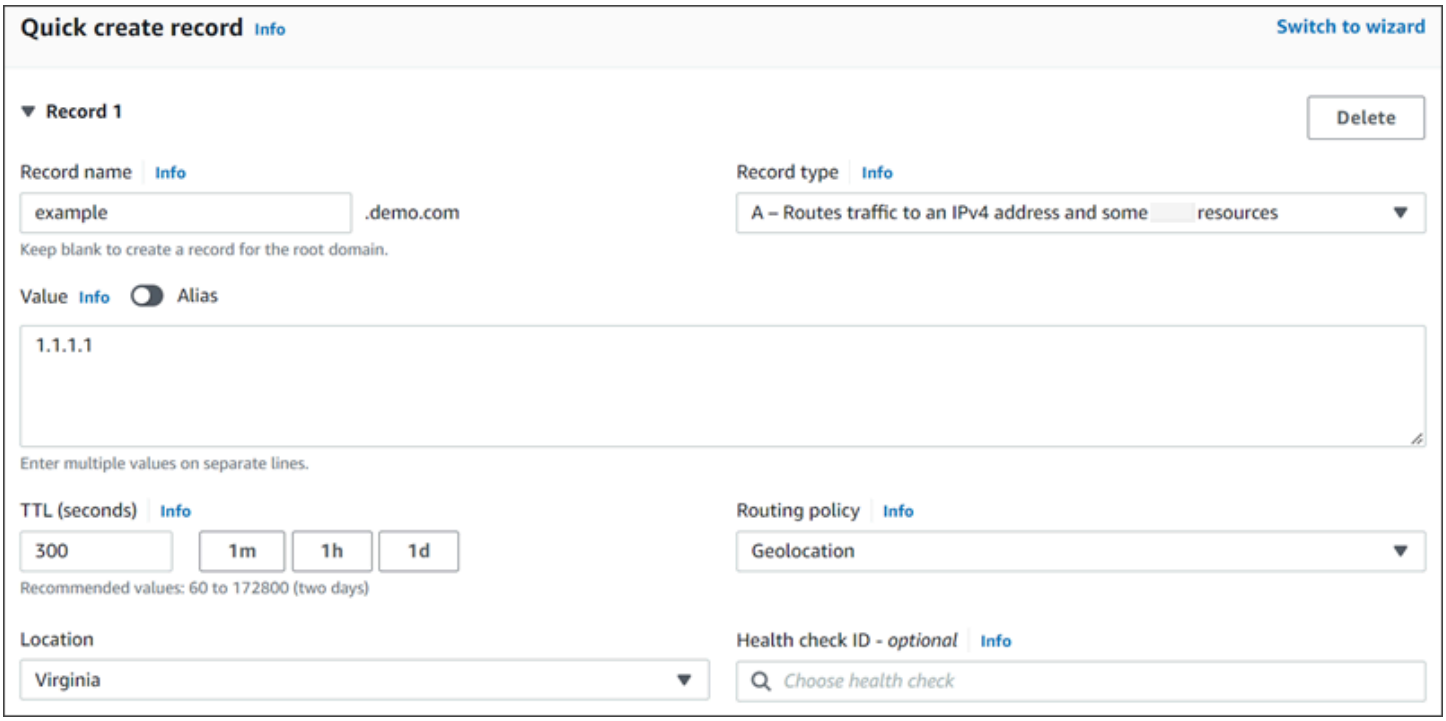
DNS 쿼리가 하이브리드 네트워크의 온프레미스 부분에서 시작된 경우, DNS 쿼리는 VPC 있는 위치의 AWS 리전 에서 시작된 것으로 간주됩니다.

상태 확인을 포함하는 경우 다음에 대한 기본 레코드를 생성할 수 있습니다.

- 지리적 위치에 매핑되지 않은 IP 주소.
- 지리적 위치 레코드를 생성하지 않은 위치에서 오는 DNS 쿼리.

DNS 쿼리의 리전에 대한 지리적 위치 레코드가 비정상이면 기본 레코드(정상인 경우)가 반환됩니다.

다음 그림의 예제 구성에서 us-east-1 AWS 리전 (버지니아)에서 오는 DNS 쿼리는 1.1.1.1 엔드포인트로 라우팅됩니다.



지리 근접 라우팅

Amazon Route 53는 지리 근접 라우팅을 사용하여 사용자와 리소스의 지리적 위치를 기반으로 트래픽을 리소스로 라우팅할 수 있습니다. 사용 가능한 가장 가까운 리소스로 트래픽을 라우팅합니다. 또는 바이어스라고 하는 값을 지정하여 해당 리소스로 라우팅하는 트래픽의 양을 늘리거나 줄일 수도 있습니다. 바이어스는 트래픽이 리소스로 라우팅되는 지리적 리전의 크기를 확장하거나 축소합니다.

리소스에 대한 지리 근접 규칙을 생성하고 각 규칙에 대해 다음 값 중 하나를 지정합니다.

- AWS 리소스를 사용하는 경우 리소스를 생성한 AWS 리전 또는 로컬 영역 그룹을 지정합니다.
- 리소스가 아닌 리소스를 사용하는 경우 리소스의 위도와 경도를AWS 지정합니다.

AWS 로컬 영역을 사용하려면 먼저 활성화해야 합니다. 자세한 내용은 AWS Local Zones User Guide의 Getting started with Local Zones를 참조하세요.

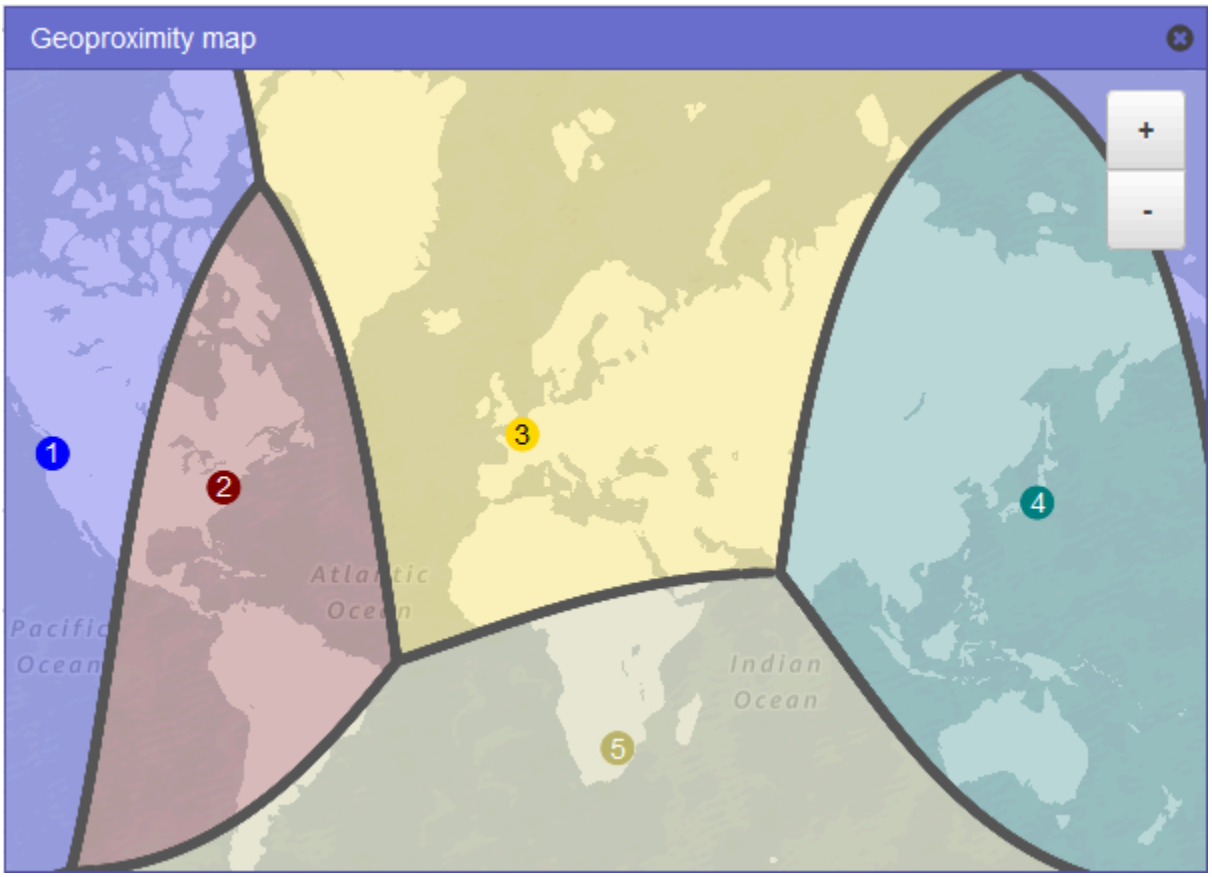
AWS 리전 와 로컬 영역의 차이점에 대해 알아보려면 Amazon EC2 사용 설명서의 리전 및 영역을 참조하세요.

Route 53가 트래픽을 리소스로 라우팅하는 지리적 리전의 크기를 선택적으로 변경하려면 바이어스에 대해 해당하는 값을 지정합니다.

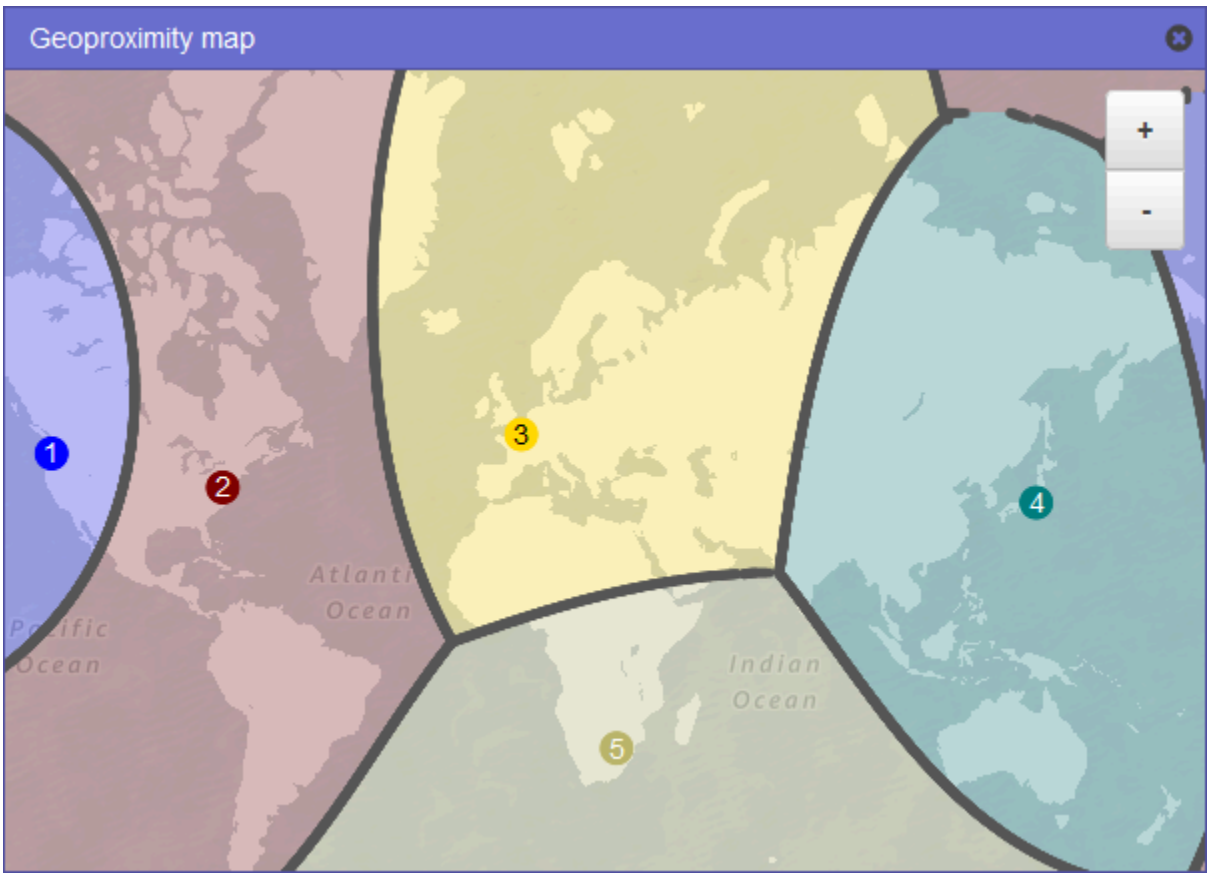
- Route 53가 트래픽을 리소스로 라우팅하는 지리적 리전의 크기를 확장하려면 바이어스에 대해 1~99의 양의 정수를 지정합니다. Route 53는 인접 리전의 크기를 축소합니다.
- Route 53가 트래픽을 리소스로 라우팅하는 지리적 리전의 크기를 축소하려면 바이어스에 대해 1~99의 음의 바이어스를 지정합니다. Route 53는 인접 리전의 크기를 확장합니다.

다음 맵은 위도 및 경도 AWS 리전 (5)로 지정된 남아프리카 요하네스버그의 위치와 4개(1~4번)를 보여줍니다.

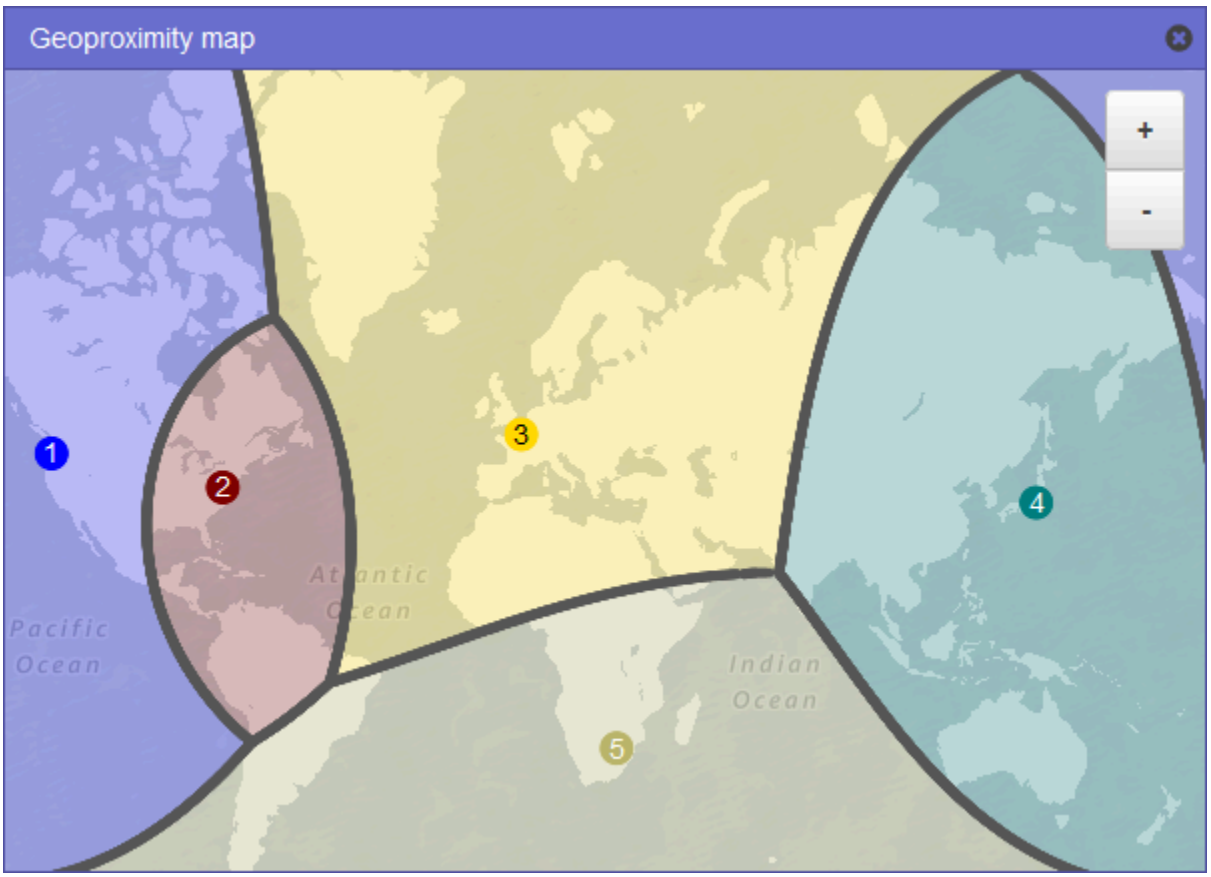
> **Note**
>
> 맵은 트래픽 흐름에서만 사용할 수 있습니다.



다음 지도를 보면 미국 동부(버지니아 북부) 리전(지도에서 2번)에 25개 이상의 바이어스를 추가하면 어떻게 되는지 알 수 있습니다. 리소스로 트래픽이 라우팅되는 리전이 북미 지역은 전보다 많아지고, 남미는 모든 지역에서 이루어집니다.



다음 지도를 보면 미국 동부(버지니아 북부) 리전의 바이어스를 25개 이하로 변경하면 어떻게 되는지 알 수 있습니다. 리소스로 트래픽이 라우팅되는 리전이 북미와 남미 지역은 이전보다 작아지고, 인접 리전 1, 3, 5의 리소스로 트래픽이 더 많이 라우팅됩니다.



리소스에 대한 바이어스를 변경할 때의 효과는 다음을 포함하여 여러 요인에 따라 달라집니다.

- 보유한 리소스의 수.
- 리소스가 서로 근접한 정도.
- 지리적 리전 간의 경계 영역 근처에 있는 사용자의 수. 예를 들어 AWS 리전 미국 동부(버지니아 북부) 및 미국 서부(오레곤)에 리소스가 있고 미국 텍사스 댈러스, 오스틴 및 샌안토니오에 사용자가 많다고 가정해 보겠습니다. 이러한 도시는 리소스 간에 거의 등거리이므로 편향의 작은 변화로 인해 리소스 간에 트래픽이 크게 변동될 수 있습니다 AWS 리전 .

예상치 못한 트래픽의 증가로 인해 리소스가 부족하지 않도록 바이어스를 조금씩 일정하게 변경하는 것이 좋습니다.

자세한 내용은 Amazon Route 53에서 EDNS0을 사용하여 사용자의 위치를 예측하는 방법 단원을 참조하십시오.

Amazon Route 53가 바이어스를 사용하여 트래픽을 라우팅하려면

다음은 Amazon Route 53가 트래픽을 라우팅하는 방법을 결정하기 위해 사용하는 수식입니다.

편향

```
Biased distance = actual distance * [1 - (bias/100)]
```

편향 값이 양수인 경우 Route 53는 DNS 쿼리의 소스와 지리 근접 레코드에 지정하는 리소스(예:의 EC2 인스턴스 AWS 리전)를 실제보다 더 가까운 것처럼 취급합니다. 예를 들어 다음과 같은 지리 근접 레코드가 있다고 가정하겠습니다.

- 양수 바이어스 값 50을 가진 웹 서버 A의 레코드
- 바이어스가 없는 웹 서버 B의 레코드

지리 근접 레코드가 양수 바이어스 값 50을 가지고 있을 때 Route 53는 쿼리의 소스와 그 레코드에 대한 리소스 사이의 거리를 반으로 줄입니다. 그러면 Route 53에서 어떤 리소스가 쿼리의 소스에 더 가까운지 계산합니다. 웹 서버 A와 B가 쿼리의 소스로부터 각각 150킬로미터와 100킬로미터 떨어져 있다고 가정해 봅시다. 어느 쪽 레코드에도 바이어스가 없다면 Route 53는 더 가까이 있는 웹 서버 B로 쿼리를 라우팅할 것입니다. 하지만 웹 서버 A의 레코드에 양수 바이어스 값 50이 있으므로, Route 53는 웹 서버 A가 쿼리의 소스로부터 75킬로미터 떨어져 있는 것처럼 처리합니다. 결과적으로, Route 53는 쿼리를 웹 서버 A로 라우팅합니다.

다음은 양수 바이어스 값 50에 대한 계산 과정입니다.

```
Bias = 50
Biased distance = actual distance * [1 - (bias/100)]

Biased distance = 150 kilometers * [1 - (50/100)]
Biased distance = 150 kilometers * (1 - .50)
Biased distance = 150 kilometers * (.50)
Biased distance = 75 kilometers
```

지연 시간 기반 라우팅

애플리케이션이 여러에서 호스팅되는 경우 지연 시간을 최소화 AWS 리전 하는에서 요청을 제공하여 사용자의 성능을 개선할 AWS 리전수 있습니다.

> **Note**
>
> 사용자와 리소스 간의 지연 시간에 대한 데이터는 전적으로 사용자와 AWS 데이터 센터 간의 트래픽을 기반으로 합니다. 에서 리소스를 사용하지 않는 경우 사용자와 리소스 간의 AWS 리

전실제 지연 시간은 AWS 지연 시간 데이터와 크게 다를 수 있습니다. 리소스가 AWS 리전과 같은 도시에 있는 경우에도 마찬가지입니다.

지연 시간 기반 라우팅을 사용하려면 여러 AWS 리전에 위치하는 리소스에 대해 지연 시간 레코드를 생성해야 합니다. Route 53에서 도메인 또는 하위 도메인(example.com 또는 acme.example.com)에 대한 DNS 쿼리를 수신하면 지연 시간 레코드가 생성된 AWS 리전 을 확인하고 사용자에게 가장 낮은 지연 시간을 제공하는 리전을 결정한 후 해당 리전의 지연 시간 레코드를 선택합니다. Route 53는 선택한 레코드의 값(예: 웹 서버의 IP 주소)으로 응답합니다.

예를 들어 미국 서부(오레곤) 리전 및 아시아 태평양(싱가포르) 리전에 Elastic Load Balancing 로드 밸런서가 있다고 가정합시다. 각 로드 밸런서에 대해 지연 시간 레코드를 생성합니다. 다음은 런던에 있는 사용자가 브라우저에 도메인 이름을 입력했을 때 발생하는 현상입니다.

1. DNS가 Route 53 이름 서버로 쿼리를 라우팅합니다.
2. Route 53는 런던과 싱가포르 리전 간, 그리고 런던과 오레곤 리전 간의 지연 시간에 대한 데이터를 참조합니다.
3. 런던 리전과 오레곤 리전 간의 지연 시간이 더 짧다면, Route 53는 오레곤 로드 밸런서의 IP 주소로 쿼리에 응답합니다. 런던 리전과 싱가포르 리전 간의 지연 시간이 더 짧다면, Route 53는 싱가포르 로드 밸런서의 IP 주소로 응답합니다.

인터넷상의 호스트 간 지연 시간은 네트워크 연결 및 라우팅이 시간에 따라 변화하는 양상에 따라 달라집니다. 지연 시간 기반 라우팅은 일정 기간에 걸쳐 수행되는 지연 시간 측정에 기반을 두고 있으며, 측정치는 그 변화 양상을 반영합니다. 이번 주에는 오레곤 리전으로 라우팅되는 요청이 다음 주에는 싱가포르 리전으로 라우팅될 수 있습니다.

Note

브라우저 또는 다른 뷰어가 EDNS0의 edns-client-subnet 확장을 지원하는 DNS 해석기를 사용하는 경우, DNS 해석기는 잘린 버전의 사용자 IP 주소를 Route 53에 전송합니다. 지연 시간 기반 라우팅이 구성된 경우 Route 53는 트래픽을 리소스로 라우팅할 때 이 값을 고려합니다. 자세한 내용은 Amazon Route 53에서 EDNS0을 사용하여 사용자의 위치를 예측하는 방법 단원을 참조하십시오.

프라이빗 호스팅 영역의 레코드에 지연 시간 라우팅 정책을 사용할 수 있습니다.

지연 시간 라우팅 정책으로 레코드를 만들 때 지정하는 값에 대한 정보는 다음 주제를 참조하십시오.

- 지연 시간 레코드에 특정한 값
- 지연 시간 별칭 레코드에 특정한 값
- 모든 라우팅 정책에 공통적인 값
- 모든 라우팅 정책의 별칭 레코드에 공통되는 값

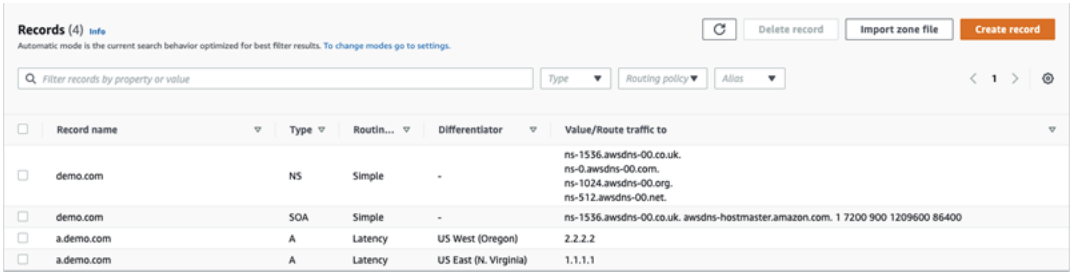
프라이빗 호스팅 영역의 지연 시간 기반 라우팅

프라이빗 호스팅 영역의 경우 Route 53는 쿼리 AWS 리전가 시작된 VPC AWS 리전 의와 동일하거나 가장 가까운 거리에 있는 엔드포인트를 사용하여 DNS 쿼리에 응답합니다.

> **Note**
>
> 아웃바운드 엔드포인트가 인바운드 엔드포인트에 전달된 경우, 레코드는 아웃바운드 엔드포인트가 아니라 인바운드 엔드포인트의 위치를 기반으로 확인됩니다.

상태 확인을 포함하고 쿼리 오리진에 대한 지연 시간이 가장 낮은 레코드가 비정상인 경우, 지연 시간이 두 번째로 낮은 정상 엔드포인트가 반환됩니다.

다음 그림의 예제 구성에서 us-east-1 AWS 리전또는 가장 가까운에서 오는 DNS 쿼리는 1.1.1.1 엔드포인트로 라우팅됩니다. us-west-2에서 오거나 이에 가장 가까운 DNS 쿼리는 2.2.2.2 엔드포인트로 라우팅됩니다.



IP 기반 라우팅

Amazon Route 53에서 IP 기반 라우팅을 사용하면 네트워크, 애플리케이션 및 클라이언트에 대한 이해를 바탕으로 DNS 라우팅을 미세 조정하여 최종 사용자를 위한 최상의 DNS 라우팅을 결정할 수 있습니다. IP 기반 라우팅은 사용자 IP-엔드포인트 매핑 형태로 Route 53에 데이터를 업로드하여 성능을 최적화하거나 네트워크 비용을 절감할 수 있는 세분화된 제어 기능을 제공합니다.

위치 정보 및 지연 시간 기반 라우팅은 Route 53가 수집 및 최신 상태로 유지하는 데이터를 기반으로 합니다. 이 접근 방식은 대부분의 고객에게 적합하지만 IP 기반 라우팅은 고객층의 특정 지식을 기반으

로 라우팅을 최적화할 수 있는 추가 기능을 제공합니다. 예를 들어 글로벌 비디오 콘텐츠 공급자가 특정 인터넷 서비스 제공업체(ISP)에서 최종 사용자로 라우팅하려 할 수 있습니다.

IP 기반 라우팅의 몇 가지 일반적인 사용 사례는 다음과 같습니다.

- 네트워크 전송 비용 또는 성능을 최적화하기 위해 특정 ISP에서 특정 엔드포인트로 최종 사용자를 라우팅하려는 경우.
- 고객의 물리적 위치에 대한 지식에 기반한 지리적 위치 라우팅과 같은 기존 Route 53 라우팅 유형에 재정의를 추가하려고 하는 경우.

IP 범위 관리 및 리소스 레코드 세트(RRSet)와 IP 범위 연결

IPv4의 경우 길이가 1~24비트인 CIDR 블록을 사용할 수 있으며 IPv6의 경우 길이가 1~48비트인 CIDR 블록을 사용할 수 있습니다. 0비트 CIDR 블록(0.0.0.0/0 또는 ::/0)을 정의하려면 기본(“*”) 위치를 사용합니다.

CIDR이 CIDR 컬렉션에 지정된 것보다 긴 DNS 쿼리의 경우 Route 53는 이를 더 짧은 CIDR 과 일치시킵니다. 예를 들어 CIDR 컬렉션에 CIDR 블록으로 2001:0DB8::/32를 지정하고 쿼리 가2001:0DB8:0000:1234::/48에서 시작된 경우 CIDR이 일치합니다. 반면에 CIDR 컬렉션에 2001:0DB8:0000:1234::/48을 지정하고 쿼리가 2001:0DB8::/32에서 시작된 경우 CDIR이 일치하지 않으므로 Route 53는 기본("*") 위치에 대한 레코드로 응답합니다.

CIDR 블록(또는 IP 범위) 집합을 CIDR 위치로 그룹화할 수 있으며, CIDR 위치는 다시 CIDR 컬렉션이라는 재사용 가능한 엔터티로 그룹화됩니다.

CIDR 블록

CIDR 표기법의 IP 범위입니다(예: 192.0.2.0/24 또는 2001:DB8::/32).

CIDR 위치

명명된 CIDR 블록 목록입니다. 예를 들어 example-isp-seattle = [192.0.2.0/24, 203.0.113.0/22, 198.51.100.0/24, 2001:DB8::/32]입니다. CIDR 위치 목록의 블록은 인접하거나 동일한 범위일 필요는 없습니다.

단일 위치는 IPv4 및 IPv6 블록을 둘 다 가질 수 있으며 이 위치는 각각 A 및 AAAA 레코드 세트에 모두 연결될 수 있습니다.

위치 이름은 대개 규칙에 따른 위치이지만 임의의 문자열이 될 수 있습니다(예: Company-A).

CIDR 컬렉션

명명된 위치의 컬렉션입니다. 예를 들어 mycollection = [example-isp-seattle, example-isp-tokyo]입니다.

IP 기반 라우팅 리소스 레코드 세트는 컬렉션의 위치를 참조하며, 동일한 레코드 세트 이름 및 유형에 대한 모든 리소스 레코드 세트는 동일한 컬렉션을 참조해야 합니다. 예를 들어 두 리전에서 웹 사이트를 만들고 서로 다른 두 개의 CIDR 위치에서 원래 IP 주소를 기반으로 특정 웹 사이트로 DNS 쿼리를 보내려면 두 위치 모두 동일한 CIDR 컬렉션에 작성되어야 합니다.

프라이빗 호스팅 영역의 레코드에는 IP 기반 라우팅 정책을 사용할 수 없습니다.

IP 기반 라우팅 정책으로 레코드를 만들 때 지정하는 값에 대한 정보는 다음 주제를 참조하세요.

- IP 기반 레코드에 특정한 값
- IP 기반 별칭 레코드에 특정한 값
- 모든 라우팅 정책에 공통적인 값
- 모든 라우팅 정책의 별칭 레코드에 공통되는 값

주제

- CIDR 위치 및 블록을 사용하여 CIDR 컬렉션 생성
- CIDR 위치 및 블록으로 작업
- CIDR 컬렉션 삭제
- 지리적 위치에서 IP 기반 라우팅으로 이동

CIDR 위치 및 블록을 사용하여 CIDR 컬렉션 생성

시작하려면 CIDR 컬렉션을 생성하고 CIDR 블록과 위치를 추가합니다.

Route 53 콘솔을 사용하여 CIDR 컬렉션을 생성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 IP 기반 라우팅(IP-based routing), CIDR 컬렉션(CIDR collections)을 차례로 선택합니다.

3. CIDR 컬렉션 생성(Create CIDR collection)을 선택합니다.
4. CIDR 컬렉션 생성(Create CIDR collection) 창의 세부 정보(Details)에 컬렉션의 이름을 입력합니다.
5. 컬렉션 생성(Create collection)을 선택하여 빈 컬렉션을 생성합니다.

   – 또는 -

   CIDR 위치 생성 섹션의 CIDR 위치 상자에 CIDR 위치의 이름을 입력합니다. 위치 이름은 임의의 식별 문자열일 수 있습니다(예: **`company 1`** 또는 **`Seattle`**). 실제 지리적 위치일 필요는 없습니다.

   > **Important**
   >
   > CIDR 위치 이름의 최대 길이는 16자입니다.

   CIDR 블록 상자에 CIDR 블록을 한 줄에 하나씩 입력합니다. 이는 IPv4의 경우 /0에서 /24까지, IPv6의 경우 /0에서 /48까지 범위인 IPv4 또는 IPv6 주소일 수 있습니다.
6. CIDR 블록을 입력한 다음 CIDR 컬렉션 생성(Create CIDR collection)를 선택하거나 다른 위치 추가(Add another location)를 선택하여 위치 및 CIDR 블록을 계속 입력합니다. 컬렉션당 여러 CIDR 위치를 입력할 수 있습니다.
7. CIDR 위치를 입력한 후 CIDR 컬렉션 생성(Create CIDR collection)을 선택합니다.

CIDR 위치 및 블록으로 작업

Route 53 콘솔을 사용하여 CIDR 위치를 사용하여 작업하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 IP 기반 라우팅(IP-based routing), CIDR 컬렉션(CIDR collections)을 선택하고 CIDR 컬렉션(CIDR collections) 섹션에서 컬렉션 이름(Collection name) 목록의 CIDR 컬렉션에 대한 링크를 클릭하세요.

   CIDR 위치(CIDR locations) 페이지에서 CIDR 위치를 생성하거나, 삭제하거나, 위치 및 해당 블록을 편집할 수 있습니다.

   - 위치를 생성하려면 CIDR 위치 생성(Create CIDR location)을 선택합니다.

- CIDR 위치 생성(Create CIDR location) 창에서 위치 이름, 위치와 연결된 CIDR 블록을 입력한 다음생성(Create)을 선택합니다.
- CIDR 위치 및 위치 내 블록을 보려면 위치 옆의 라디오 버튼을 선택하여 위치 이름과 CIDR 블록을 위치 창에 표시합니다.

  이 창에서 편집을 선택하여 위치 또는 위치의 CIDR 블록 이름을 업데이트합니다. 편집을 완료했으면 저장(Save)을 선택합니다.
- CIDR 위치 및 위치 내 블록을 삭제하려면 삭제하려는 위치 옆의 라디오 버튼을 선택한 다음 삭제(Delete)를 선택합니다. 삭제를 확인하려면 텍스트 입력 필드에 위치 이름을 입력하고 삭제(Delete)를 다시 한 번 선택합니다.

> **Important**
>
> CIDR 위치 삭제는 실행 취소할 수 없습니다. 위치와 연결된 DNS 레코드가 있는 경우 도메인에 연결할 수 없게 될 수 있습니다.

CIDR 컬렉션 삭제

Route 53 콘솔을 사용하여 CIDR 컬렉션, 컬렉션의 위치 및 블록을 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 IP 기반 라우팅(IP-based routing), CIDR 컬렉션(CIDR collections)을 차례로 선택합니다.
3. CIDR 컬렉션(CIDR collections) 섹션에서 삭제하려는 컬렉션의 링크된 이름을 클릭합니다.
4. CIDR 위치(CIDR locations) 페이지에서 각 위치를 한 번에 하나씩 선택하고 삭제(Delete)를 선택하고, 대화 상자에 이름을 입력한 다음 삭제(Delete)를 선택합니다. 컬렉션을 삭제할 수 있기 전에 CIDR 컬렉션과 연결된 각 위치를 삭제해야 합니다.
5. 각 CIDR 위치 삭제가 완료된 후 CIDR 위치(CIDR locations) 페이지에서 삭제하려는 컬렉션 옆의 라디오 버튼을 선택한 다음 삭제(Delete)를 선택합니다.

지리적 위치에서 IP 기반 라우팅으로 이동

지리적 위치 또는 지리적 근접성 라우팅 정책을 사용하고 특정 클라이언트가 물리적 위치 또는 네트워크 토폴로지에 따라 최적이 아닌 엔드포인트로 라우팅되는 것을 계속 확인하는 경우 IP 기반 라우팅을 사용하여 이러한 클라이언트의 퍼블릭 IP 범위를 더 효과적으로 타겟팅할 수 있습니다.

다음 표는 캘리포니아 IP 범위에 맞게 미세 조정할 기존 지리적 위치 라우팅에 대한 지리적 위치 구성의 예를 포함합니다.

레코드 세트 이름	라우팅 정책 및 출발지	애플리케이션 엔드포인트의 IP 주소
example.com	지리적 위치 라우팅(미국)	198.51.100.1
example.com	지리적 위치 라우팅(유럽)	198.51.100.2

캘리포니아에서 IP 범위를 재정의하여 새 애플리케이션 엔드포인트로 이동하려면 먼저 새 레코드 세트 이름으로 지리적 위치 라우팅을 다시 생성합니다.

레코드 세트 이름	라우팅 정책 및 출발지	애플리케이션 엔드포인트의 IP 주소
geo.example.com	지리적 위치 라우팅(미국)	198.51.100.1
geo.example.com	지리적 위치 라우팅(유럽)	198.51.100.2

그런 다음 IP 기반 라우팅 레코드와 최근에 재생성된 지리적 위치 라우팅 레코드세트를 가리키는 기본 레코드를 만듭니다.

레코드 세트 이름	라우팅 정책 및 출발지	애플리케이션 엔드포인트의 IP 주소
example.com	IP 기반 라우팅(기본값)	기본값으로 사용하려는 geo.example.com 응용 프로그

레코드 세트 이름	라우팅 정책 및 출발지	애플리케이션 엔드포인트의 IP 주소
		램 엔드포인트에 대한 별칭 레코드입니다. 예: `198.51.100.1` .
example.com	IP 기반 라우팅(캘리포니아 IP 범위)	`198.51.100.3`

다중값 응답 라우팅

다중값 응답 라우팅을 사용하면 Amazon Route 53가 DNS 쿼리에 대해 다수의 값(예: 웹 서버의 IP 주소)을 반환하도록 구성할 수 있습니다. 다중값은 거의 모든 레코드에 대해 지정할 수 있지만, 다중값 응답 라우팅을 사용하면 각 리소스의 상태를 확인할 수도 있으므로 Route 53는 정상 리소스의 값만 반환합니다. 이것이 로드 밸런서를 대체하는 것은 아니지만, 다수의 상태 확인 가능한 IP 주소를 반환하는 기능은 DNS를 사용하여 가용성 및 로드 밸런싱을 개선하는 한 방법입니다.

트래픽을 거의 무작위적으로 웹 서버 같은 다수의 리소스로 라우팅하려면 각 리소스마다 하나씩 다중값 응답 레코드를 생성하고, 선택적으로 Route 53 상태 확인을 각 레코드에 연결할 수 있습니다. Route 53는 최대 8개의 정상 레코드로 DNS 쿼리에 응답하며, DNS 해석기마다 다른 응답을 제공합니다. 해석기가 응답을 캐시한 후 한 웹 서버가 사용 불가능해질 경우 클라이언트 소프트웨어는 응답에 포함된 다른 IP 주소를 시도할 수 있습니다.

다음 사항에 유의하세요.

- 상태 확인을 다중 응답 레코드와 연결할 경우 Route 53는 상태 확인이 정상일 경우에만 해당 IP 주소로 DNS 쿼리에 응답합니다.
- 상태 검사를 다중 응답 레코드와 연결하지 않을 경우 Route 53는 항상 레코드가 정상이라고 간주합니다.
- 정상 레코드가 8개 이하일 경우 Route 53는 모든 DNS 쿼리에 모든 정상 레코드로 응답합니다.
- 모든 레코드가 비정상일 경우 Route 53는 최대 8개의 비정상 레코드로 DNS 쿼리에 응답합니다.

프라이빗 호스팅 영역의 레코드에 다중 응답 라우팅 정책을 사용할 수 있습니다.

다중 응답 라우팅 정책으로 레코드를 만들 때 지정하는 값에 대한 정보는 다중값 응답 레코드에 특정한 값 및모든 라우팅 정책에 공통적인 값 단원을 참조하십시오.

가중치 기반 라우팅

가중치 기반 라우팅을 사용하면 다수의 리소스를 단일 도메인 이름(example.com) 또는 하위 도메인 이름(acme.example.com)과 연결하고 각 리소스로 라우팅되는 트래픽 비율을 선택할 수 있습니다. 이러한 방식은 로드 밸런싱, 새 버전의 소프트웨어 테스트 등을 비롯한 다양한 목적에 활용될 수 있습니다.

가중치 기반 라우팅을 구성하려면 각 리소스에 대해 동일한 이름의 레코드를 생성합니다. 각 리소스에 보낼 트래픽 양에 해당하는 상대적 가중치를 각 레코드에 할당합니다. Amazon Route 53는 그룹 내 전체 레코드의 총 가중치에 대한 비율에 따라 레코드에 할당된 가중치를 기반으로 트래픽을 리소스에 전송합니다.

$$\frac{\text{Weight for a specified record}}{\text{Sum of the weights for all records}}$$

예를 들어 한 리소스에 일부 트래픽만 전송하고 나머지를 다른 리소스로 전송하려는 경우 가중치 1과 255를 지정할 수 있습니다. 가중치 1이 할당된 리소스에는 트래픽의 1/256(1/1+255)이 전송되고, 다른 리소스에는 트래픽의 255/256(255/1+255)이 전송됩니다. 가중치를 변경하여 점진적으로 균형을 조정할 수 있습니다. 특정 리소스로 트래픽 전송을 중단하려면 해당 레코드의 가중치를 0으로 변경할 수 있습니다.

가중치 기반 라우팅 정책으로 레코드를 만들 때 지정하는 값에 대한 정보는 다음 주제를 참조하십시오.

- 가중치 기반 레코드에 특정한 값
- 가중치 기반 별칭 레코드에 특정한 값
- 모든 라우팅 정책에 공통적인 값
- 모든 라우팅 정책의 별칭 레코드에 공통되는 값

프라이빗 호스팅 영역의 레코드에 가중치 기반 라우팅 정책을 사용할 수 있습니다.

상태 확인 및 가중치 기반 라우팅

가중치 기반 레코드의 그룹에서 레코드 전체에 상태 확인을 추가하지만 어떤 레코드에는 0이 아닌 가중치를 부여하고 또 다른 레코드에는 0인 가중치를 부여하는 경우 상태 확인은 모든 레코드의 가중치가 0일 때와 동일하게 작업합니다. 단, 다음 경우는 예외입니다.

- Route 53는 처음에 0이 아닌 가중치 기반 레코드만을 고려합니다(해당되는 경우).
- 0보다 큰 가중치를 지닌 레코드 전체가 비정상인 경우 Route 53는 0인 가중치 기반 레코드를 고려합니다.

다음 표는 가중치가 0인 레코드에 상태 확인이 포함된 경우의 동작을 자세히 설명합니다.

	레코드 1	레코드 2	레코드 3
가중치	1	1	0
상태 확인 포함 여부	예	예	예
상태 확인 상태	비정상	비정상	정상
DNS 쿼리가 응답되었습니까?	아니요	아니요	예
상태 확인 상태	비정상	비정상	비정상
DNS query answered?	예	예	아니요
상태 확인 상태	비정상	정상	비정상
DNS 쿼리에 대한 응답을 받았습니까?	아니요	예	아니요
상태 확인 상태	정상	정상	비정상
DNS 쿼리에 대한 응답을 받았습니까?	예	예	아니요
상태 확인 상태	정상	정상	정상

	레코드 1	레코드 2	레코드 3
DNS 쿼리에 대한 응답을 받았습니까?	예	예	아니요

다음 표는 가중치가 0인 레코드에 상태 확인이 포함되지 않은 경우의 동작을 자세히 설명합니다.

	레코드 1	레코드 2	레코드 3
가중치	1	1	0
상태 확인 포함 여부	예	예	아니요
상태 확인 상태	정상	정상	N/A
DNS query answered?	Yes	예	No
상태 확인 상태	비정상	비정상	N/A
DNS 쿼리에 대한 응답을 받았습니까?	아니요	아니요	예
상태 확인 상태	비정상	정상	N/A
DNS query answered?	아니요	예	아니요

Amazon Route 53에서 EDNS0을 사용하여 사용자의 위치를 예측하는 방법

지리적 위치, 지리적 근접성, IP 기반, 대기 시간 라우팅의 정확도를 개선하기 위해 Amazon Route 53는 EDNS0의 edns-client-subnet 확장을 지원합니다. (EDNS0은 DNS 프로토콜에 선택적으로 몇 개의

확장을 추가합니다.) Route 53는 DNS 해석기가 edns-client-subnet을 지원할 때만 이를 사용할 수 있습니다.

- 브라우저 또는 다른 최종 사용자가 edns-client-subnet을 지원하지 않는 DNS 해석기를 사용하는 경우, Route 53는 DNS 해석기의 소스 IP 주소를 이용해 사용자 위치의 근사치를 측정해 해석기의 위치에 대한 DNS 레코드로 지리 위치 쿼리에 응답합니다.
- 브라우저 또는 다른 뷰어가 edns-client-subnet을 지원하는 DNS 해석기를 사용하는 경우, DNS 해석기는 잘린 버전의 사용자 IP 주소를 Route 53에 전송합니다. Route 53는 DNS 해석기의 원본 IP 주소가 아닌 잘린 IP 주소를 기반으로 사용자의 위치를 결정합니다. 이렇게 하면 일반적으로 사용자의 위치를 보다 정확하게 예측할 수 있습니다. 그런 다음 Route 53는 사용자의 위치에 대한 DNS 레코드를 사용하여 지리적 위치 쿼리에 응답합니다.
- EDNS0는 프라이빗 호스팅 영역에 적용되지 않습니다. 프라이빗 호스팅 영역의 경우 Route 53는 프라이빗 호스팅 영역 AWS 리전 이 있는의 Route 53 Resolver에서 데이터를 사용하여 지리적 위치 및 지연 시간 라우팅 결정을 내립니다.

edns-client-subnet에 대한 자세한 내용은 EDNS Client Subnet RFC의 Client Subnet in DNS Requests를 참조하세요.

별칭 또는 비 별칭 레코드 선택

Amazon Route 53 별칭 레코드는 DNS 기능에 Route 53 고유의 확장을 제공합니다. 별칭 레코드를 사용하면 CloudFront 배포 및 Amazon S3 버킷을 포함하되 이에 국한되지 않는 선택된 AWS 리소스로 트래픽을 라우팅할 수 있습니다. 호스팅 영역의 한 레코드에서 다른 레코드로 트래픽을 라우팅할 수도 있습니다.

CNAME 레코드와 달리, zone apex라고도 하는 DNS 네임스페이스의 최상위 노드에 별칭 레코드를 만들 수 있습니다. 예를 들어, DNS 이름 example.com을 등록하면 zone apex는 example.com입니다. example.com에 대한 CNAME 레코드를 생성할 수 없지만 트래픽을 www.example.com으로 라우팅하는 example.com에 대한 별칭 레코드를 생성할 수 있습니다(www.example.com의 레코드 유형이 CNAME 유형이 아닌 한).

Route 53가 별칭 레코드에 대한 DNS 쿼리를 받으면, Route 53는 해당 리소스에 해당되는 값으로 응답합니다.

- Amazon API Gateway 사용자 지정 리전 API 또는 엣지 최적화 API - Route 53는 API의 하나 이상의 IP 주소로 응답합니다.
- Amazon VPC 인터페이스 엔드포인트 – Route 53는 인터페이스 엔드포인트의 하나 이상의 IP 주소로 응답합니다.

- CloudFront 배포 – Route 53는 콘텐츠를 제공할 수 있는 CloudFront 엣지 서버의 하나 이상의 IP 주소로 응답합니다.
- App Runner 서비스 - Route 53는 하나 이상의 IP 주소로 응답합니다.
- Elastic Beanstalk 환경 – Route 53는 환경에 대해 하나 이상의 IP 주소로 응답합니다.
- Elastic Load Balancing 로드 밸런서 – Route 53는 로드 밸런서에 대해 1개 이상의 IP 주소로 응답합니다. 여기에는 Application Load Balancer, Classic Load Balancer 및 Network Load Balancer가 포함됩니다.
- AWS Global Accelerator 액셀러레이터 - Route 53은 액셀러레이터의 IP 주소로 응답합니다.
- OpenSearch Service - Route 53은 OpenSearch Service 사용자 지정 도메인에 대해 하나 이상의 IP 주소로 응답합니다.
- 정적 웹사이트로 구성되는 Amazon S3 버킷 – Route 53는 Amazon S3 버킷의 1개의 IP 주소로 응답합니다.
- 동일한 호스팅 영역에 있는 같은 유형의 다른 Route 53 레코드 – Route 53는 해당 쿼리가 별칭 레코드가 참조한 레코드에 대한 것처럼 응답합니다(별칭 레코드와 CNAME 레코드의 비교 참조).
- AWS AppSync 도메인 이름 - Route 53은 인터페이스 엔드포인트에 대해 하나 이상의 IP 주소로 응답합니다.

자세한 내용은 AWS 리소스로 인터넷 트래픽 라우팅 단원을 참조하십시오.

별칭 레코드를 사용하여 트래픽을 AWS 리소스로 라우팅하면 Route 53는 리소스의 변경 사항을 자동으로 인식합니다. 예를 들어, example.com의 별칭 레코드가 lb1-1234.us-east-2.elb.amazonaws.com의 Elastic Load Balancing 로드 밸런서를 가리킨다고 가정합니다. 로드 밸런서의 IP 주소가 변경된다면, Route 53는 자동적으로 새로운 IP 주소를 사용하여 DNS 쿼리에 응답하기 시작합니다.

별칭 레코드가 AWS 리소스를 가리키는 경우 TTL(Time to Live)을 설정할 수 없습니다. Route 53은 리소스에 기본 TTL을 사용합니다. 별칭 레코드가 동일한 호스팅 영역의 다른 레코드를 가리키는 경우, Route 53는 별칭 레코드가 가리키는 레코드의 TTL을 사용합니다. Elastic Load Balancing의 현재 TTL 값에 대한 자세한 내용은 Elastic Load Balancing 사용 설명서의 라우팅 요청으로 이동하여 'ttl'을 검색하세요.

Route 53 콘솔을 사용하여 레코드를 생성하는 방법에 대한 자세한 내용은 Amazon Route 53 콘솔을 사용하여 레코드 생성 섹션을 참조하세요. 별칭 레코드에 대해 지정하는 값에 대한 자세한 내용은 Amazon Route 53 레코드를 생성 또는 편집할 때 지정하는 값의 해당 주제를 참조하십시오.

- 단순 별칭 레코드에 특정한 값
- 가중치 기반 별칭 레코드에 특정한 값

- 지연 시간 별칭 레코드에 특정한 값
- 장애 조치 별칭 레코드에 특정한 값
- 지리 위치 별칭 레코드에 특정한 값
- 지리 근접성 별칭 레코드에 특정된 값
- 모든 라우팅 정책의 별칭 레코드에 공통되는 값

별칭 레코드와 CNAME 레코드의 비교

별칭 레코드는 CNAME 레코드와 비슷하지만, 다음과 같은 중요한 차이점이 몇 가지 있습니다. 다음 목록은 별칭 레코드와 CNAME 레코드를 비교합니다.

쿼리를 리디렉션할 수 있는 리소스

별칭 레코드

별칭 레코드는 다음을 포함하되 이에 국한되지 않는 쿼리를 선택한 AWS 리소스로 리디렉션할 수 있습니다.

- Amazon S3 버킷
- CloudFront 배포
- 동일한 Route 53 호스팅 영역의 다른 레코드

예를 들어, acme.example.com이라는 이름의 Amazon S3 버킷으로 쿼리를 리디렉션하는 acme.example.com이라는 별칭 레코드를 생성할 수 있습니다. example.com 호스팅 영역의 zenith.example.com 레코드로 쿼리를 리디렉션하는 acme.example.com 별칭 레코드를 생성할 수도 있습니다.

CNAME 레코드

CNAME 레코드는 DNS 쿼리를 DNS 레코드로 리디렉션할 수 있습니다. 예를 들어 acme.example.com에서 zenith.example.com 또는 acme.example.org로 쿼리를 리디렉션하는 CNAME 레코드를 생성할 수 있습니다. 쿼리를 리디렉션할 도메인의 DNS 서비스로 Route 53를 사용할 필요가 없습니다.

도메인과 이름이 동일한 레코드 생성(zone apex의 레코드)

별칭 레코드

대부분의 구성에서 호스팅 영역(zone apex)과 이름이 동일한 별칭 레코드를 만들 수 있습니다. 단, zone apex(예: example.com)의 쿼리를 CNAME 유형의 동일한 호스팅 영역에 있는 레코드(예: zenith.example.com)로 리디렉션하려는 경우는 예외입니다. 별칭 레코드는 트래픽이 라우

팅되는 레코드와 동일한 유형이어야 하고 zone apex에 대한 CNAME 레코드 생성은 별칭 레코드에 대해서도 지원되지 않기 때문입니다.

CNAME 레코드

호스팅 영역(zone apex)과 이름이 동일한 CNAME 레코드는 만들 수 없습니다. 이는 도메인 이름(example.com)의 호스팅 영역과 하위 도메인(zenith.example.com)의 호스팅 영역 모두에 해당됩니다.

DNS 쿼리 요금

별칭 레코드

Route 53는 AWS 리소스에 대한 별칭 쿼리에 대해 요금을 부과하지 않습니다. 자세한 내용은 Amazon Route 53 요금을 참조하십시오.

CNAME 레코드

Route 53는 CNAME 쿼리에 대해 요금을 부과합니다.

> **Note**
>
> Route 53 호스팅 영역(동일한 호스팅 영역 또는 다른 호스팅 영역)에 있는 다른 레코드의 이름으로 리디렉션되는 CNAME 레코드를 생성하는 경우 각 DNS 쿼리는 다음 두 개의 쿼리로 요금이 부과됩니다.
>
> - Route 53는 리디렉션하려는 레코드의 이름으로 첫 번째 DNS 쿼리에 응답합니다.
> - 그런 다음 DNS 해석기는 트래픽을 리디렉션하려는 위치(예: 웹 서버의 IP 주소)에 대한 정보를 얻기 위해 첫 번째 응답의 레코드에 대한 다른 쿼리를 제출해야 합니다.
>
> CNAME 레코드가 다른 DNS 서비스와 함께 호스팅되는 레코드의 이름으로 리디렉션되는 경우 Route 53는 한 개의 쿼리에 대해 요금을 부과합니다. 다른 DNS 서비스는 두 번째 쿼리에 대해 요금을 부과할 수 있습니다.

DNS 쿼리에 지정된 레코드 유형

별칭 레코드

Route 53는 별칭 레코드 이름(예: acme.example.com)과 별칭 레코드 유형(예: A 또는 AAAA)이 DNS 쿼리의 이름 및 유형과 일치할 때만 DNS 쿼리에 응답합니다.

CNAME 레코드

CNAME 레코드는 A 또는 AAAA와 같이 DNS 쿼리에 지정된 레코드 유형에 관계없이 레코드 이름에 대한 DNS 쿼리를 리디렉션합니다.

레코드가 dig 또는 nslookup 쿼리에 나열되는 방법

별칭 레코드

dig 또는 nslookup 쿼리에 대한 응답에서 별칭 레코드는 레코드를 생성할 때 지정한 레코드 유형(예: A 또는 AAAA)으로 나열됩니다. (별칭 레코드에 지정하는 레코드 유형은 트래픽을 라우팅하는 리소스에 따라 다릅니다. 예를 들어 S3 버킷으로 트래픽을 라우팅하려면 유형에 A를 지정합니다.) 별칭 속성은 Route 53 콘솔 또는 AWS CLI `list-resource-record-sets` 명령과 같은 프로그래밍 요청에 대한 응답에서만 볼 수 있습니다.

CNAME 레코드

CNAME 레코드는 dig 또는 nslookup 쿼리에 대한 응답에서 CNAME 레코드로 나열됩니다.

지원되는 DNS 레코드 유형

Amazon Route 53은 이 섹션에 나열된 DNS 레코드 유형을 지원합니다. 각 레코드 유형 역시 API를 사용해 Route 53에 액세스할 때 `Value` 요소를 포맷하는 방법에 대한 한 가지 예를 포함합니다.

> **Note**
>
> 도메인 이름을 포함하는 레코드 유형에 대해서는 예를 들어 www.example.com과 같은 전체 주소 도메인 이름을 입력합니다. 뒤에 오는 점은 선택 사항이며, Route 53은 도메인 이름을 전체 주소 도메인 이름으로 간주합니다. 다시 말해 Route 53은 www.example.com(뒤에 점 없음)과 www.example.com.(뒤에 점 있음)을 동일하게 처리합니다.

Route 53은 별칭 레코드라고 하는 DNS 기능에 대한 확장을 제공합니다. CNAME 레코드와 마찬가지로 별칭 레코드를 사용하면 CloudFront 배포 및 Amazon S3 버킷과 같은 선택한 AWS 리소스로 트래픽을 라우팅할 수 있습니다. 별칭 레코드와 CNAME 레코드의 비교를 포함한 자세한 내용은 별칭 또는 비별칭 레코드 선택 단원을 참조하십시오.

주제

- 레코드 유형
- AAAA 레코드 유형
- CAA 레코드 유형
- CNAME 레코드 유형
- DS 레코드 유형

- HTTPS 레코드 유형
- MX 레코드 유형
- NAPTR 레코드 유식
- NS 레코드 유형
- PTR 레코드 유형
- SOA 레코드 유형
- SPF 레코드 유형
- SRV 레코드 유형
- SSHFP 레코드 유형
- SVCB 레코드 유형
- TLSA 레코드 유형
- TXT 레코드 유형

레코드 유형

A 레코드에서 점이 있는 십진법으로 된 IPv4 주소를 사용하여 웹 서버와 같은 리소스로 트래픽을 라우팅합니다.

Amazon Route 53 콘솔에 대한 예제

```
192.0.2.1
```

Route 53 API에 대한 예제

```
<Value>192.0.2.1</Value>
```

AAAA 레코드 유형

AAAA 레코드에서 콜론으로 구분된 16진법 형식의 IPv6 주소를 사용하여 웹 서버와 같은 리소스로 트래픽을 라우팅합니다.

Amazon Route 53 콘솔에 대한 예제

```
2001:0db8:85a3:0:0:8a2e:0370:7334
```

Route 53 API에 대한 예제

```
<Value>2001:0db8:85a3:0:0:8a2e:0370:7334</Value>
```

CAA 레코드 유형

CAA 레코드는 도메인 또는 하위 도메인에 대한 인증서 발급이 허용되는 인증 기관(CA)을 지정합니다. CAA 레코드를 생성하면 잘못된 CA가 도메인에 대한 인증서를 발급하는 것을 방지하는 데 도움이 됩니다. CAA 레코드는 인증 기관에서 지정한 보안 요구 사항(예: 도메인의 소유자임을 확인하기 위한 요구 사항) 대신 사용할 수 없습니다.

CAA 레코드를 사용하여 다음을 지정할 수 있습니다.

- SSL/TLS 인증서(있는 경우)를 발급할 수 있는 인증 기관(CA)
- CA가 도메인 또는 하위 도메인에 인증서를 발급할 때 연락처의 이메일 주소 또는 URL

CAA 레코드를 호스팅 영역에 추가할 때 공백으로 구분하여 다음 세 가지 설정을 지정합니다.

```
flags tag "value"
```

CAA 레코드의 형식에 대해 다음을 알아 두십시오.

- `tag` 값에는 A-Z, a-z, 0-9 등의 문자만 포함될 수 있습니다.
- `value`는 항상 인용 부호("")로 묶습니다.
- 일부 CA는 `value`에 대한 추가 값을 허용하거나 요구합니다. 이름-값 페어로 추가 값을 지정하고 세미콜론(;)으로 구분합니다. 예를 들면 다음과 같습니다.

  ```
  0 issue "ca.example.net; account=123456"
  ```
- CA가 하위 도메인(예: www.example.com)에 대한 인증서 요청을 받았는데 해당 하위 도메인에 대해 아무런 CAA 레코드도 없는 경우, CA는 상위 도메인(예: example.com)용 CAA 레코드에 대한 DNS 쿼리를 제출합니다. 상위 도메인에 대한 레코드가 존재하고 인증서 요청이 유효한 경우 CA는 하위 도메인에 대한 인증서를 발행합니다.
- CAA 레코드에 대해 지정할 값을 결정하려면 CA에 문의하는 것이 좋습니다.
- 이름이 동일한 CAA 레코드와 CNAME 레코드를 생성할 수 없습니다. DNS에서 CNAME 레코드와 기타 다른 유형의 레코드에 대해 동일한 이름을 사용하지 못하도록 하기 때문입니다.

주제

- CA가 도메인 또는 하위 도메인에 대한 인증서를 발행하도록 승인
- CA가 도메인 또는 하위 도메인에 대한 와일드카드 인증서를 발행하도록 승인

- CA가 도메인 또는 하위 도메인에 대한 인증서를 발행하지 못하도록 금지
- CA가 잘못된 인증서 요청을 수신하는 경우 CA가 사용자에게 연락하도록 요청
- CA에서 지원하는 다른 설정 사용
- 예시

CA가 도메인 또는 하위 도메인에 대한 인증서를 발행하도록 승인

CA가 도메인 또는 하위 도메인에 대한 인증서를 발행하도록 승인하려면 해당 도메인 또는 하위 도메인과 같은 이름을 가진 레코드를 만들고 다음 설정을 지정합니다.

- flags – `0`
- tag – `issue`
- value - 도메인 또는 하위 도메인에 대한 인증서를 발행하도록 승인하는 CA에 대한 코드

예를 들어, ca.example.net에서 example.com에 대한 인증서를 발행하도록 승인하려는 경우를 가정해 봅시다. 다음 설정으로 example.com에 대한 CAA 레코드를 생성합니다.

```
0 issue "ca.example.net"
```

AWS Certificate Manager 가 인증서를 발급하도록 승인하는 방법에 대한 자세한 내용은 AWS Certificate Manager 사용 설명서의 CAA 레코드 구성을 참조하세요.

CA가 도메인 또는 하위 도메인에 대한 와일드카드 인증서를 발행하도록 승인

CA가 도메인 또는 하위 도메인에 대한 와일드카드 인증서를 발행하도록 승인하려면 해당 도메인 또는 하위 도메인과 같은 이름을 가진 레코드를 만들고 다음 설정을 지정합니다. 와일드카드 인증서는 도메인 또는 하위 도메인 및 모든 하위 도메인에 적용됩니다.

- flags – `0`
- tag – `issuewild`
- value - 도메인 또는 하위 도메인과 그 하위 도메인에 대한 인증서를 발행하도록 승인하는 CA에 대한 코드

예를 들어, ca.example.net에서 example.com에 대한 와일드카드 인증서(example.com과 example.com의 모든 하위 도메인에 적용되는 인증서)를 발행하도록 승인하려는 경우를 가정해 봅시다. 다음 설정으로 example.com에 대한 CAA 레코드를 생성합니다.

```
0 issuewild "ca.example.net"
```

CA가 도메인 또는 하위 도메인에 대한 와일드카드 인증서를 발행하도록 승인하고 싶으면 해당 도메인 또는 하위 도메인과 같은 이름을 가진 레코드를 만들고 다음 설정을 지정합니다. 와일드카드 인증서는 도메인 또는 하위 도메인 및 모든 하위 도메인에 적용됩니다.

CA가 도메인 또는 하위 도메인에 대한 인증서를 발행하지 못하도록 금지

CA가 도메인 또는 하위 도메인에 대한 인증서를 발행하지 못하도록 금지하려면 해당 도메인 또는 하위 도메인과 같은 이름을 가진 레코드를 만들고 다음 설정을 지정합니다.

- flags – `0`
- tag – `issue`
- value – `";"`

예를 들어, 어떤 CA에서도 example.com에 대한 인증서를 발행하지 못하도록 하려는 경우를 가정해 봅시다. 다음 설정으로 example.com에 대한 CAA 레코드를 생성합니다.

```
0 issue ";"
```

어떤 CA에서도 example.com 또는 그 하위 도메인에 대한 인증서를 발행하지 못하도록 하려면 다음 설정으로 example.com에 대한 CAA 레코드를 생성합니다.

```
0 issuewild ";"
```

> **Note**
>
> example.com에 대한 CA 레코드를 생성하고 다음 값을 둘 다 지정하면 ca.example.net 값을 사용하는 CA가 example.com에 대한 인증서를 발행할 수 있습니다.
>
> ```
> 0 issue ";"
> 0 issue "ca.example.net"
> ```

CA가 잘못된 인증서 요청을 수신하는 경우 CA가 사용자에게 연락하도록 요청

인증서에 대해 잘못된 요청을 수신하는 CA가 귀하에게 연락하도록 하려면 다음 설정을 지정합니다.

- flags – `0`
- tag – `iodef`
- value - CA가 인증서에 대해 잘못된 요청을 수신한 경우 CA가 알리려는 URL 또는 이메일 주소입니다. 해당하는 형식을 사용합니다.

  `"mailto:email-address"`

  `"http://URL"`

  `"https://URL"`

예를 들어, 인증서에 대해 잘못된 요청을 수신하는 CA가 admin@example.com으로 이메일을 보내도록 하려는 경우 다음 설정으로 CAA 레코드를 생성합니다.

```
0 iodef "mailto:admin@example.com"
```

CA에서 지원하는 다른 설정 사용

CA가 CAA 레코드에 대해 RFC에 정해지지 않은 기능을 지원하는 경우 다음 설정을 지정합니다.

- flags - 128(이 값은 CA가 지정된 기능을 지원하지 않으면 인증서를 발행하지 못하도록 합니다.)
- tag - CA가 사용하도록 승인한 태그
- value - 태그의 값에 해당하는 값

예를 들어, CA가 잘못된 인증서 요청을 수신하는 경우 문자 메시지 전송 기능을 지원한다고 가정해 봅시다. (이 옵션을 지원하는 CA에 대해서는 알지 못합니다.) 레코드에 대한 설정은 다음과 같을 수 있습니다.

```
128 exampletag "15555551212"
```

예시

Route 53 콘솔에 대한 예제

```
0 issue "ca.example.net"
0 iodef "mailto:admin@example.com"
```

Route 53 API에 대한 예제

```
<ResourceRecord>
   <Value>0 issue "ca.example.net"</Value>
   <Value>0 iodef "mailto:admin@example.com"</Value>
</ResourceRecord>
```

CNAME 레코드 유형

CNAME 레코드는 acme.example.com과 같은 현재 레코드의 이름에 대한 DNS 쿼리를 다른 도메인(example.com or example.net) 또는 하위 도메인(acme.example.com or zenith.example.org)으로 매핑합니다.

> **Important**
>
> DNS 프로토콜을 사용하면 Zone Apex라고 하는 DNS 네임스페이스의 최상위 노드에 대한 CNAME 레코드를 생성할 수 없습니다. 예를 들어, DNS 이름 example.com을 등록하면 zone apex는 example.com입니다. example.com에 대한 CNAME 레코드를 생성할 수는 없지만, www.example.com, newproduct.example.com 등에 대한 CNAME 레코드는 생성할 수 있습니다.
>
> 뿐만 아니라, 하위 도메인에 대한 CNAME 레코드를 생성하면, 그 하위 도메인에 대해서는 다른 레코드를 생성할 수 없습니다. 예를 들어 www.example.com에 대한 CNAME을 생성한 경우, 이름 필드의 값이 www.example.com인 다른 레코드는 생성할 수 없습니다.

또한 Amazon Route 53는 CloudFront 배포 및 Amazon S3 버킷과 같은 선택된 AWS 리소스로 쿼리를 라우팅할 수 있는 별칭 레코드를 지원합니다. 별칭들은 어떤 면에서 CNAME 레코드 유형과 유사하지만, zone apex에 대한 별칭을 생성할 수 있습니다. 자세한 내용은 별칭 또는 비 별칭 레코드 선택 단원을 참조하십시오.

Route 53 콘솔에 대한 예제

```
hostname.example.com
```

Route 53 API에 대한 예제

```
<Value>hostname.example.com</Value>
```

DS 레코드 유형

DS(Delegation Signer) 레코드는 위임된 하위 도메인 영역의 영역 키를 참조합니다. DNSSEC 서명을 구성할 때 신뢰 체인을 설정하면 DS 레코드를 만들 수 있습니다. Route 53의 DNSSEC 구성에 관한 정보는 Amazon Route 53에서 DNSSEC 서명 구성 섹션을 참조하세요.

처음 세 개의 값은 키 태그, 알고리즘 및 다이제스트 유형을 나타내는 10진수입니다. 네 번째 값은 영역 키의 다이제스트입니다. DS 레코드 유형에 대한 자세한 내용은 RFC 4034를 참조하세요.

Route 53 콘솔에 대한 예제

```
123 4 5 1234567890abcdef1234567890absdef
```

Route 53 API에 대한 예제

```
<Value>123 4 5 1234567890abcdef1234567890absdef</Value>
```

HTTPS 레코드 유형

HTTPS 리소스 레코드는 확장 구성 정보를 제공하는 서비스 바인딩(SVCB) DNS 레코드의 한 형태로, 클라이언트가 HTTP 프로토콜을 사용하여 서비스에 쉽고 안전하게 연결할 수 있습니다. 구성 정보는 여러 DNS 쿼리가 필요하지 않고 하나의 DNS 쿼리에서 연결을 허용하는 파라미터로 제공됩니다.

HTTPS 리소스 레코드의 형식은 다음과 같습니다.

```
SvcPriority TargetName SvcParams(optional)
```

다음 파라미터는 RFC 9460, 섹션 9.1에 설명되어 있습니다.

SvcPriority

우선 순위를 나타내는 정수입니다. 우선 순위 0은 별칭 모드를 의미하며 일반적으로 영역 정점에서 별칭을 지정하기 위한 것입니다. 이 값은 Route 53의 경우 정수 0-32767이며,이 중 1-32767은 서비스 모드 레코드입니다. 우선 순위를 낮추고 기본 설정을 높입니다.

TargetName

별칭 대상(별칭 모드의 경우) 또는 대체 엔드포인트(ServiceMode의 경우)의 도메인 이름입니다.

SvcParams(선택 사항)

각 파라미터가 Key=Value 페어 또는 독립 실행형 키로 구성된 공백으로 구분된 목록입니다. 값이 두 개 이상인 경우 쉼표로 구분된 목록으로 표시됩니다. 다음은 정의된 SvcParams입니다.

- `1:alpn` - 애플리케이션 계층 프로토콜 협상 프로토콜 IDs 기본값은 HTTP/1.1이고, h2는 TLS를 통한 HTTP/2이며, h3는 HTTP/3(QUIC 프로토콜을 통한 HTTP)입니다.
- `2:no-default-alpn` - 기본값은 지원되지 않으므로 `alpn` 파라미터를 제공해야 합니다.
- `3:port` - 대체 엔드포인트 또는 서비스에 연결할 수 있는 포트입니다.
- `4:ipv4hint` – IPv4 주소 힌트.
- `5:ech` – 암호화된 클라이언트 Hello.
- `6:ipv6hint` – IPv6 주소 힌트.
- `7:dohpath` – HTTPS를 통한 DNS 템플릿
- `8:ohttp` - 서비스가 작동하고 Oblivious HTTP 대상

별칭 모드용 Amazon Route 53 콘솔 예제

```
0 example.com
```

서비스 모드용 Amazon Route 53 콘솔의 예

```
16 example.com alpn="h2,h3" port=808
```

별칭 모드용 Amazon Route 53 API 예제

```
<Value>0 example.com</Value>
```

서비스 모드용 Route 53 API의 예

```
<Value>16 example.com alpn="h2,h3" port=808</Value>
```

자세한 내용은 RFC 9460, DNS를 통한 서비스 바인딩 및 파라미터 사양(SVCB 및 HTTPS 리소스 레코드)을 참조하세요.

> **Note**
>
> Route 53은 임의의 알 수 없는 키 프레젠테이션 형식을 지원하지 않습니다. `keyNNNNN`

MX 레코드 유형

MX 레코드는 메일 서버의 이름을 지정하고, 두 개 이상의 메일 서버가 있는 경우 우선 순위를 지정합니다. MX 레코드의 각 값마다 다음과 같은 두 가지 값인 우선 순위와 도메인 이름이 포함됩니다.

우선순위

이메일 서버의 우선 순위를 나타내는 정수. 서버를 1개만 지정하는 경우 우선 순위는 0~65535의 정수가 될 수 있습니다. 서버를 다수 지정하는 경우 우선 순위로 지정하는 값은 이메일이 라우팅되는 이메일 서버의 순서를 의미합니다. priority 값이 가장 낮은 서버가 우선 순위를 갖습니다. 예를 들어 이메일 서버가 2개이고 우선 순위로 10과 20을 지정하면, 사용할 수 없는 경우를 제외하고 이메일이 항상 우선 순위가 10인 서버로 라우팅됩니다. 하지만 10과 10으로 지정하면 이메일이 거의 동일하게 두 서버로 라우팅됩니다.

도메인 이름

이메일 서버의 도메인 이름. A 또는 AAAA 레코드의 이름(예: mail.example.com)을 지정합니다. RFC 2181, Clarifications to the DNS Specification의 단원 10.3에서는 도메인 이름 값에 CNAME 레코드의 이름 지정을 금지합니다. (RFC에서 언급하는 "별칭"은 Route 53 별칭 레코드가 아닌 CNAME 레코드를 의미합니다.)

Amazon Route 53 콘솔에 대한 예제

```
10 mail.example.com
```

Route 53 API에 대한 예제

```
<Value>10 mail.example.com</Value>
```

NAPTR 레코드 유식

이름 인증 포인터(NAPTR)는 하나의 값을 또 다른 값으로 변환하거나 대체하기 위해 Dynamic Delegation Discovery System(DDDS) 애플리케이션에서 사용하는 레코드의 유형입니다. 예를 들어, 하나의 일반적인 용도는 전화번호를 SIP URI로 변환하는 것입니다.

NAPTR 레코드의 `Value` 요소는 공백으로 구분된 6개의 값으로 구성되어 있습니다.

Order

레코드를 두 개 이상 지정할 때 DDDS 애플리케이션이 레코드를 평가하도록 할 시퀀스입니다. 유효한 값은 0~65535입니다.

기본 설정

[Order]가 동일하게 지정된 레코드를 세 개 이상 지정할 경우 이러한 레코드가 평가되는 시퀀스에 대한 기본 설정입니다. 예를 들어, 두 개의 레코드에 [Order]가 1로 지정된 경우 DDDS 애플리케이션이 더 낮은 [Preference]이 적용되는 레코드를 먼저 평가합니다. 유효한 값은 0~65535입니다.

플래그

DDDS 애플리케이션에 고유한 설정입니다. RFC 3404에 현재 정의된 값은 대문자 및 소문자 ["A"], ["P"], ["S"] 및 ["U"]와 빈 문자열 [""]입니다. [Flags]는 인용 부호로 묶여 있습니다.

Service

DDDS 애플리케이션에 고유한 설정입니다. [Service]는 인용 부호로 묶여 있습니다.

자세한 내용은 관련 RFC를 참조하십시오.

- URI DDDS 애플리케이션 - https://tools.ietf.org/html/rfc3404#section-4.4
- S-NAPTR DDDS 애플리케이션 - https://tools.ietf.org/html/rfc3958#section-6.5
- U-NAPTR DDDS 애플리케이션 - https://tools.ietf.org/html/rfc4848#section-4.5

Regexp

DDDS 애플리케이션에서 입력 값을 출력 값으로 변환하는 데 사용하는 정규식입니다. 예를 들어, IP 전화 시스템에서 사용자가 입력한 전화번호를 SIP URI로 변환하는 정규식을 사용할 수 있습니다. [Regexp]는 인용 부호로 묶여 있습니다. [Regexp]의 값 또는 [Replacement]의 값 중 하나만 지정합니다.

정규식에 다음과 같은 인쇄 가능한 ASCII 문자를 포함할 수 있습니다.

- a-z
- 0~9
- - (하이픈)
- (공백)
- ! # $ % & ' ( ) * + , - / : ; < = > ? @ [ ] ^ _ ` { | } ~ .
- "(인용 부호) 문자열에 리터럴 따옴표를 포함하려면 \ 문자를 앞에 입력합니다(\").
- \ (backslash). 문자열에 백슬래시를 포함하려면 \ 문자를 앞에 입력합니다(\\).

다국어 도메인 이름과 같은 기타 모든 값은 8진수 형식으로 지정합니다.

Regexp에 대한 구문을 보려면 RFC 3402, 3.2절 대체식 구문을 참조하십시오.

대체

DDDS 애플리케이션에서 DNS 쿼리를 제출하도록 할 다음 도메인 이름의 정규화된 도메인 이름(FQDN)입니다. DDDS 애플리케이션이 입력 값을 [Replacement]에 지정하는 값으로 대체합니다(있는 경우). [Regexp]의 값 또는 [Replacement]의 값 중 하나만 지정합니다. Regexp의 값을 지정하는 경우에는 점(.)을 교체에 지정합니다.

도메인 이름에 a-z, 0-9 및 -(하이픈)을 포함할 수 있습니다.

DDDS 애플리케이션 및 NAPTR 레코드에 대한 자세한 내용은 다음 RFC를 참조하십시오.

- RFC 3401
- RFC 3402
- RFC 3403
- RFC 3404

Amazon Route 53 콘솔에 대한 예제

```
100 50 "u" "E2U+sip" "!^(\\+441632960083)$!sip:\\1@example.com!" .
100 51 "u" "E2U+h323" "!^\\+441632960083$!h323:operator@example.com!" .
100 52 "u" "E2U+email:mailto" "!^.*$!mailto:info@example.com!" .
```

Route 53 API에 대한 예제

```
<ResourceRecord>
   <Value>100 50 "u" "E2U+sip" "!^(\\+441632960083)$!sip:\\1@example.com!" .</Value>
   <Value>100 51 "u" "E2U+h323" "!^\\+441632960083$!h323:operator@example.com!" .</
Value>
   <Value>100 52 "u" "E2U+email:mailto" "!^.*$!mailto:info@example.com!" .</Value>
</ResourceRecord>
```

NS 레코드 유형

NS 레코드는 호스팅 영역에 대한 이름 서버를 식별합니다. 다음 사항에 유의하세요.

- NS 레코드의 가장 일반적인 용도는 도메인에 대해 인터넷 트래픽이 라우팅되는 방식을 제어하는 것입니다. 호스팅 영역의 레코드를 사용하여 도메인의 트래픽을 라우팅하려면 기본 NS 레코드에 있는 네 개의 이름 서버를 사용하도록 도메인 등록 설정을 업데이트합니다. 이는 호스팅 영역과 이름이 같은 NS 레코드입니다.

- 하위 도메인(acme.example.com)에 대해 별도의 호스팅 영역을 생성하고 해당 호스팅 영역을 사용하여 하위 도메인과 그 하위 도메인(subdomain.acme.example.com)에 대한 인터넷 트래픽을 라우팅할 수 있습니다. 루트 도메인(example.com)에 대한 호스팅 영역에 다른 NS 레코드를 생성하여 "하위 도메인에 대한 책임을 호스팅 영역으로 위임"이라고 하는 이 구성을 설정합니다. 자세한 내용은 하위 도메인에 대한 트래픽 라우팅 단원을 참조하십시오.
- 또한 NS 레코드를 사용하여 화이트 레이블 이름 서버를 구성합니다. 자세한 내용은 화이트 레이블 이름 서버 구성 단원을 참조하십시오.

NS 및 SOA 레코드에 대한 자세한 내용은 Amazon Route 53에서 퍼블릭 호스팅 영역에 대해 생성하는 NS 및 SOA 레코드 단원을 참조하십시오.

Amazon Route 53 콘솔에 대한 예제

```
ns-1.example.com
```

Route 53 API에 대한 예제

```
<Value>ns-1.example.com</Value>
```

PTR 레코드 유형

PTR 레코드는 IP 주소를 해당 도메인 이름에 매핑합니다.

Amazon Route 53 콘솔에 대한 예제

```
hostname.example.com
```

Route 53 API에 대한 예제

```
<Value>hostname.example.com</Value>
```

SOA 레코드 유형

권한 시작(SOA) 레코드에는 도메인 및 해당 Amazon Route 53 호스팅 영역에 대한 정보가 제공됩니다. SOA 레코드의 필드에 대한 자세한 내용은 Amazon Route 53에서 퍼블릭 호스팅 영역에 대해 생성하는 NS 및 SOA 레코드 단원을 참조하십시오.

Route 53 콘솔에 대한 예제

```
ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60
```

Route 53 API에 대한 예제

```
<Value>ns-2048.awsdns-64.net hostmaster.awsdns.com 1 1 1 1 60</Value>
```

SPF 레코드 유형

SPF 레코드는 이전에는 이메일 메시지 발신자의 자격 증명을 확인하는 데 사용되었습니다. 그러나 레코드 유형이 SPF인 레코드 생성은 권장하지 않습니다. RFC 7208, 즉 Sender Policy Framework(SPF) for Authorizing Use of Domains in Email, Version 1(이메일에서 도메인 사용을 인증하기 위한 메일 서버 등록제, 버전 1)은 "...[RFC4408]에 정의된 그 존재 및 메커니즘은 어떤 상호 운용성 문제로 귀결되었다. 따라서 SPF 버전 1에 대해 그것을 사용하는 것은 이제 적절하지 않다. 구현은 그것을 사용해서는 안 된다"라는 내용으로 업데이트되었습니다. RFC 7208에서는 14.1 섹션인 SPF DNS 레코드 유형을 참조하십시오.

저희는 SPF 레코드 대신에 해당되는 값을 포함하는 TXT 레코드를 생성하도록 권장합니다. 유효한 값에 대한 자세한 내용은 Wikipedia 기사 Sender Policy Framework를 참조하십시오.

Amazon Route 53 콘솔에 대한 예제

```
"v=spf1 ip4:192.168.0.1/16 -all"
```

Route 53 API에 대한 예제

```
<Value>"v=spf1 ip4:192.168.0.1/16 -all"</Value>
```

SRV 레코드 유형

SRV 레코드 `Value` 요소는 공백으로 구분된 4개의 값으로 구성되어 있습니다. 처음의 세 값은 우선 순위, 가중치, 포트를 나타내는 10진수들입니다. 4번째 값은 도메인 이름입니다. SRV 레코드는 이메일 또는 통신용 서비스 등의 서비스에 액세스하는 데 사용됩니다. SRV 레코드 유형에 대한 자세한 내용은 연결할 서비스의 설명서를 참조하세요.

Amazon Route 53 콘솔에 대한 예제

```
10 5 80 hostname.example.com
```

Route 53 API에 대한 예제

```
<Value>10 5 80 hostname.example.com</Value>
```

SSHFP 레코드 유형

Secure Shell 지문 레코드(SSHFP)는 도메인 이름과 연결된 SSH 키를 식별합니다. 신뢰 체인을 설정하려면 DNSSEC로 SSHFP 레코드를 보호해야 합니다. DNSSEC에 대한 자세한 내용은 섹션을 참조하세요. Amazon Route 53에서 DNSSEC 서명 구성

SSHFP 리소스 레코드의 형식은 다음과 같습니다.

```
[Key Algorithm] [Hash Type] Fingerprint
```

다음 파라미터는 RFC 4255에 정의되어 있습니다.

키 알고리즘

알고리즘 유형:

- 0 - 예약되어 있으며 사용되지 않습니다.
- 1: RSA – Rivest–Shamir–Adleman 알고리즘은 최초의 퍼블릭 키 암호화 시스템 중 하나이며 보안 데이터 전송에 여전히 사용되고 있습니다.
- 2: DSA - 디지털 서명 알고리즘은 디지털 서명을 위한 연방 정보 처리 표준입니다. DSA는 모듈식 지수와 이산 로그 수학 모델을 기반으로 합니다.
- 3: ECDSA - 타원 곡선 디지털 서명 알고리즘은 타원 곡선 암호화를 사용하는 DSA의 변형입니다.
- 4: Ed25519 – Ed25519 알고리즘은 SHA-512(SHA-2) 및 Curve25519를 사용하는 EdDSA 서명 체계입니다.
- 6: Ed448 – Ed448은 SHAKE256 및 Curve448을 사용하는 EdDSA 서명 체계입니다.

해시 유형

퍼블릭 키 해시를 생성하는 데 사용되는 알고리즘:

- 0 - 예약되어 있고 사용되지 않습니다.
- 1: SHA-1
- 2: SHA-256

지문

해시의 16진수 표현입니다.

Amazon Route 53 콘솔에 대한 예제

```
1 1 09F6A01D2175742B257C6B98B7C72C44C4040683
```

Route 53 API에 대한 예제

```
<Value>1 1 09F6A01D2175742B257C6B98B7C72C44C4040683</Value>
```

자세한 내용은 RFC 4255: DNS를 사용하여 보안 쉘(SSH) 키 지문을 안전하게 게시하기를 참조하세요.

SVCB 레코드 유형

SVCB 레코드를 사용하여 서비스 엔드포인트에 액세스하기 위한 구성 정보를 제공합니다. SVCB는 일반 DNS 레코드이며 다양한 애플리케이션 프로토콜의 파라미터를 협상하는 데 사용할 수 있습니다.

SVCB 리소스 레코드의 형식은 다음과 같습니다.

`SvcPriority TargetName SvcParams(optional)`

다음 파라미터는 RFC 9460, 섹션 2.3에 설명되어 있습니다.

SvcPriority

우선 순위를 나타내는 정수입니다. 우선 순위 0은 별칭 모드를 의미하며 일반적으로 영역 정점에서 별칭을 지정하기 위한 것입니다. 우선 순위를 낮추고 기본 설정을 높입니다.

TargetName

별칭 대상(별칭 모드의 경우) 또는 대체 엔드포인트(ServiceMode의 경우)의 도메인 이름입니다.

SvcParams(선택 사항)

각 파라미터가 Key=Value 페어 또는 독립 실행형 키로 구성된 공백으로 구분된 목록입니다. 값이 두 개 이상인 경우 쉼표로 구분된 목록으로 표시됩니다. 이 값은 Route 53의 경우 정수 0-32767이며,이 중 1-32767은 서비스 모드 레코드입니다. 다음은 정의된 SvcParams입니다.

- `1:alpn` - 애플리케이션 계층 프로토콜 협상 프로토콜 IDs 기본값은 HTTP/1.1이고, h2는 TLS를 통한 HTTP/2이며, h3는 HTTP/3(QUIC 프로토콜을 통한 HTTP)입니다.
- `2:no-default-alpn` - 기본값은 지원되지 않으므로 `alpn` 파라미터를 제공해야 합니다.
- `3:port` - 서비스에 연결할 수 있는 대체 엔드포인트의 포트입니다.
- `4:ipv4hint` – IPv4 주소 힌트.

- `5:ech` – 암호화된 클라이언트 Hello.
- `6:ipv6hint` – IPv6 주소 힌트.
- `7:dohpath` – HTTPS를 통한 DNS 템플릿
- `8:ohttp` - 서비스가 Oblivious HTTP 대상을 운영합니다.

별칭 모드용 Amazon Route 53 콘솔 예제

```
0 example.com
```

서비스 모드용 Amazon Route 53 콘솔의 예

```
16 example.com alpn="h2,h3" port=808
```

별칭 모드용 Amazon Route 53 API 예제

```
<Value>0 example.com</Value>
```

서비스 모드용 Route 53 API의 예

```
<Value>16 example.com alpn="h2,h3" port=808</Value>
```

자세한 내용은 RFC 9460, DNS를 통한 서비스 바인딩 및 파라미터 사양(SVCB 및 HTTPS 리소스 레코드)을 참조하세요.

> **Note**
>
> Route 53은 임의의 알 수 없는 키 프레젠테이션 형식을 지원하지 않습니다. `keyNNNNN`

TLSA 레코드 유형

TLSA 레코드를 사용하여 명명된 개체의 DNS 기반 인증(DANE)을 사용합니다. TLSA 레코드는 인증서/퍼블릭 키를 전송 계층 보안(TLS) 엔드포인트와 연결하며, 클라이언트는 DNSSEC로 서명된 TLSA 레코드를 사용하여 인증서/퍼블릭 키를 검증할 수 있습니다.

도메인에서 DNSSEC가 활성화된 경우에만 TLSA 레코드를 신뢰할 수 있습니다. DNSSEC에 대한 자세한 내용은 섹션을 참조하세요. Amazon Route 53에서 DNSSEC 서명 구성

TLSA 리소스 레코드의 형식은 다음과 같습니다.

```
[Certificate usage] Selector [Matching type] [Certificate association data]
```

다음 파라미터는 RFC 6698, 섹션 3에 지정되어 있습니다.

인증서 사용

TLS 핸드셰이크에 제공된 인증서와 일치시키는 데 사용할 제공된 연결을 지정합니다.

- 0: CA 제약 조건 - 인증서 또는 퍼블릭 키는 TLS에서 서버에서 제공하는 최종 개체 인증서의 퍼블릭 키 인프라(PKIX) 인증 경로에서 찾을 수 있어야 합니다. 이 제약 조건은 지정된 서비스에 대한 인증서를 발급하는 데 사용할 수 있는 CAs를 제한합니다.
- 1: 서비스 인증서 제약 조건 - TLS에서 서버에서 제공한 최종 개체 인증서와 일치해야 하는 최종 개체 인증서(또는 퍼블릭 키)를 지정합니다. 이 인증은 호스트의 지정된 서비스에서 사용할 수 있는 최종 엔터티 인증서를 제한합니다.
- 2: 신뢰 앵커 어설션 - TLS에서 서버에서 제공하는 최종 엔터티 인증서를 검증할 때 '트러스트 앵커'로 사용해야 하는 인증서(또는 퍼블릭 키)를 지정합니다. 도메인 관리자가 신뢰 앵커를 지정할 수 있습니다.
- 3: 도메인 발급 인증 - TLS에서 서버에서 제공한 최종 엔터티 인증서와 일치해야 하는 인증서(또는 퍼블릭 키)를 지정합니다. 이 인증을 통해 도메인 관리자는 타사 CA를 사용하지 않고 도메인에 대한 인증서를 발급할 수 있습니다. 이 인증서는 PKIX 검증을 통과할 필요가 없습니다.

Selector

핸드셰이크에서 서버에서 제공하는 인증서의 어떤 부분이 연결 값과 일치하는지 지정합니다.

- 0: 전체 인증서가 일치해야 합니다.
- 1: Subject Public Key 또는 DER 인코딩 바이너리 구조가 일치해야 합니다.

일치하는 유형

인증서 일치의 프레젠테이션(선택기 필드에 의해 결정됨)을 지정합니다.

- 0: 콘텐츠의 정확한 일치.
- 1: SHA-256 해시.
- 2: SHA-512 해시.

인증서 연결 데이터

다른 필드의 설정에 따라 일치시킬 데이터입니다.

Amazon Route 53 콘솔에 대한 예제

```
0 0 1 d2abde240d7cd3ee6b4b28c54df034b97983a1d16e8a410e4561cb106618e971
```

Route 53 API에 대한 예제

```
<Value>0 0 1 d2abde240d7cd3ee6b4b28c54df034b97983a1d16e8a410e4561cb106618e971</Value>
```

자세한 내용은 RFC 6698, DANE(명명된 엔터티의 DNS 기반 인증) TLS(전송 계층 보안) 프로토콜: TLSA를 참조하세요.

TXT 레코드 유형

TXT 레코드는 큰따옴표('')로 묶여 있는 하나 이상의 문자열을 포함합니다. 간단한 라우팅 정책을 사용할 때 도메인(example.com) 또는 하위 도메인(www.example.com)에 대한 모든 값을 같은 TXT 레코드에 포함합니다.

주제

- TXT 레코드 값 입력
- TXT 레코드 값의 특수 문자
- TXT 레코드 값의 대문자 및 소문자
- 예시

TXT 레코드 값 입력

단일 문자열에는 다음을 포함하여 최대 255자가 포함될 수 있습니다.

- a-z
- A-Z
- 0~9
- 공간
- - (하이픈)
- ! " # $ % & ' ( ) * + , - / : ; < = > ? @ [\ ] ^ _ ` { | } ~ .

255자보다 긴 값을 입력해야 하는 경우, 값을 255자 이하의 문자열로 나누고 각 문자열을 큰따옴표('')로 묶습니다. 콘솔에서 모든 문자열을 같은 줄에 나열하십시오.

```
"String 1" "String 2" "String 3"
```

API의 경우 동일한 Value 요소에 모든 문자열을 포함시킵니다.

```
<Value>"String 1" "String 2" "String 3"</Value>
```

TXT 레코드의 최대 값 길이는 4,000자입니다.

TXT 값을 하나 이상 입력하려면 행당 하나의 값을 입력합니다.

TXT 레코드 값의 특수 문자

TXT 레코드에 다음 문자가 포함되어 있는 경우, *three-digit octal code* 형식의 이스케이프 코드를 사용하여 문자를 지정해야 합니다.

- 000 - 040 사이의 8진수 문자(0 - 32 사이의 10진수, 0x00 - 0x20 사이의 16진수)
- 177 - 377 사이의 8진수 문자(127 - 255 사이의 10진수, 0x7F - 0xFF 사이의 16진수)

예를 들어 TXT 레코드의 값이 "exämple.com"인 경우 "ex\344mple.com"을 지정합니다.

ASCII 문자와 옥탈 코드 간의 매핑을 위해 인터넷에서 "ASCII 옥탈 코드"를 검색합니다. 한 가지 유용한 참조 웹 페이지는 ASCII Code - The extended ASCII table입니다.

문자열에 인용 부호(")를 포함하려면 인용 부호 앞에 백래시(\) 문자를 넣으십시오(즉, \").

TXT 레코드 값의 대문자 및 소문자

대/소문자가 유지되므로 "Ab"와 "aB"는 서로 다른 값임에 유의하십시오.

예시

Amazon Route 53 콘솔에 대한 예제

각 값을 별도의 라인에 입력합니다.

```
"This string includes \"quotation marks\"."
"The last character in this string is an accented e specified in octal format: \351"
"v=spf1 ip4:192.168.0.1/16 -all"
```

Route 53 API에 대한 예제

각 값을 별도의 Value 요소에 입력합니다.

```
<Value>"This string includes \"quotation marks\"."</Value>
<Value>"The last character in this string is an accented e specified in octal format:
 \351"</Value>
<Value>"v=spf1 ip4:192.168.0.1/16 -all"</Value>
```

Amazon Route 53 콘솔을 사용하여 레코드 생성

다음 절차는 Amazon Route 53 콘솔을 사용하여 레코드를 생성하는 방법을 설명합니다. Route 53 API를 사용하여 레코드를 생성하는 방법에 대한 자세한 내용은 Amazon Route 53 API 참조의 ChangeResourceRecordSets를 참조하세요.

> **Note**
>
> 복잡한 라우팅 구성에 대한 레코드를 만들려면 트래픽 흐름 시각적 편집기를 사용하고 구성을 트래픽 정책으로 저장할 수도 있습니다. 그런 다음 동일한 호스팅 영역이나 여러 호스팅 영역의 하나 이상의 도메인 이름(예: example.com) 또는 하위 도메인 이름(예: www.example.com)과 해당 트래픽 정책을 연결할 수 있습니다. 새 구성이 예상대로 수행되지 않을 경우 업데이트를 롤백할 수도 있습니다. 자세한 내용은 트래픽 흐름을 사용하여 DNS 트래픽 라우팅 단원을 참조하십시오.

Route 53 콘솔을 사용하여 라우팅을 생성하려면

1. 별칭 레코드를 생성하지 않는 경우에는 2단계로 이동합니다.

   또한 DNS 트래픽을 Elastic Load Balancing 로드 밸런서 또는 다른 Route 53 레코드 이외의 AWS 리소스로 라우팅하는 별칭 레코드를 생성하는 경우 2단계로 이동합니다.

   트래픽을 Elastic Load Balancing 로드 밸런서로 라우팅하는 별칭 레코드를 생성하는 경우, 그리고 서로 다른 계정을 사용해 호스팅 영역 및 로드 밸런서를 생성한 경우에는 Elastic Load Balancing 로드 밸런서의 DNS 이름 가져오기의 절차를 수행해 로드 밸런서에 대한 DNS 이름을 가져옵니다.
2. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
3. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
4. 도메인의 호스팅 영역이 이미 있다면 5단계로 건너뜁니다. 없다면 해당 절차를 수행하여 호스팅 영역을 생성합니다.

- 인터넷 트래픽을 Amazon S3 버킷 또는 Amazon EC2 인스턴스 같은 리소스로 라우팅하려면 퍼블릭 호스팅 영역 생성을 참조하세요.
- VPC에서 트래픽을 라우팅하려면 프라이빗 호스팅 영역 생성을 참조하십시오.

5. 호스팅 영역(Hosted Zones) 페이지에서 레코드를 생성할 호스팅 영역의 이름을 선택합니다.
6. 레코드 세트 생성을 선택합니다.
7. 해당하는 라우팅 정책 및 값을 선택하고 정의합니다. 자세한 내용은 생성하려는 레코드의 종류에 대한 주제를 참조하십시오.

   - 모든 라우팅 정책에 공통적인 값
   - 모든 라우팅 정책의 별칭 레코드에 공통되는 값
   - 단순 레코드에 특정한 값
   - 단순 별칭 레코드에 특정한 값
   - 장애 조치 레코드에 특정한 값
   - 장애 조치 별칭 레코드에 특정한 값
   - 지리 위치 레코드에 특정한 값
   - 지리 위치 별칭 레코드에 특정한 값
   - 지리 근접성 레코드에 특정된 값
   - 지리 근접성 별칭 레코드에 특정된 값
   - 지연 시간 레코드에 특정한 값
   - 지연 시간 별칭 레코드에 특정한 값
   - IP 기반 레코드에 특정한 값
   - IP 기반 별칭 레코드에 특정한 값
   - 다중값 응답 레코드에 특정한 값
   - 가중치 기반 레코드에 특정한 값
   - 가중치 기반 별칭 레코드에 특정한 값
8. 레코드 생성을 선택합니다.

> **Note**
>
> 새 레코드는 Route 53 DNS 서버로 전파되기까지 시간이 걸립니다. 현재 변경 사항의 전파 여부를 확인하는 유일한 방법은 GetChange API 작업을 사용하는 것입니다. 변경 사항은 일반적으로 60초 이내에 모든 Route 53 이름의 서버로 전파됩니다.

9. 레코드를 여러 개 생성하는 경우에는 7~8단계를 반복합니다.

Elastic Load Balancing 로드 밸런서의 DNS 이름 가져오기

1. 별칭 레코드를 생성할 Classic, Application 또는 Network Load Balancer를 생성하는 데 사용된 AWS 계정을 AWS Management Console 사용하여에 로그인합니다.
2. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
3. 탐색 창에서 [Load Balancers]를 클릭합니다.
4. 로드 밸런서 목록에서 별칭 레코드를 만들고자 하는 로드 밸런서를 선택합니다.
5. [Description] 탭에서 [DNS name] 값을 찾습니다.
6. 다른 Elastic Load Balancing 로드 밸런서를 위한 별칭 레코드를 생성하고 싶다면, 4~5단계를 반복하세요.
7. 에서 로그아웃합니다 AWS Management Console.
8. Route 53 호스팅 영역을 생성하는 데 사용한 AWS 계정을 사용하여에 AWS Management Console 다시 로그인합니다.
9. Amazon Route 53 콘솔을 사용하여 레코드 생성 절차의 3단계로 돌아갑니다.

리소스 레코드 세트 권한

리소스 레코드 세트 권한은 ID 및 액세스 관리(IAM) 정책 조건을 사용하여 Route 53 콘솔에서의 작업 또는 ChangeResourceRecordSets API 사용에 대해 세분화된 권한을 설정할 수 있습니다.

리소스 레코드 세트는 동일한 이름과 유형(그리고 클래스가 있음. 하지만 대부분의 용도에서 클래스는 항상 IN, 즉 인터넷임)을 가진 여러 리소스 레코드로 정의되나, 서로 다른 데이터를 포함합니다. 예를 들어 지리적 위치 라우팅을 선택한 경우 동일한 도메인의 서로 다른 엔드포인트를 가리키는 A 레코드나 AAAA 레코드가 여러 개 있을 수 있습니다. 이러한 A 레코드나 AAAA 레코드가 모두 함께 리소스 레코드 세트를 구성합니다. DNS 용어에 대한 자세한 내용은 RFC 7719를 참조하세요.

IAM 정책 조건인 `route53:ChangeResourceRecordSetsActions`, `route53:ChangeResourceRecordSetsRecordTypes`및 `route53:ChangeResourceRecordSetsNormalizedRecordNames`를 사용하면 다른 AWS 계정의 다른 AWS 사용자에게 세분화된 관리 권한을 부여할 수 있습니다. 다른 사람에게 다음 권한을 부여할 수 있습니다.

- 단일 리소스 레코드 세트.

- 특정 DNS 레코드 유형의 모든 리소스 레코드 세트.
- 이름에 특정 문자열이 포함된 리소스 레코드 세트.
- ChangeResourceRecordSets API 또는 Route 53 콘솔을 사용할 때는 `CREATE | UPSERT | DELETE` 작업 중 아무거나 또는 모두를 수행합니다.

어떤 Route 53 정책 조건이든 결합된 액세스 권한을 생성할 수도 있습니다. 예를 들어, 다른 사람에게 markeing-example.com의 A 레코드 데이터를 수정할 수 있는 권한을 부여하고, 해당 사용자가 레코드를 삭제하도록 허용하지 않을 수 있습니다.

리소스 레코드 세트 권한 및 사용 방법에 대한 예제에 대한 자세한 내용은 섹션을 참조하세요IAM 정책 조건을 사용하여 세분화된 액세스 제어 구현.

AWS 사용자를 인증하는 방법은 섹션을 참조ID를 통한 인증하고 Route 53 리소스에 대한 액세스를 제어하는 방법은 섹션을 참조하세요액세스 제어.

Amazon Route 53 레코드를 생성 또는 편집할 때 지정하는 값

Amazon Route 53 콘솔을 사용하여 레코드를 생성할 때 지정하는 값은 사용하려는 라우팅 정책과 트래픽을 AWS 리소스로 라우팅하는 별칭 레코드를 생성할지 여부에 따라 달라집니다.

대상 AWS 리소스를 지정하는 특정 리소스(예: Elastic Load Balancing, CloudFront 배포, Amazon S3 버킷)로 트래픽을 라우팅하는 별칭 레코드입니다. 선택적으로 상태 확인을 연결하고 대상 상태 평가를 구성할 수도 있습니다. 다음 주제에서는 각 라우팅 정책 및 레코드 유형에 필요한 값에 대한 상세한 정보를 제공하여 Route 53 레코드를 효과적으로 구성하는 데 도움이 됩니다.

주제

- 지리 근접성 별칭 레코드에 특정된 값
- 지연 시간 레코드에 특정한 값
- 지연 시간 별칭 레코드에 특정한 값
- IP 기반 레코드에 특정한 값
- IP 기반 별칭 레코드에 특정한 값
- 다중값 응답 레코드에 특정한 값
- 가중치 기반 레코드에 특정한 값
- 가중치 기반 별칭 레코드에 특정한 값

모든 라우팅 정책에 공통적인 값

이것은 Amazon Route 53 레코드를 생성 또는 편집할 때 지정할 수 있는 공통적인 값입니다. 이러한 값은 모든 라우팅 정책에서 사용됩니다.

주제

- 레코드 이름
- 값/트래픽 라우팅 대상
- TTL(초)

레코드 이름

트래픽을 라우팅할 도메인 또는 하위 도메인의 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

> **Note**
>
> 호스팅 영역과 이름이 동일한 레코드를 생성할 경우 이름 필드에 값(예: @ 기호)을 입력하지 마십시오.

CNAME 레코드

레코드 유형(Record type) 값이 CNAME인 레코드를 생성하는 경우 레코드의 이름은 호스팅 영역의 이름과 같을 수 없습니다.

특수 문자

a-z, 0-9, -(하이픈) 이외의 문자를 지정하는 방법과 국제 도메인 이름을 지정하는 방법은 다음(DNS 도메인 이름 형식)을 참조하십시오.

와일드카드 문자

이름에 별표(*) 문자를 사용할 수 있습니다. DNS는 이름에 표시되는 위치에 따라 * 문자를 와일드카드 또는 * 문자(ASCII 42)로 처리합니다. 자세한 내용은 호스팅 영역 및 레코드의 이름에 별표(*) 사용 단원을 참조하십시오.

> **Important**
>
> * 와일드카드를 유형이 NS인 리소스 레코드 세트에 사용할 수 없습니다.

값/트래픽 라우팅 대상

IP 주소 또는 레코드 유형에 따라 다른 값(IP address or another value depending on the record type)을 선택합니다. 레코드 유형(Record type) 값에 해당하는 값을 입력합니다. CNAME을 제외한 모든 유형은 둘 이상의 값을 입력할 수 있습니다. 각 값을 별도의 라인에 입력합니다.

A – IPv4 주소

IPv4 형식의 IP 주소(예: 192.0.2.235)

AAAA - IPv6 주소

IPv6 형식의 IP 주소(예: 2001:0db8:85a3:0:0:8a2e:0370:7334)

CAA - 인증 기관 인증

레코드 이름(Record name)으로 지정되는 도메인 또는 하위 도메인에 대한 인증서나 와일드카드 인증서 발급이 허용되는 인증 기관을 제어하는 공백으로 구분된 3개의 값. CAA 레코드를 사용하여 다음을 지정할 수 있습니다.

- SSL/TLS 인증서(있는 경우)를 발급할 수 있는 인증 기관(CA)
- CA가 도메인 또는 하위 도메인에 인증서를 발급할 때 연락처의 이메일 주소 또는 URL

CNAME – 정식 이름

Route 53에서 이 레코드의 DNS 쿼리에 대한 응답으로 반환하려는 정규화된 도메인 이름(예: www.example.com)입니다. 뒤에 오는 점은 선택 사항이며, Route 53은 도메인 이름을 정규화

된 도메인 이름으로 간주합니다. 다시 말해 Route 53은 www.example.com(뒤에 점 없음)과 www.example.com.(뒤에 점 있음)을 동일하게 처리합니다.

MX - 메일 교환

우선 순위와 메일 서버를 지정하는 도메인 이름(예: 10 mailserver.example.com) 뒤에 오는 점은 선택 사항으로 처리됩니다.

NAPTR - 이름 권한 포인터

하나의 값을 또 다른 값으로 변환하거나 대체하기 위해 Dynamic Delegation Discovery System(DDDS) 애플리케이션이 사용하는 공백으로 구분된 6개의 설정. 자세한 내용은 NAPTR 레코드 유식 단원을 참조하십시오.

PTR - 포인터

Route 53이 반환하려는 도메인 이름입니다.

NS - 이름 서버

이름 서버의 도메인 이름(예: ns1.example.com)

> **Note**
>
> 단순 라우팅 정책만 사용하여 NS 레코드를 지정할 수 있습니다.

SPF - 발신자 정책 프레임워크

인용 부호 안에 들어 있는 SPF 레코드(예: "v=spf1 ip4:192.168.0.1/16-all"). SPF 레코드는 권장되지 않습니다. 자세한 내용은 지원되는 DNS 레코드 유형 단원을 참조하십시오.

SRV - 서비스 로케이터

SRV 기록. SRV 레코드는 이메일 또는 통신용 서비스 등의 서비스에 액세스하는 데 사용됩니다. SRV 레코드 유형에 대한 자세한 내용은 연결할 서비스의 설명서를 참조하세요. 뒤에 오는 점은 선택 사항으로 처리됩니다.

SRV 레코드 유형은 다음과 같습니다.

[우선 순위] [가중치] [포트] [서버 호스트 이름]

예:

1 10 5269 xmpp-server.example.com.

TXT - 텍스트

텍스트 레코드. 인용 부호 안에 들어 있는 텍스트(예: "Sample Text Entry").

TTL(초)

DNS recursive resolver가 이 레코드에 관한 정보를 캐싱할 시간(초)입니다. 더 긴 값(예: 172800초 또는 2일)을 지정한 경우, 이 레코드의 최신 정보를 얻으려면 DNS recursive resolver의 Route 53에 대한 호출 수를 줄여야 합니다. 이렇게 하면 지연 시간을 줄이고 Route 53 서비스 비용을 줄이는 효과가 있습니다. 자세한 내용은 Amazon Route 53가 도메인의 트래픽을 라우팅하는 방법 단원을 참조하십시오.

그러나 TTL에 더 긴 값을 지정하면 recursive resolver가 Route 53에 최신 정보를 요청하기 전에 기간이 더 긴 캐시 값을 사용하므로 레코드(예: 새 IP 주소) 변경이 적용되는 데 걸리는 시간이 길어집니다. 이미 사용 중인 도메인이나 하위 도메인의 설정을 변경하는 경우 처음에는 더 짧은 값(예: 300초)을 지정하고 새 설정이 올바른지 확인한 후 값을 늘리는 것이 좋습니다.

이 레코드를 상태 점검과 연관시킬 경우에는 클라이언트가 상태 변경에 빠르게 응답하도록 TTL을 60초 이하로 지정하는 것이 좋습니다.

모든 라우팅 정책의 별칭 레코드에 공통되는 값

이것은 Amazon Route 53 레코드를 생성 또는 편집할 때 지정할 수 있는 공통적인 별칭 값입니다. 이러한 값은 모든 라우팅 정책에서 사용됩니다.

주제

- 레코드 이름
- 값/트래픽 라우팅 대상

레코드 이름

트래픽을 라우팅할 도메인 또는 하위 도메인의 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

> **Note**
>
> 호스팅 영역과 이름이 동일한 레코드를 생성할 경우 이름 필드에 값(예: @ 기호)을 입력하지 마십시오.

CNAME 레코드

유형 값이 CNAME인 레코드를 생성하는 경우 레코드의 이름은 호스팅 영역의 이름과 같을 수 없습니다.

CloudFront 배포 및 Amazon S3 버킷에 대한 별칭

지정하는 값은 트래픽을 라우팅하는 AWS 리소스에 따라 부분적으로 달라집니다.

- CloudFront 배포(CloudFront distribution) – 배포에 레코드 이름과 일치하는 대체 도메인 이름이 포함되어야 합니다. 예를 들어, 레코드 이름이 acme.example.com인 경우 CloudFront 배포에 acme.example.com이 대체 도메인 이름 중 하나로 포함되어야 합니다. 자세한 내용은 Amazon CloudFront 개발자 안내서에서 대체 도메인 이름(CNAME) 사용을 참조하세요.
- Amazon S3 버킷 - 레코드 이름은 Amazon S3 버킷 이름과 일치해야 합니다. 예를 들어, 버킷의 이름이 acme.example.com이면 이 레코드의 이름도 acme.example.com이어야 합니다.

  그리고 웹사이트 호스팅용 버킷을 구성해야 합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 웹 사이트 호스팅에 대한 버킷 구성을 참조하십시오.

특수 문자

a-z, 0-9, -(하이픈) 이외의 문자를 지정하는 방법과 국제 도메인 이름을 지정하는 방법은 다음(DNS 도메인 이름 형식)을 참조하십시오.

와일드카드 문자

이름에 별표(*) 문자를 사용할 수 있습니다. DNS는 이름에 표시되는 위치에 따라 * 문자를 와일드카드 또는 * 문자(ASCII 42)로 처리합니다. 자세한 내용은 호스팅 영역 및 레코드의 이름에 별표(*) 사용 단원을 참조하십시오.

값/트래픽 라우팅 대상

목록에서 선택하거나 필드에 입력하는 값은 트래픽을 라우팅하는 AWS 리소스에 따라 달라집니다.

트래픽을 특정 AWS 리소스로 라우팅하도록 Route 53를 구성하는 방법에 대한 자세한 내용은 섹션을 참조하세요AWS 리소스로 인터넷 트래픽 라우팅.

Important

동일한 AWS 계정을 사용하여 트래픽을 라우팅하는 호스팅 영역과 리소스를 생성하고 리소스가 엔드포인트 목록에 표시되지 않는 경우 다음을 확인합니다.

- 레코드 유형(Record type)에 대해 지원되는 값을 선택했는지 확인합니다. 지원되는 값은 트래픽을 라우팅하는 리소스에 고유합니다. 예를 들어 S3 버킷으로 트래픽을 라우팅하려면 레코드 유형(Record type에 대한 A - IPv4 주소를 선택해야 합니다.
- 계정에 해당 리소스를 나열하는 데 필요한 IAM 권한이 있는지 확인합니다. 예를 들어, CloudFront 배포가 엔드포인트(Endpoint) 목록에 나타나려면, 계정에 `cloudfront:ListDistributions` 작업을 수행할 권한이 있어야 합니다.

  IAM 정책 예제는 Amazon Route 53 콘솔 사용에 필요한 권한 단원을 참조하세요.

다른 AWS 계정을 사용하여 호스팅 영역과 리소스를 생성한 경우 엔드포인트 목록에 리소스가 표시되지 않습니다. 리소스 유형이 엔드포인트(Endpoint)에 입력할 값을 결정하려면 다음 문서를 참조하세요.

API Gateway 사용자 지정 리전 API와 엣지 최적화 API

API Gateway 사용자 지정 리전 API와 엣지 최적화 API의 경우 다음 중 하나를 수행하세요.

- 동일 계정을 사용하여 Route 53 호스팅 영역과 API를 생성한 경우 - 엔드포인트(Endpoint)를 선택하고 목록에서 API를 선택합니다. API가 많은 경우 API 엔드포인트의 처음 몇 자를 입력하여 목록을 필터링할 수 있습니다.

  > **Note**
  >
  > 이 레코드 이름은 API의 사용자 지정 도메인 이름과 일치해야 합니다(예: api.example.com).

- 다른 계정을 사용하여 Route 53 호스팅 영역과 API를 생성한 경우 - API에 대한 API 엔드포인트(예: api.example.com)를 입력합니다.

  하나의 AWS 계정을 사용하여 현재 호스팅 영역을 생성하고 다른 계정을 사용하여 API를 생성한 경우 API Gateway API 아래의 엔드포인트 목록에 API가 표시되지 않습니다. APIs

  한 계정을 사용하여 현재 호스팅 영역을 생성하고 하나 이상의 다른 계정을 사용하여 모든 API 버킷을 생성한 경우 엔드포인트(Endpoints) 목록에는 API Gateway APIs의 사용 가능한 대상 없음(No Targets Available)이 표시됩니다. 자세한 내용은 도메인 이름을 사용하여 Amazon API Gateway API로 트래픽 라우팅 단원을 참조하십시오.

CloudFront 배포

CloudFront 배포에 대해 다음 중 하나를 수행합니다.

- 동일 계정을 사용하여 Route 53 호스팅 영역과 CloudFront 배포를 생성한 경우 - 엔드포인트(Endpoint)를 선택하고 목록에서 배포를 선택합니다. 배포가 많을 경우에는 배포 도메인 이름의 처음 몇 자를 입력하여 목록을 필터링할 수 있습니다.

  목록에 배포가 없을 때는 다음에 유의하십시오.

  - 이 레코드의 이름은 배포의 대체 도메인 이름과 일치해야 합니다.
  - 배포에 대체 도메인 이름을 추가한 경우 변경 사항이 모든 CloudFront 엣지 로케이션으로 전해지는데 15분 걸릴 수 있습니다. 변경 사항이 전파되기 전까지 Route 53은 새 대체 도메인 이름을 알 수 없습니다.

- 다른 계정을 사용하여 Route 53 호스팅 영역 및 배포를 생성한 경우 - 배포의 CloudFront 도메인 이름을 입력합니다(예: d111111abcdef8.cloudfront.net).

  한 AWS 계정을 사용하여 현재 호스팅 영역을 생성하고 다른 계정을 사용하여 배포를 생성한 경우 엔드포인트 목록에 배포가 표시되지 않습니다.

한 계정을 사용하여 현재 호스팅 영역을 생성하고 하나 이상의 다른 계정을 사용하여 모든 배포를 생성한 경우에는 엔드포인트(Endpoints) 목록에 CloudFront 배포(CloudFront Distributions) 아래 사용 가능한 대상 없음(No Targets Available)이 표시됩니다.

> **Important**
>
> 모든 엣지 로케이션으로 전파되지 않은 CloudFront 배포로 쿼리를 라우팅하지 않거나 사용자가 해당 콘텐츠에 액세스할 수 없습니다.

CloudFront 배포에는 레코드 이름과 일치하는 대체 도메인 이름이 포함되어야 합니다. 예를 들어, 레코드 이름이 acme.example.com인 경우 CloudFront 배포에 acme.example.com이 대체 도메인 이름 중 하나로 포함되어야 합니다. 자세한 내용은 Amazon CloudFront 개발자 안내서에서 대체 도메인 이름(CNAME) 사용을 참조하세요.

배포에 대해 IPv6가 활성화되어 있다면 두 개의 레코드를 생성합니다. 하나는 레코드 유형(Record type) 값이 A - IPv4 주소이고 하나는 값이 AAAA — IPv6 주소입니다. 자세한 내용은 도메인 이름을 사용하여 Amazon CloudFront 배포로 트래픽 라우팅 단원을 참조하십시오.

App Runner 서비스

App Runner 서비스의 경우 다음 중 하나를 수행합니다.

- 동일한 계정을 사용하여 Route 53 호스팅 영역과 App Runner 서비스를 생성한 경우를 선택한 AWS 리전다음 목록에서 트래픽을 라우팅할 환경의 도메인 이름을 선택합니다.
- 다른 계정을 사용하여 Route 53 호스팅 영역과 App Runner를 생성한 경우 - 사용자 지정 도메인 이름을 입력합니다. 자세한 내용은 App Runner의 사용자 지정 도메인 이름 관리를 참조하세요.

  하나의 AWS 계정을 사용하여 현재 호스팅 영역을 생성하고 다른 계정을 사용하여 App Runner를 생성한 경우 App Runner는 엔드포인트 목록에 표시되지 않습니다.

자세한 내용은 Amazon Route 53를 구성하여 App Runner 서비스로 트래픽 라우팅 단원을 참조하십시오.

리전별 하위 도메인이 있는 Elastic Beanstalk 환경

Elastic Beanstalk 환경의 도메인 이름에 환경을 배포한 리전이 포함되는 경우 트래픽을 환경으로 라우팅하는 별칭 레코드를 생성할 수 있습니다. 예를 들어 도메인 이름 `my-environment.us-west-2.elasticbeanstalk.com`은 리전이 지정된 도메인 이름입니다.

> **Important**
>
> 2016년 초 이전에 생성된 환경의 경우 도메인 이름에 리전이 포함되지 않습니다. 이러한 환경으로 트래픽을 라우팅하려면 별칭 레코드 대신에 CNAME 레코드를 생성해야 합니다. 루트 도메인 이름에는 CNAME 레코드를 생성할 수 없습니다. 예를 들어 도메인 이름이 example.com이라면 acme.example.com에 대한 트래픽을 Elastic Beanstalk 환경으로 라우팅하는 레코드를 생성할 수 있습니다. 그러나 example.com에 대한 트래픽을 Elastic Beanstalk 환경으로 라우팅하는 레코드는 생성할 수 없습니다.

리전화된 하위 도메인이 있는 Elastic Beanstalk 환경에 대해서는 다음 중 한 가지 작업을 수행하세요.

- 동일 계정을 사용하여 Route 53 호스팅 영역과 Elastic Beanstalk 환경을 생성한 경우 - 엔드포인트(Endpoint)를 선택하고 목록에서 환경을 선택합니다. 환경이 많을 경우에는 환경에 대한 CNAME 속성의 처음 몇 자를 입력하여 목록을 필터링할 수 있습니다.
- 서로 다른 계정을 사용하여 Route 53 호스팅 영역과 Elastic Beanstalk 환경을 생성한 경우 – Elastic Beanstalk 환경에 대한 CNAME 속성을 입력합니다.

자세한 내용은 AWS Elastic Beanstalk 환경으로 트래픽 라우팅 단원을 참조하십시오.

ELB 로드 밸런서

ELB 로드 밸런서의 경우 다음 중 하나를 수행합니다.

- 동일 계정을 사용하여 Route 53 호스팅 영역과 로드 밸런서를 생성한 경우 – 엔드포인트(Endpoint)를 선택하고 목록에서 로드 밸런서를 선택합니다. 로드 밸런서가 많은 경우에는 DNS 이름의 처음 몇 자를 입력하여 목록을 필터링할 수 있습니다.
- 다른 계정을 사용하여 Route 53 호스팅 영역과 로드 밸런서를 생성한 경우 – Elastic Load Balancing 로드 밸런서의 DNS 이름 가져오기 절차에서 얻은 값을 입력합니다.

  하나의 AWS 계정을 사용하여 현재 호스팅 영역을 생성하고 다른 계정을 사용하여 로드 밸런서를 생성한 경우 로드 밸런서는 엔드포인트 목록에 표시되지 않습니다.

  한 계정을 사용하여 현재 호스팅 영역을 생성하고 하나 이상의 다른 계정을 사용하여 모든 로드 밸런서를 생성한 경우 엔드포인트(Endpoints) 목록에는 Elastic Load Balancers 아래 사용 가능한 대상 없음(No Targets Available)이 표시됩니다.

다른 계정의 애플리케이션 및 Classic Load Balancer의 경우 콘솔이 앞에 dualstack.을 추가합니다. 웹 브라우저와 같은 클라이언트가 도메인 이름(example.com) 또는 하위 도메인 이

름(www.example.com)에 대한 IP 주소를 요청할 때 클라이언트는 IPv4 주소(A 레코드), IPv6 주소(AAAA 레코드), 또는 IPv4 및 IPv6 주소(별도 요청의 경우) 둘 다를 요청할 수 있습니다. dualstack.을 지정하면 Route 53에서 클라이언트가 요청한 IP 주소 형식에 따라 로드 밸런서에 적절한 IP 주소로 응답할 수 있습니다.

자세한 내용은 ELB 로드 밸런서로 트래픽 라우팅 단원을 참조하십시오.

AWS Global Accelerator 액셀러레이터

AWS Global Accelerator 액셀러레이터에 액셀러레이터의 DNS 이름을 입력합니다. 현재 AWS 계정을 사용하거나 다른 계정을 사용하여 생성한 액셀러레이터의 DNS 이름을 입력할 수 AWS 있습니다.

Amazon S3 버킷

웹 사이트 엔드포인트로 구성되는 Amazon S3 버킷은 다음 중 하나를 수행합니다.

- 동일 계정을 사용하여 Route 53 호스팅 영역과 Amazon S3 버킷을를 생성한 경우 - 엔드포인트(Endpoint)를 선택하고 목록에서 버킷을 선택합니다. 버킷이 많은 경우 DNS 이름의 처음 몇 자를 입력하여 목록을 필터링할 수 있습니다.

  엔드포인트(Endpoint)의 값은 버킷의 Amazon S3 웹 사이트 엔드포인트로 변경됩니다.
- 다른 계정을 사용하여 Route 53 호스팅 영역과 Amazon S3 버킷을 생성한 경우 – S3 버킷을 생성한 리전의 이름을 입력합니다. Amazon Web Services 일반 참조의 Amazon S3 웹 사이트 엔드포인트 테이블에 있는 웹 사이트 엔드포인트 열에 표시되는 값을 사용합니다.

  현재 AWS 계정 이외의 계정을 사용하여 Amazon S3 버킷을 생성한 경우, 버킷이 엔드포인트 목록에 표시되지 않습니다.

웹 사이트 호스팅용 버킷을 구성해야 합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 웹 사이트 호스팅에 대한 버킷 구성을 참조하십시오.

레코드의 이름은 Amazon S3 버킷의 이름과 일치해야 합니다. 예를 들어, Amazon S3 버킷의 이름이 acme.example.com이면 이 레코드의 이름도 acme.example.com이어야 합니다.

가중 별칭, 지연 시간 별칭, 장애 조치 별칭 또는 지리 위치 별칭 레코드 그룹에서 Amazon S3 버킷으로 쿼리를 라우팅하는 레코드 한 개만 생성할 수 있는데 그 이유는 레코드의 이름이 버킷 이름과 일치해야 하며, 버킷 이름은 전세계적으로 고유해야 하기 때문입니다.

Amazon OpenSearch Service

OpenSearch Service의 경우 다음 중 하나를 수행합니다.

- OpenSearch Service 사용자 지정 도메인: 레코드 이름이 사용자 지정 도메인과 일치해야 합니다. 예를 들어 사용자 지정 도메인의 이름이 test.example.com인 경우이 레코드의 이름도 test.example.com 이어야 합니다.
- 동일한 계정을 사용하여 Route 53 호스팅 영역과 OpenSearch Service 도메인을 생성한 경우를 선택한 AWS 리전다음 도메인 이름을 선택합니다.
- 다른 계정을 사용하여 Route 53 호스팅 영역과 OpenSearch Service 도메인을 생성한 경우 - 사용자 지정 도메인 이름을 입력합니다. 자세한 내용은 사용자 지정 엔드포인트 생성을 참조하세요.

  하나의 AWS 계정을 사용하여 현재 호스팅 영역을 생성하고 다른 계정을 사용하여 OpenSearch Service 도메인을 생성한 경우 도메인이 엔드포인트 목록에 표시되지 않습니다.

  하나의 계정을 사용하여 현재 호스팅 영역을 생성하고 하나 이상의 다른 계정을 사용하여 모든 OpenSearch Service 도메인을 생성하는 경우 엔드포인트 목록에 OpenSearch Service에서 사용할 수 있는 대상 없음이 표시됩니다.

자세한 내용은 트래픽을 Amazon OpenSearch Service 도메인 엔드포인트로 라우팅하도록 Amazon Route 53 구성 단원을 참조하십시오.

Amazon VPC 인터페이스 엔드포인트

Amazon VPC 인터페이스 엔드포인트에 대해 다음 중 하나를 수행하세요.

- 동일 계정을 사용하여 Route 53 호스팅 영역과 인터페이스 엔드포인트를 생성한 경우 – 엔드포인트(Endpoint)를 선택한 다음 목록에서 인터페이스 엔드포인트를 선택합니다. 인터페이스 엔드포인트가 많은 경우 DNS 호스트 이름의 처음 몇 자를 입력하여 목록을 필터링할 수 있습니다.
- 다른 계정을 사용하여 Route 53 호스팅 영역과 인터페이스 엔드포인트를 생성한 경우 – 인터페이스 엔드포인트에 대한 DNS 호스트 이름(예: vpce-123456789abcdef01-example-us-east-1a.elasticloadbalancing.us-east-1.vpce.amazonaws.com)을 입력합니다.

  하나의 AWS 계정을 사용하여 현재 호스팅 영역을 생성하고 다른 계정을 사용하여 인터페이스 엔드포인트를 생성하는 경우 인터페이스 엔드포인트가 VPC 엔드포인트 아래의 엔드포인트 목록에 표시되지 않습니다.

  한 계정을 사용하여 현재 호스팅 영역을 생성하고 하나 이상의 다른 계정을 사용하여 모든 인터페이스 엔드포인트를 생성한 경우 엔드포인트(Endpoints) 목록에는 VPC 엔드포인트(VPC endpoints) 아래에 사용 가능한 대상 없음(No Targets Available)이 표시됩니다.

  자세한 내용은 도메인 이름을 사용하여 Amazon Virtual Private Cloud 인터페이스 엔드포인트로 트래픽 라우팅 단원을 참조하십시오.

이 호스팅 영역의 레코드

이 호스팅 영역 내 레코드의 경우 엔드포인트(Endpoint)를 선택하고 해당하는 레코드를 선택합니다. 레코드가 많은 경우 이름의 처음 몇 자를 입력하여 목록을 필터링할 수 있습니다.

호스팅 영역에 기본 NS 및 SOA 레코드만 있는 경우에는 엔드포인트(Endpoints) 목록에 사용 가능한 대상 없음(No Targets Available)이 표시됩니다.

> **Note**
>
> 호스팅 영역(zone apex라고도 함)과 이름이 같은 별칭 레코드를 생성한다면, 레코드 유형(Record type) 값이 CNAME인 레코드를 선택할 수 없습니다. 이는 별칭 레코드가 트래픽이 라우팅되는 레코드와 동일한 형식이어야 하고, zone apex에 대한 CNAME 레코드 생성은 별칭 레코드에 대해서도 지원되지 않기 때문입니다.

단순 레코드에 특정한 값

단순 레코드를 생성할 때 다음과 같은 값을 지정합니다.

주제

- 라우팅 정책
- 레코드 이름
- 값/트래픽 라우팅 대상
- 레코드 유형
- TTL(초)

라우팅 정책

단순 라우팅(Simple routing)을 선택합니다.

레코드 이름

트래픽을 라우팅할 도메인 또는 하위 도메인의 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

> **Note**
>
> 호스팅 영역과 이름이 동일한 레코드를 생성할 경우 이름 필드에 값(예: @ 기호)을 입력하지 마십시오.

레코드 이름에 대한 자세한 내용은 레코드 이름 섹션을 참조하십시오.

값/트래픽 라우팅 대상

IP 주소 또는 레코드 유형에 따라 다른 값(IP address or another value depending on the record type)을 선택합니다. 레코드 유형(Record type) 값에 해당하는 값을 입력합니다. CNAME을 제외한 모든 유형은 둘 이상의 값을 입력할 수 있습니다. 각 값을 별도의 라인에 입력합니다.

트래픽을 라우팅하거나 다음 값을 지정할 수 있습니다.

- A – IPv4 주소
- AAAA - IPv6 주소
- CAA - 인증 기관 인증

- CNAME – 정식 이름
- MX - 메일 교환
- NAPTR - 이름 권한 포인터
- NS - 이름 서버

  이름 서버의 도메인 이름(예: ns1.example.com)

  > **Note**
  >
  > 단순 라우팅 정책만 사용하여 NS 레코드를 지정할 수 있습니다.

- PTR - 포인터
- SPF - 발신자 정책 프레임워크
- SRV - 서비스 로케이터
- TXT - 텍스트

위의 값에 대한 자세한 내용은 값/트래픽 라우팅 대상에 일반적인 값을 참조하세요.

레코드 유형

DNS 레코드 유형입니다. 자세한 내용은 지원되는 DNS 레코드 유형 단원을 참조하십시오.

Route 53이 DNS 쿼리에 응답하는 방식에 따라 레코드 유형(Record type)에 대한 값을 선택합니다.

TTL(초)

DNS recursive resolver가 이 레코드에 관한 정보를 캐싱할 시간(초)입니다. 더 긴 값(예: 172800초 또는 2일)을 지정한 경우, 이 레코드의 최신 정보를 얻으려면 DNS recursive resolver의 Route 53에 대한 호출 수를 줄여야 합니다. 이렇게 하면 지연 시간을 줄이고 Route 53 서비스 비용을 줄이는 효과가 있습니다. 자세한 내용은 Amazon Route 53가 도메인의 트래픽을 라우팅하는 방법 단원을 참조하십시오.

그러나 TTL에 더 긴 값을 지정하면 recursive resolver가 Route 53에 최신 정보를 요청하기 전에 기간이 더 긴 캐시 값을 사용하므로 레코드(예: 새 IP 주소) 변경이 적용되는 데 걸리는 시간이 길어집니다. 이미 사용 중인 도메인이나 하위 도메인의 설정을 변경하는 경우 처음에는 더 짧은 값(예: 300초)을 지정하고 새 설정이 올바른지 확인한 후 값을 늘리는 것이 좋습니다.

단순 별칭 레코드에 특정한 값

별칭 레코드를 생성할 때 다음과 같은 값을 지정합니다. 자세한 내용은 별칭 또는 비 별칭 레코드 선택 단원을 참조하십시오.

> **Note**
>
> 에서 Route 53를 사용하는 경우 AWS GovCloud (US) Region이 기능에 몇 가지 제한이 있습니다. 자세한 내용은 AWS GovCloud (US) 사용 설명서의 Amazon Route 53 페이지를 참조하세요.

주제

- 라우팅 정책
- 레코드 이름
- 값/트래픽 라우팅 대상
- 레코드 유형
- 대상 상태 평가

라우팅 정책

단순 라우팅(Simple routing)을 선택합니다.

레코드 이름

트래픽을 라우팅할 도메인 또는 하위 도메인의 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

> **Note**
>
> 호스팅 영역과 이름이 동일한 레코드를 생성할 경우 이름 필드에 값(예: @ 기호)을 입력하지 마십시오.

레코드 이름에 대한 자세한 내용은 레코드 이름 섹션을 참조하십시오.

값/트래픽 라우팅 대상

목록에서 선택하거나 필드에 입력하는 값은 트래픽을 라우팅하는 AWS 리소스에 따라 달라집니다.

대상으로 지정할 수 있는 AWS 리소스에 대한 자세한 내용은 값/라우팅 트래픽에 대한 별칭 레코드의 공통 값을 참조하세요.

트래픽을 특정 AWS 리소스로 라우팅하도록 Route 53를 구성하는 방법에 대한 자세한 내용은 섹션을 참조하세요AWS 리소스로 인터넷 트래픽 라우팅.

레코드 유형

DNS 레코드 유형입니다. 자세한 내용은 지원되는 DNS 레코드 유형 단원을 참조하십시오.

트래픽을 라우팅할 AWS 리소스를 기반으로 해당 값을 선택합니다.

API Gateway 사용자 지정 리전 API 또는 엣지 최적화 API

A - IPv4 주소(A - IPv4 address)를 선택합니다.

Amazon VPC 인터페이스 엔드포인트

A - IPv4 주소(A - IPv4 address)를 선택합니다.

CloudFront 배포

A - IPv4 주소(A - IPv4 address)를 선택합니다.

배포에 대해 IPv6가 활성화되어 있다면 두 개의 레코드를 생성합니다. 하나는 유형(Type) 값이 A - IPv4 주소(A - IPv4 address)이고 하나는 값이 AAAA - IPv6 주소(AAAA - IPv6 address)입니다.

App Runner 서비스

A - IPv4 주소(A - IPv4 address)를 선택합니다.

리전별 하위 도메인이 있는 Elastic Beanstalk 환경

A - IPv4 주소(A - IPv4 address)를 선택합니다.

ELB 로드 밸런서

A - IPv4 address(A - IPv4 주소) 또는 AAAA - IPv6 address(AAAA - IPv6 주소) 선택

Amazon S3 버킷

A - IPv4 주소(A - IPv4 address)를 선택합니다.

OpenSearch Service

A - IPv4 address(A - IPv4 주소) 또는 AAAA - IPv6 address(AAAA - IPv6 주소) 선택

호스팅 영역의 또 다른 레코드

별칭을 생성 중인 레코드 유형을 선택합니다. NS 및 SOA를 제외한 모든 유형이 지원됩니다.

> **Note**
>
> 호스팅 영역(zone apex라고도 함)과 이름이 같은 별칭 레코드를 생성한다면, 유형 값이 CNAME인 레코드로 트래픽을 라우팅할 수 없습니다. 이는 별칭 레코드가 트래픽이 라우팅되는 레코드와 동일한 형식이어야 하고, zone apex에 대한 CNAME 레코드 생성은 별칭 레코드에 대해서도 지원되지 않기 때문입니다.

대상 상태 평가

라우팅 정책(Routing policy) 값이 단순(Simple)인 경우 아니요(No) 또는 기본값인 예(Yes) 중 하나를 선택할 수 있습니다. 대상 상태 평가(Evaluate target health)는 단순(Simple) 라우팅에 영향을 미치지 않기 때문입니다. 지정된 이름과 유형이 있는 레코드가 하나만 있는 경우 Route 53은 리소스가 정상인지 여부에 관계없이 해당 레코드의 값을 사용하여 DNS 쿼리에 응답합니다.

장애 조치 레코드에 특정한 값

장애 조치 레코드를 생성할 때 다음과 같은 값을 지정합니다.

> **Note**
>
> 프라이빗 호스팅 영역에서 장애 조치 레코드를 생성하는 방법에 대한 자세한 내용은 프라이빗 호스팅 영역에서 장애 조치 구성 단원을 참조하십시오.

주제

- 라우팅 정책
- 레코드 이름
- 레코드 유형
- TTL(초)
- 값/트래픽 라우팅 대상
- 장애 조치 레코드 유형
- 상태 확인
- 레코드 ID

라우팅 정책

장애 조치(Failover)를 선택합니다.

레코드 이름

트래픽을 라우팅할 도메인 또는 하위 도메인의 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

> **Note**
>
> 호스팅 영역과 이름이 동일한 레코드를 생성할 경우 레코드 이름(Record name) 필드에 값(예: @ 기호)을 입력하지 마세요.

장애 조치 레코드 그룹의 레코드 모두에 대해 동일한 이름을 입력합니다.

레코드 이름에 대한 자세한 내용은 레코드 이름 섹션을 참조하십시오.

레코드 유형

DNS 레코드 유형입니다. 자세한 내용은 지원되는 DNS 레코드 유형 단원을 참조하십시오.

기본 및 보조 장애 조치 레코드 모두에 대해 동일 값을 선택합니다.

TTL(초)

DNS recursive resolver가 이 레코드에 관한 정보를 캐싱할 시간(초)입니다. 더 긴 값(예: 172800초 또는 2일)을 지정한 경우, 이 레코드의 최신 정보를 얻으려면 DNS recursive resolver의 Route 53에 대한 호출 수를 줄여야 합니다. 이렇게 하면 지연 시간을 줄이고 Route 53 서비스 비용을 줄이는 효과가 있습니다. 자세한 내용은 Amazon Route 53가 도메인의 트래픽을 라우팅하는 방법 단원을 참조하십시오.

그러나 TTL에 더 긴 값을 지정하면 recursive resolver가 Route 53에 최신 정보를 요청하기 전에 기간이 더 긴 캐시 값을 사용하므로 레코드(예: 새 IP 주소) 변경이 적용되는 데 걸리는 시간이 길어집니다. 이미 사용 중인 도메인이나 하위 도메인의 설정을 변경하는 경우 처음에는 더 짧은 값(예: 300초)을 지정하고 새 설정이 올바른지 확인한 후 값을 늘리는 것이 좋습니다.

이 레코드를 상태 점검과 연관시킬 경우에는 클라이언트가 상태 변경에 빠르게 응답하도록 TTL을 60초 이하로 지정하는 것이 좋습니다.

값/트래픽 라우팅 대상

IP 주소 또는 레코드 유형에 따라 다른 값(IP address or another value depending on the record type)을 선택합니다. 레코드 유형(Record type) 값에 해당하는 값을 입력합니다. CNAME을 제외한 모든 유형은 둘 이상의 값을 입력할 수 있습니다. 각 값을 별도의 라인에 입력합니다.

트래픽을 라우팅하거나 다음 값을 지정할 수 있습니다.

- A – IPv4 주소
- AAAA - IPv6 주소
- CAA - 인증 기관 인증
- CNAME – 정식 이름
- MX - 메일 교환
- NAPTR - 이름 권한 포인터
- PTR - 포인터
- SPF - 발신자 정책 프레임워크
- SRV - 서비스 로케이터

- TXT - 텍스트

위의 값에 대한 자세한 내용은 값/트래픽 라우팅 대상에 일반적인 값을 참조하세요.

장애 조치 레코드 유형

이 레코드에 해당하는 값을 선택합니다. 장애 조치가 제대로 작동하려면 기본 및 보조 장애 조치 레코드를 각각 1개씩 생성해야 합니다.

레코드 이름(Record name) 및 레코드 유형(Record type) 값이 장애 조치 레코드와 같은 비-장애 조치 레코드를 생성할 수 있습니다.

상태 확인

Route 53가 지정된 엔드포인트 상태를 점검하고 엔드포인트가 정상할 때만 이 레코드를 사용하여 DNS 쿼리에 응답하길 원할 경우 상태 확인을 선택합니다.

Route 53는 레코드에 지정된 엔드포인트, 예를 들어 값(Value) 필드에서 IP 주소로 지정된 엔드포인트의 상태는 점검하지 않습니다. 레코드의 상태 확인을 선택하면 Route 53가 상태 확인에서 지정한 엔드포인트의 상태를 점검합니다. Route 53가 엔드포인트가 정상인지 여부를 결정하는 방법은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 섹션을 참조하세요.

상태 확인과 레코드를 연관시키는 것은 Route 53가 둘 이상의 레코드 사이에서 DNS 쿼리에 응답할 레코드를 선택할 때 그리고 Route 53가 상태 확인 상태를 선택의 기준으로 삼을 때만 유용합니다. 다음 구성에서만 상태 확인을 사용합니다.

- 이름, 유형 및 라우팅 정책(예: 장애 조치 또는 가중치 레코드)이 동일한 레코드 그룹의 모든 레코드 상태를 확인하고 모든 레코드에 대한 상태 확인 ID를 지정하는 경우. 레코드의 상태 확인에서 양호하지 않은 엔드포인트가 지정될 경우 Route 53는 해당 레코드 값을 사용하는 쿼리에 대한 응답을 중단합니다.
- 별칭 레코드 또는 장애 조치 별칭, 지리적 위치 별칭, 대기 시간 별칭, IP 기반 별칭 또는 가중치 기반 별칭 그룹에 속한 레코드에 대해 대상 상태 평가(Evaluate Target Health)에서 예(Yes)를 선택하는 경우. 별칭 레코드가 동일한 호스팅 영역의 별칭이 아닌 레코드를 참조하는 경우 참조된 레코드의 상태 확인도 지정해야 합니다. 상태 확인과 별칭 레코드를 연관시키고 대상 상태 평가에서 예를 선택하는 경우 둘 다 true로 평가되어야 합니다. 자세한 내용은 상태 확인을 별칭 레코드와 연결하면 어떻게 됩니까? 단원을 참조하십시오.

상태 확인에서 도메인 이름만으로 엔드포인트를 지정할 경우에는 각 엔드포인트마다 별도의 상태 확인을 생성하는 것이 좋습니다. 예를 들어, www.example.com의 콘텐츠를 제공하는 각 HTTP 서버마다

상태 확인을 생성합니다. 도메인 이름의 값은 레코드의 이름(example.com)이 아니라 서버의 도메인 이름(예: us-east-2-www.example.com)을 지정합니다.

> **Important**
>
> 이 구성에서 도메인 이름의 값이 레코드의 이름과 일치하는 상태 확인을 생성한 후 상태 확인을 이러한 레코드와 연결하는 경우 상태 확인 결과를 예측할 수 없습니다.

레코드 ID

기본 및 보조 레코드를 고유하게 식별하는 값을 선택합니다.

장애 조치 별칭 레코드에 특정한 값

장애 조치 별칭 레코드를 생성할 때 다음과 같은 값을 지정합니다.

자세한 내용은 다음 주제를 참조하세요.

- 프라이빗 호스팅 영역에서 장애 조치 레코드를 생성하는 방법에 대한 자세한 내용은 프라이빗 호스팅 영역에서 장애 조치 구성 단원을 참조하십시오.
- 별칭 레코드에 대한 자세한 내용은 별칭 또는 비 별칭 레코드 선택 단원을 참조하십시오.

주제

- 라우팅 정책
- 레코드 이름
- 레코드 유형
- 값/트래픽 라우팅 대상
- 장애 조치 레코드 유형
- 상태 확인
- 대상 상태 평가
- 레코드 ID

라우팅 정책

장애 조치(Failover)를 선택합니다.

레코드 이름

트래픽을 라우팅할 도메인 또는 하위 도메인의 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

> **Note**
>
> 호스팅 영역과 이름이 동일한 레코드를 생성할 경우 레코드 이름(Record name) 필드에 값(예: @ 기호)을 입력하지 마세요.

장애 조치 레코드 그룹의 레코드 모두에 대해 동일한 이름을 입력합니다.

레코드 이름에 대한 자세한 내용은 레코드 이름 섹션을 참조하십시오.

레코드 유형

DNS 레코드 유형입니다. 자세한 내용은 지원되는 DNS 레코드 유형 단원을 참조하십시오.

트래픽을 라우팅할 AWS 리소스를 기반으로 해당 값을 선택합니다. 기본 및 보조 장애 조치 레코드 모두에 대해 동일 값을 선택합니다.

API Gateway 사용자 지정 리전 API 또는 엣지 최적화 API

A - IPv4 주소(A - IPv4 address)를 선택합니다.

Amazon VPC 인터페이스 엔드포인트

A - IPv4 주소(A - IPv4 address)를 선택합니다.

CloudFront 배포

A - IPv4 주소(A - IPv4 address)를 선택합니다.

배포에 대해 IPv6가 활성화되어 있다면 두 개의 레코드를 생성합니다. 하나는 유형(Type) 값이 A - IPv4 주소(A - IPv4 address)이고 하나는 값이 AAAA - IPv6 주소(AAAA - IPv6 address)입니다.

App Runner 서비스

A - IPv4 주소(A - IPv4 address)를 선택합니다.

리전별 하위 도메인이 있는 Elastic Beanstalk 환경

A - IPv4 주소(A - IPv4 address)를 선택합니다.

ELB 로드 밸런서

A - IPv4 address(A - IPv4 주소) 또는 AAAA - IPv6 address(AAAA - IPv6 주소) 선택

Amazon S3 버킷

A - IPv4 주소(A - IPv4 address)를 선택합니다.

OpenSearch Service

A - IPv4 address(A - IPv4 주소) 또는 AAAA - IPv6 address(AAAA - IPv6 주소) 선택

호스팅 영역의 또 다른 레코드

별칭을 생성 중인 레코드 유형을 선택합니다. NS 및 SOA를 제외한 모든 유형이 지원됩니다.

> **Note**
>
> 호스팅 영역(zone apex라고도 함)과 이름이 같은 별칭 레코드를 생성한다면, 유형 값이 CNAME인 레코드로 트래픽을 라우팅할 수 없습니다. 이는 별칭 레코드가 트래픽이 라우팅되는 레코드와 동일한 형식이어야 하고, zone apex에 대한 CNAME 레코드 생성은 별칭 레코드에 대해서도 지원되지 않기 때문입니다.

값/트래픽 라우팅 대상

목록에서 선택하거나 필드에 입력하는 값은 트래픽을 라우팅하는 AWS 리소스에 따라 달라집니다.

대상으로 지정할 수 있는 AWS 리소스에 대한 자세한 내용은 값/라우팅 트래픽에 대한 별칭 레코드의 공통 값을 참조하세요.

트래픽을 특정 AWS 리소스로 라우팅하도록 Route 53를 구성하는 방법에 대한 자세한 내용은 섹션을 참조하세요AWS 리소스로 인터넷 트래픽 라우팅.

> **Note**
>
> 주 장애 조치 및 보조 장애 조치 레코드를 만들 때 이름(Name) 및 레코드 유형(Record type)에 대해 동일한 값을 갖는 하나의 장애 조치(failover) 와 하나의 장애 조치 별칭(alias)을 선택적으로 만들 수 있습니다. 장애 조치와 장애 조치 별칭 레코드를 혼합할 경우 둘 중 하나는 기본 레코드가 될 수 있습니다.

장애 조치 레코드 유형

이 레코드에 해당하는 값을 선택합니다. 장애 조치가 제대로 작동하려면 기본 및 보조 장애 조치 레코드를 각각 1개씩 생성해야 합니다.

레코드 이름(Record name) 및 레코드 유형(Record type) 값이 장애 조치 레코드와 같은 비-장애 조치 레코드를 생성할 수 있습니다.

상태 확인

Route 53가 지정된 엔드포인트 상태를 점검하고 엔드포인트가 정상할 때만 이 레코드를 사용하여 DNS 쿼리에 응답하길 원할 경우 상태 확인을 선택합니다.

Route 53는 레코드에 지정된 엔드포인트, 예를 들어 값(Value) 필드에서 IP 주소로 지정된 엔드포인트의 상태는 점검하지 않습니다. 레코드의 상태 확인을 선택하면 Route 53가 상태 확인에서 지정한 엔

드포인트의 상태를 점검합니다. Route 53가 엔드포인트가 정상인지 여부를 결정하는 방법은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 섹션을 참조하세요.

상태 확인과 레코드를 연관시키는 것은 Route 53가 둘 이상의 레코드 사이에서 DNS 쿼리에 응답할 레코드를 선택할 때 그리고 Route 53가 상태 확인 상태를 선택의 기준으로 삼을 때만 유용합니다. 다음 구성에서만 상태 확인을 사용합니다.

- 이름, 유형 및 라우팅 정책(예: 장애 조치 또는 가중치 레코드)이 동일한 레코드 그룹의 모든 레코드 상태를 확인하고 모든 레코드에 대한 상태 확인 ID를 지정하는 경우. 레코드의 상태 확인에서 양호하지 않은 엔드포인트가 지정될 경우 Route 53는 해당 레코드 값을 사용하는 쿼리에 대한 응답을 중단합니다.
- 별칭 레코드 또는 장애 조치 별칭, 지리적 위치 별칭, 대기 시간 별칭, IP 기반 별칭 또는 가중치 기반 별칭 그룹에 속한 레코드에 대해 대상 상태 평가(Evaluate Target Health)에서 예(Yes)를 선택하는 경우. 별칭 레코드가 동일한 호스팅 영역의 별칭이 아닌 레코드를 참조하는 경우 참조된 레코드의 상태 확인도 지정해야 합니다. 상태 확인과 별칭 레코드를 연관시키고 대상 상태 평가에서 예를 선택하는 경우 둘 다 true로 평가되어야 합니다. 자세한 내용은 상태 확인을 별칭 레코드와 연결하면 어떻게 됩니까? 단원을 참조하십시오.

상태 확인에서 도메인 이름만으로 엔드포인트를 지정할 경우에는 각 엔드포인트마다 별도의 상태 확인을 생성하는 것이 좋습니다. 예를 들어, www.example.com의 콘텐츠를 제공하는 각 HTTP 서버마다 상태 확인을 생성합니다. 도메인 이름의 값은 레코드의 이름(example.com)이 아니라 서버의 도메인 이름(예: us-east-2-www.example.com)을 지정합니다.

> **Important**
>
> 이 구성에서 도메인 이름의 값이 레코드의 이름과 일치하는 상태 확인을 생성한 후 상태 확인을 이러한 레코드와 연결하는 경우 상태 확인 결과를 예측할 수 없습니다.

대상 상태 평가

엔드포인트에서 지정된 리소스의 상태를 확인하여 Route 53가 레코드를 사용해 DNS 쿼리에 응답할지 여부를 결정하게 하려는 경우 예(Yes)를 선택합니다.

다음 사항에 유의하세요.

API Gateway 사용자 지정 리전 API와 엣지 최적화 API

엔드포인트가 API Gateway 사용자 지정 리전 API 또는 엣지 최적화 API인 경우 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정하기 위한 특별한 요구 사항은 없습니다.

CloudFront 배포

엔드포인트가 CloudFront 배포인 경우 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정할 수 없습니다.

리전별 하위 도메인이 있는 Elastic Beanstalk 환경

엔드포인트(Endpoint)에 Elastic Beanstalk 환경을 지정하고 환경에 ELB 로드 밸런서가 포함된 경우, Elastic Load Balancing은 로드 밸런서에 등록된 정상 Amazon EC2 인스턴스로만 쿼리를 라우팅합니다. (하나의 환경에 한 개 이상의 Amazon EC2 인스턴스가 포함된 경우 ELB 로드 밸런서가 자동으로 포함됩니다.) 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정했는데 정상인 Amazon EC2 인스턴스가 없거나 로드 밸런서 자체가 비정상인 경우 Route 53는 양호한 다른 리소스로 쿼리를 라우팅합니다.

환경에 하나의 Amazon EC2 인스턴스가 포함된 경우에는 특별한 요구 사항이 없습니다.

ELB 로드 밸런서

상태 확인 동작은 로드 밸런서의 유형에 따라 달랍니다.

- Classic Load Balancer: 엔드포인트(Endpoint)에 ELB Classic Load Balancer를 지정한 경우, Elastic Load Balancing은 로드 밸런서에 등록된 정상 Amazon EC2 인스턴스로만 쿼리를 라우팅합니다. 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정하고 EC2 인스턴스가 정상 상태가 아니거나 로드 밸런서 자체가 비정상인 경우 Route 53는 쿼리를 다른 리소스로 라우팅합니다.
- Application Load Balancer 및 Network Load Balancer - ELB Application Load Balancer 또는 Network Load Balancer를 지정하고 대상 상태 평가(Evaluate Target Health)를 예(Yes)로 설정한 경우 은 로드 밸런서와 연결된 대상 그룹의 상태에 따라 쿼리를 로드 밸런서로 라우팅합니다.
  - Application Load Balancer 또는 Network Load Balancer가 정상 상태로 간주되려면 대상을 포함하는 대상 그룹에 정상 상태 대상이 하나 이상 포함되어야 합니다. 대상 그룹에 정상이 아닌 대상만 포함되는 경우 로드 밸런서는 정상이 아닌 상태로 간주되고 Route 53는 쿼리를 다른 리소스로 라우팅합니다.
  - 등록된 대상이 없는 대상 그룹은 정상이 아닌 상태로 간주됩니다.

> **Note**
>
> 로드 밸런서를 생성할 때 Elastic Load Balancing 상태 확인에 대한 설정을 구성하게 되는데, 이러한 확인은 Route 53 상태 확인은 아니지만 비슷한 기능을 수행합니다. ELB 로드 밸런서에 등록하는 EC2 인스턴스에 대해 Route 53 상태 확인을 생성하지 마십시오.

S3 버킷

엔드포인트가 S3 버킷인 경우 대상 상태 평가(Evaluate Target Health)를 예(Yes)로 설정하는 데 필요한 특정 요건은 없습니다.

Amazon VPC 인터페이스 엔드포인트

엔드포인트가 Amazon VPC 인터페이스 엔드포인트인 경우 대상 상태 평가(Evaluate Target Health)를 예(Yes)로 설정하는 데 필요한 특별한 요구 사항이 없습니다.

동일 호스팅 영역 내 다른 레코드

엔드포인트에서 지정하는 AWS 리소스가 레코드 또는 레코드 그룹(예: 가중치 기반 레코드 그룹)이지만 다른 별칭 레코드가 아닌 경우 상태 확인을 엔드포인트의 모든 레코드와 연결하는 것이 좋습니다. 자세한 내용은 상태 확인을 생략하면 어떻게 됩니까? 단원을 참조하십시오.

레코드 ID

기본 및 보조 레코드를 고유하게 식별하는 값을 선택합니다.

지리 위치 레코드에 특정한 값

지리 위치 레코드를 생성할 때 다음과 같은 값을 지정합니다.

주제

- 라우팅 정책
- 레코드 이름
- 레코드 유형
- TTL(초)
- 값/트래픽 라우팅 대상
- 위치
- 미국 주
- 상태 확인
- 레코드 ID

라우팅 정책

지리적 위치(Geolocation)를 선택합니다.

레코드 이름

트래픽을 라우팅할 도메인 또는 하위 도메인의 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

> **Note**
>
> 호스팅 영역과 이름이 동일한 레코드를 생성할 경우 이름 필드에 값(예: @ 기호)을 입력하지 마십시오.

지리 위치 레코드 그룹의 모든 레코드에 대해 동일한 이름을 입력합니다.

레코드 이름에 대한 자세한 내용은 레코드 이름 섹션을 참조하십시오.

레코드 유형

DNS 레코드 유형입니다. 자세한 내용은 지원되는 DNS 레코드 유형 단원을 참조하십시오.

지리 위치 레코드 그룹의 모든 레코드에 대해 동일 값을 선택합니다.

TTL(초)

DNS recursive resolver가 이 레코드에 관한 정보를 캐싱할 시간(초)입니다. 더 긴 값(예: 172800초 또는 2일)을 지정한 경우, 이 레코드의 최신 정보를 얻으려면 DNS recursive resolver의 Route 53에 대한 호출 수를 줄여야 합니다. 이렇게 하면 지연 시간을 줄이고 Route 53 서비스 비용을 줄이는 효과가 있습니다. 자세한 내용은 Amazon Route 53가 도메인의 트래픽을 라우팅하는 방법 단원을 참조하십시오.

그러나 TTL에 더 긴 값을 지정하면 recursive resolver가 Route 53에 최신 정보를 요청하기 전에 기간이 더 긴 캐시 값을 사용하므로 레코드(예: 새 IP 주소) 변경이 적용되는 데 걸리는 시간이 길어집니다. 이미 사용 중인 도메인이나 하위 도메인의 설정을 변경하는 경우 처음에는 더 짧은 값(예: 300초)을 지정하고 새 설정이 올바른지 확인한 후 값을 늘리는 것이 좋습니다.

이 레코드를 상태 점검과 연관시킬 경우에는 클라이언트가 상태 변경에 빠르게 응답하도록 TTL을 60초 이하로 지정하는 것이 좋습니다.

값/트래픽 라우팅 대상

IP 주소 또는 레코드 유형에 따라 다른 값(IP address or another value depending on the record type)을 선택합니다. 레코드 유형(Record type) 값에 해당하는 값을 입력합니다. CNAME을 제외한 모든 유형은 둘 이상의 값을 입력할 수 있습니다. 각 값을 별도의 라인에 입력합니다.

트래픽을 라우팅하거나 다음 값을 지정할 수 있습니다.

- A – IPv4 주소
- AAAA - IPv6 주소
- CAA - 인증 기관 인증
- CNAME – 정식 이름
- MX - 메일 교환
- NAPTR - 이름 권한 포인터
- PTR - 포인터
- SPF - 발신자 정책 프레임워크
- SRV - 서비스 로케이터
- TXT - 텍스트

위의 값에 대한 자세한 내용은 값/트래픽 라우팅 대상에 일반적인 값을 참조하세요.

위치

쿼리를 보낸 위치를 기반으로 하는 DNS 쿼리에 응답하도록 Route 53을 구성할 때는 Route 53이 이 레코드 설정으로 응답하길 원하는 대륙 또는 국가를 선택합니다. Route 53이 미국의 개별 주에 대한 DNS 쿼리에 응답하길 원할 경우 먼저 위치(Location)목록에서 미국(United States)을 선택한 다음 하위 위치(Sublocation) 그룹에서 주를 선택합니다.

프라이빗 호스팅 영역의 경우 리소스가 AWS 리전 있는에 가장 가까운 대륙, 국가 또는 하위 부문을 선택합니다. 예를 들어 리소스가 us-east-1에 있으면 북미, 미국 또는 버지니아를 지정할 수 있습니다.

> **Important**
>
> 위치(Location)에 대한 기본(Default) 값을 갖는 하나의 지리적 위치 레코드를 생성하는 것이 좋습니다. 그러면 레코드를 생성하지 않은 지리적 위치와 Route 53이 위치를 식별하지 못하는 IP 주소도 포함됩니다.

레코드 이름(Record name) 및 레코드 유형(Record type) 값이 지리적 위치 레코드와 같은 값을 갖는 비-지리적 위치 레코드를 생성할 수 없습니다.

자세한 내용은 지리적 라우팅 단원을 참조하십시오.

다음은 Amazon Route 53이 각 대륙과 연결되는 국가입니다. 국가 코드는 ISO 3166부터 시작합니다. 자세한 내용은 Wikipedia 도움말 ISO 3166-1 alpha-2를 참조하십시오.

아프리카(AF)

AO, BF, BI, BJ, BW, CD, CF, CG, CI, CM, CV, DJ, DZ, EG, ER, ET, GA, GH, GM, GN, GQ, GW, KE, KM, LR, LS, LY, MA, MG, ML, MR, MU, MW, MZ, NA, NE, NG, RE, RW, SC, SD, SH, SL, SN, SO, SS, ST, SZ, TD, TG, TN, TZ, UG, YT, ZA, ZM, ZW

남극 대륙(AN)

AQ, GS, TF

아시아(AS)

AE, AF, AM, AZ, BD, BH, BN, BT, CC, CN, GE, HK, ID, IL, IN, IO, IQ, IR, JO, JP, KG, KH, KP, KR, KW, KZ, LA, LB, LK, MM, MN, MO, MV, MY, NP, OM, PH, PK, PS, QA, SA, SG, SY, TH, TJ, TM, TW, UZ, VN, YE

유럽(EU)

AD, AL, AT, AX, BA, BE, BG, BY, CH, CY, CZ, DE, DK, EE, ES, FI, FO, FR, GB, GG, GI, GR, HR, HU, IE, IM, IS, IT, JE, LI, LT, LU, LV, MC, MD, ME, MK, MT, NL, NO, PL, PT, RO, RS, RU, SE, SI, SJ, SK, SM, TR, UA, VA, XK

북아메리카(NA)

AG, AI, AW, BB, BL, BM, BQ, BS, BZ, CA, CR, CU, CW, DM, DO, GD, GL, GP, GT, HN, HT, JM, KN, KY, LC, MF, MQ, MS, MX, NI, PA, PM, PR, SV, SX, TC, TT, US, VC, VG, VI

오세아니아(OC)

AS, AU, CK, FJ, FM, GU, KI, MH, MP, NC, NF, NR, NU, NZ, PF, PG, PN, PW, SB, TK, TL, TO, TV, UM, VU, WF, WS

남아메리카(SA)

AR, BO, BR, CL, CO, EC, FK, GF, GY, PE, PY, SR, UY, VE

> **Note**
>
> Route 53은 다음 국가, 즉 부베 섬(BV), 크리스마스 섬(CX), 서부 사하라(EH), 허드 섬 및 맥도널드 제도(HM)의 지리 위치 레코드 생성을 지원하지 않습니다. 이들 국가의 IP 주소에 관한 데이터가 없습니다.

미국 주

Route 53이 쿼리가 발생한 미국 주를 토대로 DNS 쿼리에 응답하도록 구성할 때는 미국 주(U.S. states) 목록에서 주를 선택합니다. 미국 영토(예: 푸에르토리코)는 위치 목록에 국가로 표시됩니다.

> **Important**
>
> 일부 IP 주소는 개별 주가 아니라 미국과 관련이 있습니다. 미국 내 모든 주의 레코드를 생성할 경우에는 이러한 무관한 IP 주소의 쿼리를 라우팅할 미국 레코드도 생성하는 것이 좋습니다. 미국의 레코드를 생성하지 않으면 Route 53이 비연관 미국 IP 주소의 DNS 쿼리에 기본 지리 위치 레코드(생성한 경우)의 설정 또는 "응답 없음"으로 응답합니다.

상태 확인

Route 53가 지정된 엔드포인트 상태를 점검하고 엔드포인트가 정상할 때만 이 레코드를 사용하여 DNS 쿼리에 응답하길 원할 경우 상태 확인을 선택합니다.

Route 53는 레코드에 지정된 엔드포인트, 예를 들어 값(Value) 필드에서 IP 주소로 지정된 엔드포인트의 상태는 점검하지 않습니다. 레코드의 상태 확인을 선택하면 Route 53가 상태 확인에서 지정한 엔드포인트의 상태를 점검합니다. Route 53가 엔드포인트가 정상인지 여부를 결정하는 방법은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 섹션을 참조하세요.

상태 확인과 레코드를 연관시키는 것은 Route 53가 둘 이상의 레코드 사이에서 DNS 쿼리에 응답할 레코드를 선택할 때 그리고 Route 53가 상태 확인 상태를 선택의 기준으로 삼을 때만 유용합니다. 다음 구성에서만 상태 확인을 사용합니다.

- 이름, 유형 및 라우팅 정책(예: 장애 조치 또는 가중치 레코드)이 동일한 레코드 그룹의 모든 레코드 상태를 확인하고 모든 레코드에 대한 상태 확인 ID를 지정하는 경우. 레코드의 상태 확인에서 양호하지 않은 엔드포인트가 지정될 경우 Route 53는 해당 레코드 값을 사용하는 쿼리에 대한 응답을 중단합니다.
- 별칭 레코드 또는 장애 조치 별칭, 지리적 위치 별칭, 대기 시간 별칭, IP 기반 별칭 또는 가중치 기반 별칭 그룹에 속한 레코드에 대해 대상 상태 평가(Evaluate Target Health)에서 예(Yes)를 선택하는 경우. 별칭 레코드가 동일한 호스팅 영역의 별칭이 아닌 레코드를 참조하는 경우 참조된 레코드의 상태 확인도 지정해야 합니다. 상태 확인과 별칭 레코드를 연관시키고 대상 상태 평가에서 예를 선택하는 경우 둘 다 true로 평가되어야 합니다. 자세한 내용은 상태 확인을 별칭 레코드와 연결하면 어떻게 됩니까? 단원을 참조하십시오.

상태 확인에서 도메인 이름만으로 엔드포인트를 지정할 경우에는 각 엔드포인트마다 별도의 상태 확인을 생성하는 것이 좋습니다. 예를 들어, www.example.com의 콘텐츠를 제공하는 각 HTTP 서버마다 상태 확인을 생성합니다. 도메인 이름의 값은 레코드의 이름(example.com)이 아니라 서버의 도메인 이름(예: us-east-2-www.example.com)을 지정합니다.

> **Important**
>
> 이 구성에서 도메인 이름의 값이 레코드의 이름과 일치하는 상태 확인을 생성한 후 상태 확인을 이러한 레코드와 연결하는 경우 상태 확인 결과를 예측할 수 없습니다.

지리 위치 레코드에서 엔드포인트가 양호하지 않을 경우 Route 53은 규모가 더 큰 관련 지리적 리전의 레코드를 조회합니다. 예를 들어, 미국 내 주, 미국, 북미 및 전체 위치에 대한 레코드가 있다고 가정합

니다(위치가 기본값임). 주 레코드의 엔드포인트가 양호하지 않을 경우 Route 53은 미국, 북미 및 전체 위치 순으로 엔드포인트가 양호한 레코드를 찾을 때까지 레코드를 확인합니다. 모든 지리적 위치에 대한 레코드를 포함하여 모든 적용 가능한 레코드가 비정상적인 경우 Route 53은 가장 작은 지리적 리전에 대한 레코드 값을 사용하여 DNS 쿼리에 응답합니다.

레코드 ID

지리 위치 레코드 그룹에 있는 이 레코드를 고유하게 식별하는 값을 선택합니다.

지리 위치 별칭 레코드에 특정한 값

지리 위치 별칭 레코드를 생성할 때 다음과 같은 값을 지정합니다.

자세한 내용은 별칭 또는 비 별칭 레코드 선택 단원을 참조하십시오.

주제

- 라우팅 정책
- 레코드 이름
- 레코드 유형
- 값/트래픽 라우팅 대상
- 위치
- 미국 주
- 상태 확인
- 대상 상태 평가
- 레코드 ID

라우팅 정책

지리적 위치(Geolocation)를 선택합니다.

레코드 이름

트래픽을 라우팅할 도메인 또는 하위 도메인의 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

> **Note**
>
> 호스팅 영역과 이름이 동일한 레코드를 생성할 경우 레코드 이름(Record name) 필드에 값(예: @ 기호)을 입력하지 마세요.

지리 위치 레코드 그룹의 모든 레코드에 대해 동일한 이름을 입력합니다.

레코드 이름에 대한 자세한 내용은 레코드 이름 섹션을 참조하십시오.

레코드 유형

DNS 레코드 유형입니다. 자세한 내용은 지원되는 DNS 레코드 유형 단원을 참조하십시오.

트래픽을 라우팅할 AWS 리소스를 기반으로 해당 값을 선택합니다. 지리 위치 레코드 그룹의 모든 레코드에 대해 동일 값을 선택합니다.

API Gateway 사용자 지정 리전 API 또는 엣지 최적화 API

A - IPv4 주소(A - IPv4 address)를 선택합니다.

Amazon VPC 인터페이스 엔드포인트

A - IPv4 주소(A - IPv4 address)를 선택합니다.

CloudFront 배포

A - IPv4 주소(A - IPv4 address)를 선택합니다.

배포에 대해 IPv6가 활성화되어 있다면 두 개의 레코드를 생성합니다. 하나는 유형(Type) 값이 A - IPv4 주소(A - IPv4 address)이고 하나는 값이 AAAA - IPv6 주소(AAAA - IPv6 address)입니다.

App Runner 서비스

A - IPv4 주소(A - IPv4 address)를 선택합니다.

리전별 하위 도메인이 있는 Elastic Beanstalk 환경

A - IPv4 주소(A - IPv4 address)를 선택합니다.

ELB 로드 밸런서

A - IPv4 address(A - IPv4 주소) 또는 AAAA - IPv6 address(AAAA - IPv6 주소) 선택

Amazon S3 버킷

A - IPv4 주소(A - IPv4 address)를 선택합니다.

OpenSearch Service

A - IPv4 address(A - IPv4 주소) 또는 AAAA - IPv6 address(AAAA - IPv6 주소) 선택

호스팅 영역의 또 다른 레코드

별칭을 생성 중인 레코드 유형을 선택합니다. NS 및 SOA를 제외한 모든 유형이 지원됩니다.

> **Note**
>
> 호스팅 영역(zone apex라고도 함)과 이름이 같은 별칭 레코드를 생성한다면, 유형 값이 CNAME인 레코드로 트래픽을 라우팅할 수 없습니다. 이는 별칭 레코드가 트래픽이 라우팅되는 레코드와 동일한 형식이어야 하고, zone apex에 대한 CNAME 레코드 생성은 별칭 레코드에 대해서도 지원되지 않기 때문입니다.

값/트래픽 라우팅 대상

목록에서 선택하거나 필드에 입력하는 값은 트래픽을 라우팅하는 AWS 리소스에 따라 달라집니다.

대상으로 지정할 수 있는 AWS 리소스에 대한 자세한 내용은 섹션을 참조하세요값/트래픽 라우팅 대상.

트래픽을 특정 AWS 리소스로 라우팅하도록 Route 53를 구성하는 방법에 대한 자세한 내용은 섹션을 참조하세요AWS 리소스로 인터넷 트래픽 라우팅.

위치

쿼리를 보낸 위치를 기반으로 하는 DNS 쿼리에 응답하도록 Route 53을 구성할 때는 Route 53이 이 레코드 설정으로 응답하길 원하는 대륙 또는 국가를 선택합니다. Route 53이 미국의 개별 주에 대한 DNS 쿼리에 응답하길 원할 경우 먼저 위치(Location) 목록에서 미국(United States)을 선택한 다음 미국 주(U.S. states) 목록에서 주를 선택합니다.

프라이빗 호스팅 영역의 경우 리소스가 AWS 리전 있는에 가장 가까운 대륙, 국가 또는 하위 부문을 선택합니다. 예를 들어 리소스가 us-east-1에 있으면 북미, 미국 또는 버지니아를 지정할 수 있습니다.

> **Important**
>
> 위치(Location)에 대한 기본(Default) 값을 갖는 하나의 지리적 위치 레코드를 생성하는 것이 좋습니다. 그러면 레코드를 생성하지 않은 지리적 위치와 Route 53이 위치를 식별하지 못하는 IP 주소도 포함됩니다.

레코드 이름(Record name) 및 레코드 유형(Record type) 값이 지리적 위치 레코드와 같은 값을 갖는 비-지리적 위치 레코드를 생성할 수 없습니다.

자세한 내용은 지리적 라우팅 단원을 참조하십시오.

다음은 Amazon Route 53이 각 대륙과 연결되는 국가입니다. 국가 코드는 ISO 3166부터 시작합니다. 자세한 내용은 Wikipedia 도움말 ISO 3166-1 alpha-2를 참조하십시오.

아프리카(AF)

AO, BF, BI, BJ, BW, CD, CF, CG, CI, CM, CV, DJ, DZ, EG, ER, ET, GA, GH, GM, GN, GQ, GW, KE, KM, LR, LS, LY, MA, MG, ML, MR, MU, MW, MZ, NA, NE, NG, RE, RW, SC, SD, SH, SL, SN, SO, SS, ST, SZ, TD, TG, TN, TZ, UG, YT, ZA, ZM, ZW

남극 대륙(AN)

AQ, GS, TF

아시아(AS)

AE, AF, AM, AZ, BD, BH, BN, BT, CC, CN, GE, HK, ID, IL, IN, IO, IQ, IR, JO, JP, KG, KH, KP, KR, KW, KZ, LA, LB, LK, MM, MN, MO, MV, MY, NP, OM, PH, PK, PS, QA, SA, SG, SY, TH, TJ, TM, TW, UZ, VN, YE

유럽(EU)

AD, AL, AT, AX, BA, BE, BG, BY, CH, CY, CZ, DE, DK, EE, ES, FI, FO, FR, GB, GG, GI, GR, HR, HU, IE, IM, IS, IT, JE, LI, LT, LU, LV, MC, MD, ME, MK, MT, NL, NO, PL, PT, RO, RS, RU, SE, SI, SJ, SK, SM, TR, UA, VA, XK

북아메리카(NA)

AG, AI, AW, BB, BL, BM, BQ, BS, BZ, CA, CR, CU, CW, DM, DO, GD, GL, GP, GT, HN, HT, JM, KN, KY, LC, MF, MQ, MS, MX, NI, PA, PM, PR, SV, SX, TC, TT, US, VC, VG, VI

오세아니아(OC)

AS, AU, CK, FJ, FM, GU, KI, MH, MP, NC, NF, NR, NU, NZ, PF, PG, PN, PW, SB, TK, TL, TO, TV, UM, VU, WF, WS

남아메리카(SA)

AR, BO, BR, CL, CO, EC, FK, GF, GY, PE, PY, SR, UY, VE

> **Note**
>
> Route 53은 다음 국가, 즉 부베 섬(BV), 크리스마스 섬(CX), 서부 사하라(EH), 허드 섬 및 맥도널드 제도(HM)의 지리 위치 레코드 생성을 지원하지 않습니다. 이들 국가의 IP 주소에 관한 데이터가 없습니다.

미국 주

Route 53이 쿼리가 발생한 미국 주를 토대로 DNS 쿼리에 응답하도록 구성할 때는 미국 주(U.S. states) 목록에서 주를 선택합니다. 미국 영토(예: 푸에르토리코)는 위치 목록에 국가로 표시됩니다.

> **Important**
>
> 일부 IP 주소는 개별 주가 아니라 미국과 관련이 있습니다. 미국 내 모든 주의 레코드를 생성할 경우에는 이러한 무관한 IP 주소의 쿼리를 라우팅할 미국 레코드도 생성하는 것이 좋습니다. 미국의 레코드를 생성하지 않으면 Route 53이 비연관 미국 IP 주소의 DNS 쿼리에 기본 지리 위치 레코드(생성한 경우)의 설정 또는 "응답 없음"으로 응답합니다.

상태 확인

Route 53가 지정된 엔드포인트 상태를 점검하고 엔드포인트가 정상할 때만 이 레코드를 사용하여 DNS 쿼리에 응답하길 원할 경우 상태 확인을 선택합니다.

Route 53는 레코드에 지정된 엔드포인트, 예를 들어 값(Value) 필드에서 IP 주소로 지정된 엔드포인트의 상태는 점검하지 않습니다. 레코드의 상태 확인을 선택하면 Route 53가 상태 확인에서 지정한 엔드포인트의 상태를 점검합니다. Route 53가 엔드포인트가 정상인지 여부를 결정하는 방법은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 섹션을 참조하세요.

상태 확인과 레코드를 연관시키는 것은 Route 53가 둘 이상의 레코드 사이에서 DNS 쿼리에 응답할 레코드를 선택할 때 그리고 Route 53가 상태 확인 상태를 선택의 기준으로 삼을 때만 유용합니다. 다음 구성에서만 상태 확인을 사용합니다.

- 이름, 유형 및 라우팅 정책(예: 장애 조치 또는 가중치 레코드)이 동일한 레코드 그룹의 모든 레코드 상태를 확인하고 모든 레코드에 대한 상태 확인 ID를 지정하는 경우. 레코드의 상태 확인에서 양호하지 않은 엔드포인트가 지정될 경우 Route 53는 해당 레코드 값을 사용하는 쿼리에 대한 응답을 중단합니다.
- 별칭 레코드 또는 장애 조치 별칭, 지리적 위치 별칭, 대기 시간 별칭, IP 기반 별칭 또는 가중치 기반 별칭 그룹에 속한 레코드에 대해 대상 상태 평가(Evaluate Target Health)에서 예(Yes)를 선택하는 경우. 별칭 레코드가 동일한 호스팅 영역의 별칭이 아닌 레코드를 참조하는 경우 참조된 레코드의 상태 확인도 지정해야 합니다. 상태 확인과 별칭 레코드를 연관시키고 대상 상태 평가에서 예를 선택하는 경우 둘 다 true로 평가되어야 합니다. 자세한 내용은 상태 확인을 별칭 레코드와 연결하면 어떻게 됩니까? 단원을 참조하십시오.

상태 확인에서 도메인 이름만으로 엔드포인트를 지정할 경우에는 각 엔드포인트마다 별도의 상태 확인을 생성하는 것이 좋습니다. 예를 들어, www.example.com의 콘텐츠를 제공하는 각 HTTP 서버마다 상태 확인을 생성합니다. 도메인 이름(Domain name)의 값은 레코드의 이름(example.com)이 아니라 서버의 도메인 이름(예: us-east-2-www.example.com)을 지정합니다.

> **Important**
>
> 이 구성에서 [Domain name]의 값이 레코드의 이름과 일치하는 상태 확인을 생성한 후 상태 확인을 이러한 레코드와 연결하는 경우 상태 확인 결과를 예측할 수 없습니다.

지리 위치 레코드에서 엔드포인트가 양호하지 않을 경우 Route 53은 규모가 더 큰 관련 지리적 리전의 레코드를 조회합니다. 예를 들어, 미국 내 주, 미국, 북미 및 전체 위치에 대한 레코드가 있다고 가정합니다(위치가 기본값임). 주 레코드의 엔드포인트가 양호하지 않을 경우 Route 53은 미국, 북미 및 전체 위치 순으로 엔드포인트가 양호한 레코드를 찾을 때까지 레코드를 확인합니다. 모든 지리적 위치에 대한 레코드를 포함하여 모든 적용 가능한 레코드가 비정상적인 경우 Route 53은 가장 작은 지리적 리전에 대한 레코드 값을 사용하여 DNS 쿼리에 응답합니다.

대상 상태 평가

엔드포인트에서 지정된 리소스의 상태를 확인하여 Route 53가 레코드를 사용해 DNS 쿼리에 응답할지 여부를 결정하게 하려는 경우 예(Yes)를 선택합니다.

다음 사항에 유의하세요.

API Gateway 사용자 지정 리전 API와 엣지 최적화 API

엔드포인트가 API Gateway 사용자 지정 리전 API 또는 엣지 최적화 API인 경우 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정하기 위한 특별한 요구 사항은 없습니다.

CloudFront 배포

엔드포인트가 CloudFront 배포인 경우 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정할 수 없습니다.

리전별 하위 도메인이 있는 Elastic Beanstalk 환경

엔드포인트(Endpoint)에 Elastic Beanstalk 환경을 지정하고 환경에 ELB 로드 밸런서가 포함된 경우, Elastic Load Balancing은 로드 밸런서에 등록된 정상 Amazon EC2 인스턴스로만 쿼리를 라우팅합니다. (하나의 환경에 한 개 이상의 Amazon EC2 인스턴스가 포함된 경우 ELB 로드 밸런서가 자동으로 포함됩니다.) 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정했는데 정상인 Amazon EC2 인스턴스가 없거나 로드 밸런서 자체가 비정상인 경우 Route 53는 양호한 다른 리소스로 쿼리를 라우팅합니다.

환경에 하나의 Amazon EC2 인스턴스가 포함된 경우에는 특별한 요구 사항이 없습니다.

ELB 로드 밸런서

상태 확인 동작은 로드 밸런서의 유형에 따라 달랍니다.

- Classic Load Balancer: 엔드포인트(Endpoint)에 ELB Classic Load Balancer를 지정한 경우, Elastic Load Balancing은 로드 밸런서에 등록된 정상 Amazon EC2 인스턴스로만 쿼리를 라우팅합니다. 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정하고 EC2 인스턴스가 정상 상태가 아니거나 로드 밸런서 자체가 비정상인 경우 Route 53는 쿼리를 다른 리소스로 라우팅합니다.
- Application Load Balancer 및 Network Load Balancer - ELB Application Load Balancer 또는 Network Load Balancer를 지정하고 대상 상태 평가(Evaluate Target Health)를 예(Yes)로 설정한 경우 Route 53는 로드 밸런서와 연결된 대상 그룹의 상태에 따라 쿼리를 로드 밸런서로 라우팅합니다.
  - Application 또는 Network Load Balancer가 정상 상태로 간주되려면 대상을 포함하는 모든 대상 그룹에 정상 상태 대상이 하나 이상 포함되어야 합니다. 대상 그룹에 정상이 아닌 대상만 포함되는 경우 로드 밸런서는 정상이 아닌 상태로 간주되고 Route 53는 쿼리를 다른 리소스로 라우팅합니다.
  - 등록된 대상이 없는 대상 그룹은 정상이 아닌 상태로 간주됩니다.

> **Note**
>
> 로드 밸런서를 생성할 때 Elastic Load Balancing 상태 확인에 대한 설정을 구성하게 되는데, 이러한 확인은 Route 53 상태 확인은 아니지만 비슷한 기능을 수행합니다. ELB 로드 밸런서에 등록하는 EC2 인스턴스에 대해 Route 53 상태 확인을 생성하지 마십시오.

S3 버킷

엔드포인트가 S3 버킷인 경우 대상 상태 평가(Evaluate Target Health)를 예(Yes)로 설정하는 데 필요한 특정 요건은 없습니다.

Amazon VPC 인터페이스 엔드포인트

엔드포인트가 Amazon VPC 인터페이스 엔드포인트인 경우 대상 상태 평가(Evaluate Target Health)를 예(Yes)로 설정하는 데 필요한 특별한 요구 사항이 없습니다.

동일 호스팅 영역 내 다른 레코드

엔드포인트에서 지정하는 AWS 리소스가 레코드 또는 레코드 그룹(예: 가중치 기반 레코드 그룹)이지만 다른 별칭 레코드가 아닌 경우 상태 확인을 엔드포인트의 모든 레코드와 연결하는 것이 좋습니다. 자세한 내용은 상태 확인을 생략하면 어떻게 됩니까? 단원을 참조하십시오.

레코드 ID

지리 위치 레코드 그룹에 있는 이 레코드를 고유하게 식별하는 값을 선택합니다.

지리 근접성 레코드에 특정된 값

지리 근접성 레코드를 생성할 때 다음과 같은 값을 지정합니다.

주제

- 라우팅 정책
- 레코드 이름
- 레코드 유형
- TTL(초)
- 값/트래픽 라우팅 대상
- 엔드포인트 위치
- 편향
- 상태 확인
- 레코드 ID

라우팅 정책

지리 근접성을 선택합니다.

레코드 이름

트래픽을 라우팅할 도메인 또는 하위 도메인의 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

> **Note**
>
> 호스팅 영역과 이름이 동일한 레코드를 생성할 경우 이름 필드에 값(예: @ 기호)을 입력하지 마십시오.

지리 근접성 레코드 그룹의 모든 레코드에 대해 동일한 이름을 입력합니다.

레코드 이름에 대한 자세한 내용은 레코드 이름 섹션을 참조하십시오.

레코드 유형

DNS 레코드 유형입니다. 자세한 내용은 지원되는 DNS 레코드 유형 단원을 참조하십시오.

지리 근접성 레코드 그룹의 모든 레코드에 대해 동일한 값을 선택합니다.

TTL(초)

DNS recursive resolver가 이 레코드에 관한 정보를 캐싱할 시간(초)입니다. 더 긴 값(예: 172800초 또는 2일)을 지정한 경우, 이 레코드의 최신 정보를 얻으려면 DNS recursive resolver의 Route 53에 대한 호출 수를 줄여야 합니다. 이렇게 하면 지연 시간을 줄이고 Route 53 서비스 비용을 줄이는 효과가 있습니다. 자세한 내용은 Amazon Route 53가 도메인의 트래픽을 라우팅하는 방법 단원을 참조하십시오.

그러나 TTL에 더 긴 값을 지정하면 recursive resolver가 Route 53에 최신 정보를 요청하기 전에 기간이 더 긴 캐시 값을 사용하므로 레코드(예: 새 IP 주소) 변경이 적용되는 데 걸리는 시간이 길어집니다. 이미 사용 중인 도메인이나 하위 도메인의 설정을 변경하는 경우 처음에는 더 짧은 값(예: 300초)을 지정하고 새 설정이 올바른지 확인한 후 값을 늘리는 것이 좋습니다.

이 레코드를 상태 점검과 연관시킬 경우에는 클라이언트가 상태 변경에 빠르게 응답하도록 TTL을 60초 이하로 지정하는 것이 좋습니다.

값/트래픽 라우팅 대상

IP 주소 또는 레코드 유형에 따라 다른 값(IP address or another value depending on the record type)을 선택합니다. 레코드 유형(Record type) 값에 해당하는 값을 입력합니다. CNAME을 제외한 모든 유형은 둘 이상의 값을 입력할 수 있습니다. 각 값을 별도의 라인에 입력합니다.

트래픽을 라우팅하거나 다음 값을 지정할 수 있습니다.

- A – IPv4 주소
- AAAA - IPv6 주소
- CAA - 인증 기관 인증
- CNAME – 정식 이름
- MX - 메일 교환
- NAPTR - 이름 권한 포인터
- PTR - 포인터
- SPF - 발신자 정책 프레임워크
- SRV - 서비스 로케이터
- TXT - 텍스트

위의 값에 대한 자세한 내용은 값/트래픽 라우팅 대상에 일반적인 값을 참조하세요.

엔드포인트 위치

다음 방법 중 하나를 사용하여 리소스 엔드포인트 위치를 지정할 수 있습니다.

사용자 지정 좌표

지리적 영역의 경도와 위도를 지정합니다.

AWS 리전

위치 목록에서 사용 가능한 리전을 선택합니다.

리전에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

AWS 로컬 영역 그룹

위치 목록에서 사용 가능한 로컬 영역 그룹을 선택합니다.

로컬 영역에 대한 자세하 내용은 AWS 로컬 영역 사용 설명서의 사용 가능한 로컬 영역을 참조하세요. 로컬 영역 그룹은 일반적으로 종료 문자가 없는 로컬 영역입니다. 예를 들어 로컬 영역이 `us-east-1-bue-1a`인 경우 로컬 영역 그룹은 `us-east-1-bue-1`입니다.

describe-availability-zones CLI 명령을 사용하여 특정 로컬 영역에 대한 로컬 영역 그룹을 식별할 수도 있습니다.

```
aws ec2 describe-availability-zones --region us-west-2 --all-availability-zones --query
 "AvailabilityZones[?ZoneName=='us-west-2-den-1a']" | grep "GroupName"
```

이 명령은 로컬 영역 `us-west-2-den-1a`가 로컬 영역 그룹 `us-west-2-den-1`에 속하도록 지정하여 `"GroupName": "us-west-2-den-1"`를 반환합니다.

레코드 이름 및 레코드 유형 값이 지리 근접성 레코드와 같은 값을 갖는 비-지리 근접성 레코드를 생성할 수 없습니다.

동일한 레코드 이름 및 레코드 유형에 대해 동일한 위치를 지정하는 지리 근접성 리소스 레코드 세트 2개를 생성할 수도 없습니다.

편향

편향은 Route 53가 트래픽을 리소스로 라우팅하는 지리적 영역의 크기를 확장하거나 축소합니다. 긍정 편향은 영역을 확장하고 부정 편향은 영역을 축소합니다. 자세한 내용은 Amazon Route 53가 바이어스를 사용하여 트래픽을 라우팅하려면 단원을 참조하십시오.

상태 확인

Route 53가 지정된 엔드포인트 상태를 점검하고 엔드포인트가 정상할 때만 이 레코드를 사용하여 DNS 쿼리에 응답하길 원할 경우 상태 확인을 선택합니다.

Route 53는 레코드에 지정된 엔드포인트, 예를 들어 값(Value) 필드에서 IP 주소로 지정된 엔드포인트의 상태는 점검하지 않습니다. 레코드의 상태 확인을 선택하면 Route 53가 상태 확인에서 지정한 엔드포인트의 상태를 점검합니다. Route 53가 엔드포인트가 정상인지 여부를 결정하는 방법은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 섹션을 참조하세요.

상태 확인과 레코드를 연관시키는 것은 Route 53가 둘 이상의 레코드 사이에서 DNS 쿼리에 응답할 레코드를 선택할 때 그리고 Route 53가 상태 확인 상태를 선택의 기준으로 삼을 때만 유용합니다. 다음 구성에서만 상태 확인을 사용합니다.

- 이름, 유형 및 라우팅 정책(예: 장애 조치 또는 가중치 레코드)이 동일한 레코드 그룹의 모든 레코드 상태를 확인하고 모든 레코드에 대한 상태 확인 ID를 지정하는 경우. 레코드의 상태 확인에서 양호하지 않은 엔드포인트가 지정될 경우 Route 53는 해당 레코드 값을 사용하는 쿼리에 대한 응답을 중단합니다.
- 별칭 레코드 또는 장애 조치 별칭, 지리적 위치 별칭, 지리 근접성 별칭, 대기 시간 별칭, IP 기반 별칭 또는 가중치 기반 별칭 그룹에 속한 레코드에 대해 대상 상태 평가에서 예를 선택하는 경우. 별칭 레코드가 동일한 호스팅 영역의 별칭이 아닌 레코드를 참조하는 경우 참조된 레코드의 상태 확인도 지정해야 합니다. 상태 확인과 별칭 레코드를 연관시키고 대상 상태 평가에서 예를 선택하는 경우 둘 다 true로 평가되어야 합니다. 자세한 내용은 상태 확인을 별칭 레코드와 연결하면 어떻게 됩니까? 단원을 참조하십시오.

상태 확인에서 도메인 이름만으로 엔드포인트를 지정할 경우에는 각 엔드포인트마다 별도의 상태 확인을 생성하는 것이 좋습니다. 예를 들어, www.example.com의 콘텐츠를 제공하는 각 HTTP 서버마다 상태 확인을 생성합니다. 도메인 이름의 값은 레코드의 이름(example.com)이 아니라 서버의 도메인 이름(예: us-east-2-www.example.com)을 지정합니다.

> **Important**
>
> 이 구성에서 도메인 이름의 값이 레코드의 이름과 일치하는 상태 확인을 생성한 후 상태 확인을 이러한 레코드와 연결하는 경우 상태 확인 결과를 예측할 수 없습니다.

지리 근접성 레코드의 경우 엔드포인트가 비정상이면 Route 53는 여전히 정상인 가장 가까운 엔드포인트를 찾습니다.

레코드 ID

지리 근접성 레코드 그룹에 있는 이 레코드를 고유하게 식별하는 값을 입력합니다.

지리 근접성 별칭 레코드에 특정된 값

지리 근접성 별칭 레코드를 생성할 때 다음과 같은 값을 지정합니다.

자세한 내용은 별칭 또는 비 별칭 레코드 선택 단원을 참조하십시오.

주제

- 라우팅 정책
- 레코드 이름
- 레코드 유형
- 값/트래픽 라우팅 대상
- 엔드포인트 위치
- 편향
- 상태 확인
- 대상 상태 평가
- 레코드 ID

라우팅 정책

지리 근접성을 선택합니다.

레코드 이름

트래픽을 라우팅할 도메인 또는 하위 도메인의 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

> **Note**
>
> 호스팅 영역과 이름이 동일한 레코드를 생성할 경우 레코드 이름(Record name) 필드에 값(예: @ 기호)을 입력하지 마세요.

지리 근접성 레코드 그룹의 모든 레코드에 대해 동일한 이름을 입력합니다.

레코드 이름에 대한 자세한 내용은 레코드 이름 섹션을 참조하십시오.

레코드 유형

DNS 레코드 유형입니다. 자세한 내용은 지원되는 DNS 레코드 유형 단원을 참조하십시오.

트래픽을 라우팅할 AWS 리소스를 기반으로 해당 값을 선택합니다. 지리 근접성 레코드 그룹의 모든 레코드에 대해 동일한 값을 선택합니다.

API Gateway 사용자 지정 리전 API 또는 엣지 최적화 API

A - IPv4 주소(A - IPv4 address)를 선택합니다.

Amazon VPC 인터페이스 엔드포인트

A - IPv4 주소(A - IPv4 address)를 선택합니다.

CloudFront 배포

A - IPv4 주소(A - IPv4 address)를 선택합니다.

배포에 대해 IPv6가 활성화되어 있다면 두 개의 레코드를 생성합니다. 하나는 유형(Type) 값이 A - IPv4 주소(A - IPv4 address)이고 하나는 값이 AAAA - IPv6 주소(AAAA - IPv6 address)입니다.

App Runner 서비스

A - IPv4 주소(A - IPv4 address)를 선택합니다.

리전별 하위 도메인이 있는 Elastic Beanstalk 환경

A - IPv4 주소(A - IPv4 address)를 선택합니다.

ELB 로드 밸런서

A - IPv4 address(A - IPv4 주소) 또는 AAAA - IPv6 address(AAAA - IPv6 주소) 선택

Amazon S3 버킷

A - IPv4 주소(A - IPv4 address)를 선택합니다.

OpenSearch Service

A - IPv4 address(A - IPv4 주소) 또는 AAAA - IPv6 address(AAAA - IPv6 주소) 선택

호스팅 영역의 또 다른 레코드

별칭을 생성 중인 레코드 유형을 선택합니다. NS 및 SOA를 제외한 모든 유형이 지원됩니다.

> **Note**
>
> 호스팅 영역(zone apex라고도 함)과 이름이 같은 별칭 레코드를 생성한다면, 유형 값이 CNAME인 레코드로 트래픽을 라우팅할 수 없습니다. 이는 별칭 레코드가 트래픽이 라우팅

되는 레코드와 동일한 형식이어야 하고, zone apex에 대한 CNAME 레코드 생성은 별칭 레코드에 대해서도 지원되지 않기 때문입니다.

값/트래픽 라우팅 대상

목록에서 선택하거나 필드에 입력하는 값은 트래픽을 라우팅하는 AWS 리소스에 따라 달라집니다.

대상으로 지정할 수 있는 AWS 리소스에 대한 자세한 내용은 섹션을 참조하세요값/트래픽 라우팅 대상.

트래픽을 특정 AWS 리소스로 라우팅하도록 Route 53를 구성하는 방법에 대한 자세한 내용은 섹션을 참조하세요AWS 리소스로 인터넷 트래픽 라우팅.

엔드포인트 위치

다음 방법 중 하나를 사용하여 리소스 엔드포인트 위치를 지정할 수 있습니다.

사용자 지정 좌표

지리적 영역의 경도와 위도를 지정합니다.

AWS 리전

위치 목록에서 사용 가능한 리전을 선택합니다.

리전에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

AWS 로컬 영역 그룹

위치 목록에서 사용 가능한 로컬 영역 리전을 선택합니다.

로컬 영역에 대한 자세하 내용은 AWS 로컬 영역 사용 설명서의 사용 가능한 로컬 영역을 참조하세요. 로컬 영역 그룹은 일반적으로 종료 문자가 없는 로컬 영역입니다. 예를 들어 로컬 영역이 `us-east-1-bue-1a`인 경우 로컬 영역 그룹은 `us-east-1-bue-1`입니다.

describe-availability-zones CLI 명령을 사용하여 특정 로컬 영역에 대한 로컬 영역 그룹을 식별할 수도 있습니다.

```
aws ec2 describe-availability-zones --region us-west-2 --all-availability-zones --query
 "AvailabilityZones[?ZoneName=='us-west-2-den-1a']" | grep "GroupName"
```

이 명령은 로컬 영역 us-west-2-den-1a가 로컬 영역 그룹 us-west-2-den-1에 속하도록 지정하여 "GroupName": "us-west-2-den-1"를 반환합니다.

레코드 이름 및 레코드 유형 값이 지리 근접성 레코드와 같은 값을 갖는 비-지리 근접성 레코드를 생성할 수 없습니다.

동일한 레코드 이름 및 레코드 유형에 대해 동일한 위치를 지정하는 지리 근접성 리소스 레코드 세트 2개를 생성할 수도 없습니다.

자세한 내용은 available-local-zones.html을 참조하세요.

편향

편향은 Route 53가 트래픽을 리소스로 라우팅하는 지리적 영역의 크기를 확장하거나 축소합니다. 긍정 편향은 영역을 확장하고 부정 편향은 영역을 축소합니다. 자세한 내용은 Amazon Route 53가 바이어스를 사용하여 트래픽을 라우팅하려면 단원을 참조하십시오.

상태 확인

Route 53가 지정된 엔드포인트 상태를 점검하고 엔드포인트가 정상할 때만 이 레코드를 사용하여 DNS 쿼리에 응답하길 원할 경우 상태 확인을 선택합니다.

Route 53는 레코드에 지정된 엔드포인트, 예를 들어 값(Value) 필드에서 IP 주소로 지정된 엔드포인트의 상태는 점검하지 않습니다. 레코드의 상태 확인을 선택하면 Route 53가 상태 확인에서 지정한 엔드포인트의 상태를 점검합니다. Route 53가 엔드포인트가 정상인지 여부를 결정하는 방법은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 섹션을 참조하세요.

상태 확인과 레코드를 연관시키는 것은 Route 53가 둘 이상의 레코드 사이에서 DNS 쿼리에 응답할 레코드를 선택할 때 그리고 Route 53가 상태 확인 상태를 선택의 기준으로 삼을 때만 유용합니다. 다음 구성에서만 상태 확인을 사용합니다.

- 이름, 유형 및 라우팅 정책(예: 장애 조치 또는 가중치 레코드)이 동일한 레코드 그룹의 모든 레코드 상태를 확인하고 모든 레코드에 대한 상태 확인 ID를 지정하는 경우. 레코드의 상태 확인에서 양호하지 않은 엔드포인트가 지정될 경우 Route 53는 해당 레코드 값을 사용하는 쿼리에 대한 응답을 중단합니다.
- 별칭 레코드 또는 장애 조치 별칭, 지리적 위치 별칭, 지리 근접성 별칭, 대기 시간 별칭, IP 기반 별칭 또는 가중치 기반 별칭 그룹에 속한 레코드에 대해 대상 상태 평가에서 예를 선택하는 경우. 별칭 레코드가 동일한 호스팅 영역의 별칭이 아닌 레코드를 참조하는 경우 참조된 레코드의 상태 확인도 지정해야 합니다. 상태 확인과 별칭 레코드를 연관시키고 대상 상태 평가에서 예를 선택하는 경우 둘 다 true로 평가되어야 합니다. 자세한 내용은 상태 확인을 별칭 레코드와 연결하면 어떻게 됩니까? 단원을 참조하십시오.

상태 확인에서 도메인 이름만으로 엔드포인트를 지정할 경우에는 각 엔드포인트마다 별도의 상태 확인을 생성하는 것이 좋습니다. 예를 들어, www.example.com의 콘텐츠를 제공하는 각 HTTP 서버마다 상태 확인을 생성합니다. 도메인 이름(Domain name)의 값은 레코드의 이름(example.com)이 아니라 서버의 도메인 이름(예: us-east-2-www.example.com)을 지정합니다.

> **Important**
>
> 이 구성에서 [Domain name]의 값이 레코드의 이름과 일치하는 상태 확인을 생성한 후 상태 확인을 이러한 레코드와 연결하는 경우 상태 확인 결과를 예측할 수 없습니다.

지리 근접성 레코드의 경우 엔드포인트가 비정상이면 Route 53는 여전히 정상인 가장 가까운 엔드포인트를 찾습니다.

대상 상태 평가

엔드포인트에서 지정된 리소스의 상태를 확인하여 Route 53가 레코드를 사용해 DNS 쿼리에 응답할지 여부를 결정하게 하려는 경우 예(Yes)를 선택합니다.

다음 사항에 유의하세요.

API Gateway 사용자 지정 리전 API와 엣지 최적화 API

엔드포인트가 API Gateway 사용자 지정 리전 API 또는 엣지 최적화 API인 경우 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정하기 위한 특별한 요구 사항은 없습니다.

CloudFront 배포

엔드포인트가 CloudFront 배포인 경우 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정할 수 없습니다.

리전별 하위 도메인이 있는 Elastic Beanstalk 환경

엔드포인트(Endpoint)에 Elastic Beanstalk 환경을 지정하고 환경에 ELB 로드 밸런서가 포함된 경우, Elastic Load Balancing은 로드 밸런서에 등록된 정상 Amazon EC2 인스턴스로만 쿼리를 라우팅합니다. (하나의 환경에 한 개 이상의 Amazon EC2 인스턴스가 포함된 경우 ELB 로드 밸런서가 자동으로 포함됩니다.) 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정했는데 정상인 Amazon EC2 인스턴스가 없거나 로드 밸런서 자체가 비정상인 경우 Route 53는 양호한 다른 리소스로 쿼리를 라우팅합니다.

환경에 하나의 Amazon EC2 인스턴스가 포함된 경우에는 특별한 요구 사항이 없습니다.

ELB 로드 밸런서

상태 확인 동작은 로드 밸런서의 유형에 따라 달랍니다.

- Classic Load Balancer: 엔드포인트(Endpoint)에 ELB Classic Load Balancer를 지정한 경우, Elastic Load Balancing은 로드 밸런서에 등록된 정상 Amazon EC2 인스턴스로만 쿼리를 라우팅합니다. 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정하고 EC2 인스턴스가 정상 상태가 아니거나 로드 밸런서 자체가 비정상인 경우 Route 53는 쿼리를 다른 리소스로 라우팅합니다.
- Application Load Balancer 및 Network Load Balancer - ELB Application Load Balancer 또는 Network Load Balancer를 지정하고 대상 상태 평가(Evaluate Target Health)를 예(Yes)로 설정한 경우 Route 53는 로드 밸런서와 연결된 대상 그룹의 상태에 따라 쿼리를 로드 밸런서로 라우팅합니다.
  - Application 또는 Network Load Balancer가 정상 상태로 간주되려면 대상을 포함하는 모든 대상 그룹에 정상 상태 대상이 하나 이상 포함되어야 합니다. 대상 그룹에 정상이 아닌 대상만 포함되는 경우 로드 밸런서는 정상이 아닌 상태로 간주되고 Route 53는 쿼리를 다른 리소스로 라우팅합니다.
  - 등록된 대상이 없는 대상 그룹은 정상이 아닌 상태로 간주됩니다.

> **Note**
>
> 로드 밸런서를 생성할 때 Elastic Load Balancing 상태 확인에 대한 설정을 구성하게 되는데, 이러한 확인은 Route 53 상태 확인은 아니지만 비슷한 기능을 수행합니다. ELB 로드 밸런서에 등록하는 EC2 인스턴스에 대해 Route 53 상태 확인을 생성하지 마십시오.

S3 버킷

엔드포인트가 S3 버킷인 경우 대상 상태 평가(Evaluate Target Health)를 예(Yes)로 설정하는 데 필요한 특정 요건은 없습니다.

Amazon VPC 인터페이스 엔드포인트

엔드포인트가 Amazon VPC 인터페이스 엔드포인트인 경우 대상 상태 평가(Evaluate Target Health)를 예(Yes)로 설정하는 데 필요한 특별한 요구 사항이 없습니다.

동일 호스팅 영역 내 다른 레코드

엔드포인트에서 지정하는 AWS 리소스가 레코드 또는 레코드 그룹(예: 가중치 기반 레코드 그룹)이지만 다른 별칭 레코드가 아닌 경우 상태 확인을 엔드포인트의 모든 레코드와 연결하는 것이 좋습니다. 자세한 내용은 상태 확인을 생략하면 어떻게 됩니까? 단원을 참조하십시오.

레코드 ID

지리 근접성 레코드 그룹에 있는 이 레코드를 고유하게 식별하는 값을 입력합니다.

지연 시간 레코드에 특정한 값

지연 시간 레코드를 생성할 때 다음과 같은 값을 지정합니다.

주제

- 라우팅 정책
- 레코드 이름
- 레코드 유형
- TTL(초)
- 값/트래픽 라우팅 대상
- 리전
- 상태 확인
- 레코드 ID

라우팅 정책

지연 시간(Latency)을 선택합니다.

레코드 이름

트래픽을 라우팅할 도메인 또는 하위 도메인의 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

> **Note**
>
> 호스팅 영역과 이름이 동일한 레코드를 생성할 경우 레코드 이름(Record name) 필드에 값(예: @ 기호)을 입력하지 마세요.

지연 시간 레코드 그룹의 모든 레코드에 대해 동일한 이름을 입력합니다.

레코드 이름에 대한 자세한 내용은 레코드 이름 섹션을 참조하십시오.

레코드 유형

DNS 레코드 유형입니다. 자세한 내용은 지원되는 DNS 레코드 유형 단원을 참조하십시오.

Route 53이 DNS 쿼리에 응답하는 방식에 따라 유형(Type)에 대한 값을 선택합니다.

지연 시간 레코드 그룹의 모든 레코드에 대해 동일 값을 선택합니다.

TTL(초)

DNS recursive resolver가 이 레코드에 관한 정보를 캐싱할 시간(초)입니다. 더 긴 값(예: 172800초 또는 2일)을 지정한 경우, 이 레코드의 최신 정보를 얻으려면 DNS recursive resolver의 Route 53에 대한 호출 수를 줄여야 합니다. 이렇게 하면 지연 시간을 줄이고 Route 53 서비스 비용을 줄이는 효과가 있습니다. 자세한 내용은 Amazon Route 53가 도메인의 트래픽을 라우팅하는 방법 단원을 참조하십시오.

그러나 TTL에 더 긴 값을 지정하면 recursive resolver가 Route 53에 최신 정보를 요청하기 전에 기간이 더 긴 캐시 값을 사용하므로 레코드(예: 새 IP 주소) 변경이 적용되는 데 걸리는 시간이 길어집니다. 이미 사용 중인 도메인이나 하위 도메인의 설정을 변경하는 경우 처음에는 더 짧은 값(예: 300초)을 지정하고 새 설정이 올바른지 확인한 후 값을 늘리는 것이 좋습니다.

이 레코드를 상태 점검과 연관시킬 경우에는 클라이언트가 상태 변경에 빠르게 응답하도록 TTL을 60초 이하로 지정하는 것이 좋습니다.

값/트래픽 라우팅 대상

IP 주소 또는 레코드 유형에 따라 다른 값(IP address or another value depending on the record type)을 선택합니다. 레코드 유형(Record type) 값에 해당하는 값을 입력합니다. CNAME을 제외한 모든 유형은 둘 이상의 값을 입력할 수 있습니다. 각 값을 별도의 라인에 입력합니다.

트래픽을 라우팅하거나 다음 값을 지정할 수 있습니다.

- A – IPv4 주소
- AAAA - IPv6 주소
- CAA - 인증 기관 인증
- CNAME – 정식 이름
- MX - 메일 교환
- NAPTR - 이름 권한 포인터
- PTR - 포인터
- SPF - 발신자 정책 프레임워크
- SRV - 서비스 로케이터
- TXT - 텍스트

위의 값에 대한 자세한 내용은 값/트래픽 라우팅 대상에 일반적인 값을 참조하세요.

리전

이 레코드에 지정된 리소스가 상주하는 Amazon EC2 리전입니다. Route 53은 지정한 다른 값을 기반으로 하는 Amazon EC2 리전을 권장합니다. 이는 프라이빗 호스팅 영역에도 적용됩니다. 이 값을 변경하지 않는 것이 좋습니다.

다음 사항에 유의하세요.

- 각 Amazon EC2 리전에 대해 지연 시간 레코드 하나만을 생성할 수 있습니다.
- 모든 Amazon EC2 리전에 대해 지연 시간 레코드를 생성할 필요가 없습니다. Route 53은 지연 시간 레코드를 생성할 리전 중에서 지연 시간이 가장 좋은 리전을 선택합니다.
- 레코드 이름(Record name) 및 레코드 유형(Record type) 값이 지연 시간 레코드와 같은 비-지연 시간 레코드를 생성할 수 없습니다.
- cn-north-1 리전이 붙은 레코드를 생성할 경우 Route 53이 항상 지연 시간과 상관없이 이 레코드를 사용하여 중국 내부에서 보낸 쿼리에 응답합니다.

지연 시간 레코드 사용에 대한 자세한 내용은 지연 시간 기반 라우팅 단원을 참조하십시오.

상태 확인

Route 53가 지정된 엔드포인트 상태를 점검하고 엔드포인트가 정상할 때만 이 레코드를 사용하여 DNS 쿼리에 응답하길 원할 경우 상태 확인을 선택합니다.

Route 53는 레코드에 지정된 엔드포인트, 예를 들어 값(Value) 필드에서 IP 주소로 지정된 엔드포인트의 상태는 점검하지 않습니다. 레코드의 상태 확인을 선택하면 Route 53가 상태 확인에서 지정한 엔드포인트의 상태를 점검합니다. Route 53가 엔드포인트가 정상인지 여부를 결정하는 방법은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 섹션을 참조하세요.

상태 확인과 레코드를 연관시키는 것은 Route 53가 둘 이상의 레코드 사이에서 DNS 쿼리에 응답할 레코드를 선택할 때 그리고 Route 53가 상태 확인 상태를 선택의 기준으로 삼을 때만 유용합니다. 다음 구성에서만 상태 확인을 사용합니다.

- 이름, 유형 및 라우팅 정책(예: 장애 조치 또는 가중치 레코드)이 동일한 레코드 그룹의 모든 레코드 상태를 확인하고 모든 레코드에 대한 상태 확인 ID를 지정하는 경우. 레코드의 상태 확인에서 양호하지 않은 엔드포인트가 지정될 경우 Route 53는 해당 레코드 값을 사용하는 쿼리에 대한 응답을 중단합니다.
- 별칭 레코드 또는 장애 조치 별칭, 지리적 위치 별칭, 대기 시간 별칭, IP 기반 별칭 또는 가중치 기반 별칭 그룹에 속한 레코드에 대해 대상 상태 평가(Evaluate Target Health)에서 예(Yes)를 선택하는

경우. 별칭 레코드가 동일한 호스팅 영역의 별칭이 아닌 레코드를 참조하는 경우 참조된 레코드의 상태 확인도 지정해야 합니다. 상태 확인과 별칭 레코드를 연관시키고 대상 상태 평가에서 예를 선택하는 경우 둘 다 true로 평가되어야 합니다. 자세한 내용은 상태 확인을 별칭 레코드와 연결하면 어떻게 됩니까? 단원을 참조하십시오.

상태 확인에서 도메인 이름만으로 엔드포인트를 지정할 경우에는 각 엔드포인트마다 별도의 상태 확인을 생성하는 것이 좋습니다. 예를 들어, www.example.com의 콘텐츠를 제공하는 각 HTTP 서버마다 상태 확인을 생성합니다. 도메인 이름(Domain name)의 값은 레코드의 이름(example.com)이 아니라 서버의 도메인 이름(예: us-east-2-www.example.com)을 지정합니다.

> **Important**
>
> 이 구성에서 [Domain name]의 값이 레코드의 이름과 일치하는 상태 확인을 생성한 후 상태 확인을 이러한 레코드와 연결하는 경우 상태 확인 결과를 예측할 수 없습니다.

레코드 ID

지연 시간 레코드 그룹에 있는 이 레코드를 고유하게 식별하는 값을 선택합니다.

지연 시간 별칭 레코드에 특정한 값

지연 시간 별칭 레코드를 생성할 때 다음과 같은 값을 지정합니다.

자세한 내용은 별칭 또는 비 별칭 레코드 선택 단원을 참조하십시오.

주제

- 라우팅 정책
- 레코드 이름
- 레코드 유형
- 값/트래픽 라우팅 대상
- 리전
- 상태 확인
- 대상 상태 평가
- 레코드 ID

라우팅 정책

지연 시간(Latency)을 선택합니다.

레코드 이름

트래픽을 라우팅할 도메인 또는 하위 도메인의 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

> **Note**
>
> 호스팅 영역과 이름이 동일한 레코드를 생성할 경우 레코드 이름(Record name) 필드에 값(예: @ 기호)을 입력하지 마세요.

지연 시간 레코드 그룹의 모든 레코드에 대해 동일한 이름을 입력합니다.

버킷 이름에 대한 자세한 내용은 레코드 이름 섹션을 참조하십시오.

레코드 유형

DNS 레코드 유형입니다. 자세한 내용은 지원되는 DNS 레코드 유형 단원을 참조하십시오.

트래픽을 라우팅할 AWS 리소스를 기반으로 해당 값을 선택합니다.

API Gateway 사용자 지정 리전 API 또는 엣지 최적화 API

A - IPv4 주소(A - IPv4 address)를 선택합니다.

Amazon VPC 인터페이스 엔드포인트

A - IPv4 주소(A - IPv4 address)를 선택합니다.

CloudFront 배포

A - IPv4 주소(A - IPv4 address)를 선택합니다.

배포에 대해 IPv6가 활성화되어 있다면 두 개의 레코드를 생성합니다. 하나는 유형(Type) 값이 A - IPv4 주소(A - IPv4 address)이고 하나는 값이 AAAA - IPv6 주소(AAAA - IPv6 address)입니다.

App Runner 서비스

A - IPv4 주소(A - IPv4 address)를 선택합니다.

리전별 하위 도메인이 있는 Elastic Beanstalk 환경

A - IPv4 주소(A - IPv4 address)를 선택합니다.

ELB 로드 밸런서

A - IPv4 address(A - IPv4 주소) 또는 AAAA - IPv6 address(AAAA - IPv6 주소) 선택

Amazon S3 버킷

A - IPv4 주소(A - IPv4 address)를 선택합니다.

OpenSearch Service

A - IPv4 address(A - IPv4 주소) 또는 AAAA - IPv6 address(AAAA - IPv6 주소) 선택

호스팅 영역의 또 다른 레코드

별칭을 생성 중인 레코드 유형을 선택합니다. NS 및 SOA를 제외한 모든 유형이 지원됩니다.

> **Note**
>
> 호스팅 영역(zone apex라고도 함)과 이름이 같은 별칭 레코드를 생성한다면, 유형 값이 CNAME인 레코드로 트래픽을 라우팅할 수 없습니다. 이는 별칭 레코드가 트래픽이 라우팅되는 레코드와 동일한 형식이어야 하고, zone apex에 대한 CNAME 레코드 생성은 별칭 레코드에 대해서도 지원되지 않기 때문입니다.

지연 시간 레코드 그룹의 모든 레코드에 대해 동일 값을 선택합니다.

값/트래픽 라우팅 대상

목록에서 선택하거나 필드에 입력하는 값은 트래픽을 라우팅하는 AWS 리소스에 따라 달라집니다.

대상으로 지정할 수 있는 AWS 리소스에 대한 자세한 내용은 값/라우팅 트래픽에 대한 별칭 레코드의 공통 값을 참조하세요.

트래픽을 특정 AWS 리소스로 라우팅하도록 Route 53를 구성하는 방법에 대한 자세한 내용은 섹션을 참조하세요AWS 리소스로 인터넷 트래픽 라우팅.

리전

이 레코드에 지정된 리소스가 상주하는 Amazon EC2 리전입니다. Route 53은 지정한 다른 값을 기반으로 하는 Amazon EC2 리전을 권장합니다. 이는 프라이빗 호스팅 영역에도 적용됩니다. 이 값을 변경하지 않는 것이 좋습니다.

다음 사항에 유의하세요.

- 각 Amazon EC2 리전에 대해 지연 시간 레코드 하나만을 생성할 수 있습니다.
- 모든 Amazon EC2 리전에 대해 지연 시간 레코드를 생성할 필요가 없습니다. Route 53은 지연 시간 레코드를 생성할 리전 중에서 지연 시간이 가장 좋은 리전을 선택합니다.
- 레코드 이름(Record name) 및 레코드 유형(Record type) 값이 지연 시간 레코드와 같은 비-지연 시간 레코드를 생성할 수 없습니다.
- cn-north-1 리전이 붙은 레코드를 생성할 경우 Route 53이 항상 지연 시간과 상관없이 이 레코드를 사용하여 중국 내부에서 보낸 쿼리에 응답합니다.

지연 시간 레코드 사용에 대한 자세한 내용은 지연 시간 기반 라우팅 단원을 참조하십시오.

상태 확인

Route 53가 지정된 엔드포인트 상태를 점검하고 엔드포인트가 정상할 때만 이 레코드를 사용하여 DNS 쿼리에 응답하길 원할 경우 상태 확인을 선택합니다.

Route 53는 레코드에 지정된 엔드포인트, 예를 들어 값(Value) 필드에서 IP 주소로 지정된 엔드포인트의 상태는 점검하지 않습니다. 레코드의 상태 확인을 선택하면 Route 53가 상태 확인에서 지정한 엔드포인트의 상태를 점검합니다. Route 53가 엔드포인트가 정상인지 여부를 결정하는 방법은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 섹션을 참조하세요.

상태 확인과 레코드를 연관시키는 것은 Route 53가 둘 이상의 레코드 사이에서 DNS 쿼리에 응답할 레코드를 선택할 때 그리고 Route 53가 상태 확인 상태를 선택의 기준으로 삼을 때만 유용합니다. 다음 구성에서만 상태 확인을 사용합니다.

- 이름, 유형 및 라우팅 정책(예: 장애 조치 또는 가중치 레코드)이 동일한 레코드 그룹의 모든 레코드 상태를 확인하고 모든 레코드에 대한 상태 확인 ID를 지정하는 경우. 레코드의 상태 확인에서 양호하지 않은 엔드포인트가 지정될 경우 Route 53는 해당 레코드 값을 사용하는 쿼리에 대한 응답을 중단합니다.
- 별칭 레코드 또는 장애 조치 별칭, 지리적 위치 별칭, 대기 시간 별칭, IP 기반 별칭 또는 가중치 기반 별칭 그룹에 속한 레코드에 대해 대상 상태 평가(Evaluate Target Health)에서 예(Yes)를 선택하는 경우. 별칭 레코드가 동일한 호스팅 영역의 별칭이 아닌 레코드를 참조하는 경우 참조된 레코드의 상태 확인도 지정해야 합니다. 상태 확인과 별칭 레코드를 연관시키고 대상 상태 평가에서 예를 선택하는 경우 둘 다 true로 평가되어야 합니다. 자세한 내용은 상태 확인을 별칭 레코드와 연결하면 어떻게 됩니까? 단원을 참조하십시오.

상태 확인에서 도메인 이름만으로 엔드포인트를 지정할 경우에는 각 엔드포인트마다 별도의 상태 확인을 생성하는 것이 좋습니다. 예를 들어, www.example.com의 콘텐츠를 제공하는 각 HTTP 서버마다 상태 확인을 생성합니다. 도메인 이름(Domain name)의 값은 레코드의 이름(example.com)이 아니라 서버의 도메인 이름(예: us-east-2-www.example.com)을 지정합니다.

> **Important**
>
> 이 구성에서 도메인 이름의 값이 레코드의 이름과 일치하는 상태 확인을 생성한 후 상태 확인을 이러한 레코드와 연결하는 경우 상태 확인 결과를 예측할 수 없습니다.

대상 상태 평가

엔드포인트에서 지정된 리소스의 상태를 확인하여 Route 53가 레코드를 사용해 DNS 쿼리에 응답할지 여부를 결정하게 하려는 경우 예(Yes)를 선택합니다.

다음 사항에 유의하세요.

API Gateway 사용자 지정 리전 API와 엣지 최적화 API

엔드포인트가 API Gateway 사용자 지정 리전 API 또는 엣지 최적화 API인 경우 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정하기 위한 특별한 요구 사항은 없습니다.

CloudFront 배포

엔드포인트가 CloudFront 배포인 경우 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정할 수 없습니다.

리전별 하위 도메인이 있는 Elastic Beanstalk 환경

엔드포인트(Endpoint)에 Elastic Beanstalk 환경을 지정하고 환경에 ELB 로드 밸런서가 포함된 경우, Elastic Load Balancing은 로드 밸런서에 등록된 정상 Amazon EC2 인스턴스로만 쿼리를 라우팅합니다. (하나의 환경에 한 개 이상의 Amazon EC2 인스턴스가 포함된 경우 ELB 로드 밸런서가 자동으로 포함됩니다.) 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정했는데 정상인 Amazon EC2 인스턴스가 없거나 로드 밸런서 자체가 비정상인 경우 Route 53는 양호한 다른 리소스로 쿼리를 라우팅합니다.

환경에 하나의 Amazon EC2 인스턴스가 포함된 경우에는 특별한 요구 사항이 없습니다.

ELB 로드 밸런서

상태 확인 동작은 로드 밸런서의 유형에 따라 달랍니다.

- Classic Load Balancer: 엔드포인트(Endpoint)에 ELB Classic Load Balancer를 지정한 경우, Elastic Load Balancing은 로드 밸런서에 등록된 정상 Amazon EC2 인스턴스로만 쿼리를 라우팅합니다. 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정하고 EC2 인스턴스가 정상 상태가 아니거나 로드 밸런서 자체가 비정상인 경우 Route 53는 쿼리를 다른 리소스로 라우팅합니다.
- Application Load Balancer 및 Network Load Balancer - ELB Application Load Balancer 또는 Network Load Balancer를 지정하고 대상 상태 평가(Evaluate Target Health)를 예(Yes)로 설정한 경우 Route 53는 로드 밸런서와 연결된 대상 그룹의 상태에 따라 쿼리를 로드 밸런서로 라우팅합니다.
  - Application 또는 Network Load Balancer가 정상 상태로 간주되려면 대상을 포함하는 모든 대상 그룹에 정상 상태 대상이 하나 이상 포함되어야 합니다. 대상 그룹에 정상이 아닌 대상만 포함되는 경우 로드 밸런서는 정상이 아닌 상태로 간주되고 Route 53는 쿼리를 다른 리소스로 라우팅합니다.
  - 등록된 대상이 없는 대상 그룹은 정상이 아닌 상태로 간주됩니다.

> **Note**
>
> 로드 밸런서를 생성할 때 Elastic Load Balancing 상태 확인에 대한 설정을 구성하게 되는데, 이러한 확인은 Route 53 상태 확인은 아니지만 비슷한 기능을 수행합니다. ELB 로드 밸런서에 등록하는 EC2 인스턴스에 대해 Route 53 상태 확인을 생성하지 마십시오.

S3 버킷

엔드포인트가 S3 버킷인 경우 대상 상태 평가(Evaluate Target Health)를 예(Yes)로 설정하는 데 필요한 특정 요건은 없습니다.

Amazon VPC 인터페이스 엔드포인트

엔드포인트가 Amazon VPC 인터페이스 엔드포인트인 경우 대상 상태 평가(Evaluate Target Health)를 예(Yes)로 설정하는 데 필요한 특별한 요구 사항이 없습니다.

동일 호스팅 영역 내 다른 레코드

엔드포인트에서 지정하는 AWS 리소스가 레코드 또는 레코드 그룹(예: 가중치 기반 레코드 그룹)이지만 다른 별칭 레코드가 아닌 경우 상태 확인을 엔드포인트의 모든 레코드와 연결하는 것이 좋습니다. 자세한 내용은 상태 확인을 생략하면 어떻게 됩니까? 단원을 참조하십시오.

레코드 ID

지연 시간 레코드 그룹에 있는 이 레코드를 고유하게 식별하는 값을 선택합니다.

IP 기반 레코드에 특정한 값

IP 기반 레코드를 생성할 때 다음과 같은 값을 지정합니다.

> **Note**
>
> 프라이빗 호스팅 영역에서 IP 기반 레코드를 생성할 수는 있지만 지원되지 않습니다.

주제

- 라우팅 정책
- 레코드 이름
- 레코드 유형
- TTL(초)
- 값/트래픽 라우팅 대상
- 위치
- 상태 확인
- 레코드 ID

라우팅 정책

IP 기반(IP-based)을 선택합니다.

레코드 이름

트래픽을 라우팅할 도메인 또는 하위 도메인의 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

> **Note**
>
> 호스팅 영역과 이름이 동일한 레코드를 생성할 경우 레코드 이름(Record name) 필드에 값(예: @ 기호)을 입력하지 마세요.

IP 기반 레코드 그룹의 모든 레코드에 대해 동일한 이름을 입력합니다.

CNAME 레코드

레코드 유형(Record type) 값이 CNAME인 레코드를 생성하는 경우 레코드의 이름은 호스팅 영역의 이름과 같을 수 없습니다.

특수 문자

a-z, 0-9, -(하이픈) 이외의 문자를 지정하는 방법과 국제 도메인 이름을 지정하는 방법은 다음(DNS 도메인 이름 형식)을 참조하십시오.

와일드카드 문자

이름에 별표(*) 문자를 사용할 수 있습니다. DNS는 이름에 표시되는 위치에 따라 * 문자를 와일드카드 또는 * 문자(ASCII 42)로 처리합니다. 자세한 내용은 호스팅 영역 및 레코드의 이름에 별표(*) 사용 단원을 참조하십시오.

레코드 유형

DNS 레코드 유형입니다. 자세한 내용은 지원되는 DNS 레코드 유형 단원을 참조하십시오.

Route 53가 DNS 쿼리에 응답하는 방식에 따라 유형(Type)에 대한 값을 선택합니다.

IP 기반 레코드 그룹의 모든 레코드에 대해 동일한 값을 선택합니다.

TTL(초)

DNS recursive resolver가 이 레코드에 관한 정보를 캐싱할 시간(초)입니다. 더 긴 값(예: 172800초 또는 2일)을 지정한 경우, 이 레코드의 최신 정보를 얻으려면 DNS recursive resolver의 Route 53에 대한 호출 수를 줄여야 합니다. 이렇게 하면 지연 시간을 줄이고 Route 53 서비스 비용을 줄이는 효과가 있습니다. 자세한 내용은 Amazon Route 53가 도메인의 트래픽을 라우팅하는 방법 단원을 참조하십시오.

그러나 TTL에 더 긴 값을 지정하면 recursive resolver가 Route 53에 최신 정보를 요청하기 전에 기간이 더 긴 캐시 값을 사용하므로 레코드(예: 새 IP 주소) 변경이 적용되는 데 걸리는 시간이 길어집니다. 이미 사용 중인 도메인이나 하위 도메인의 설정을 변경하는 경우 처음에는 더 짧은 값(예: 300초)을 지정하고 새 설정이 올바른지 확인한 후 값을 늘리는 것이 좋습니다.

이 레코드를 상태 점검과 연관시킬 경우에는 클라이언트가 상태 변경에 빠르게 응답하도록 TTL을 60초 이하로 지정하는 것이 좋습니다.

값/트래픽 라우팅 대상

IP 주소 또는 레코드 유형에 따라 다른 값(IP address or another value depending on the record type)을 선택합니다. 레코드 유형(Record type) 값에 해당하는 값을 입력합니다. CNAME을 제외한 모든 유형은 둘 이상의 값을 입력할 수 있습니다. 각 값을 별도의 라인에 입력합니다.

트래픽을 라우팅하거나 다음 값을 지정할 수 있습니다.

- A – IPv4 주소
- AAAA - IPv6 주소
- CAA - 인증 기관 인증
- CNAME – 정식 이름
- MX - 메일 교환
- NAPTR - 이름 권한 포인터
- PTR - 포인터
- SPF - 발신자 정책 프레임워크
- SRV - 서비스 로케이터
- TXT - 텍스트

위의 값에 대한 자세한 내용은 값/트래픽 라우팅 대상 값/트래픽 라우팅 대상에 일반적인 값을 참조하세요.

위치

이 레코드에서 지정된 리소스가 CIDR 위치 내 CIDR 블록 값으로 지정된 CIDR 위치의 이름입니다.

IP 기반 레코드 사용에 대한 자세한 내용은 IP 기반 라우팅을 참조하세요.

상태 확인

Route 53가 지정된 엔드포인트 상태를 점검하고 엔드포인트가 정상할 때만 이 레코드를 사용하여 DNS 쿼리에 응답하길 원할 경우 상태 확인을 선택합니다.

Route 53는 레코드에 지정된 엔드포인트, 예를 들어 값(Value) 필드에서 IP 주소로 지정된 엔드포인트의 상태는 점검하지 않습니다. 레코드의 상태 확인을 선택하면 Route 53가 상태 확인에서 지정한 엔드포인트의 상태를 점검합니다. Route 53가 엔드포인트가 정상인지 여부를 결정하는 방법은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 섹션을 참조하세요.

상태 확인과 레코드를 연관시키는 것은 Route 53가 둘 이상의 레코드 사이에서 DNS 쿼리에 응답할 레코드를 선택할 때 그리고 Route 53가 상태 확인 상태를 선택의 기준으로 삼을 때만 유용합니다. 다음 구성에서만 상태 확인을 사용합니다.

- 이름, 유형 및 라우팅 정책(예: 장애 조치 또는 가중치 레코드)이 동일한 레코드 그룹의 모든 레코드 상태를 확인하고 모든 레코드에 대한 상태 확인 ID를 지정하는 경우. 레코드의 상태 확인에서 양호하지 않은 엔드포인트가 지정될 경우 Route 53는 해당 레코드 값을 사용하는 쿼리에 대한 응답을 중단합니다.
- 별칭 레코드 또는 장애 조치 별칭, 지리적 위치 별칭, IP 기반 별칭, 대기 시간 별칭 또는 가중치 기반 별칭 그룹에 속한 레코드에 대해 대상 상태 평가(Evaluate Target Health)에서 예(Yes)를 선택하는 경우. 별칭 레코드가 동일한 호스팅 영역의 별칭이 아닌 레코드를 참조하는 경우 참조된 레코드의 상태 확인도 지정해야 합니다. 상태 확인과 별칭 레코드를 연관시키고 대상 상태 평가에서 예를 선택하는 경우 둘 다 true로 평가되어야 합니다. 자세한 내용은 상태 확인을 별칭 레코드와 연결하면 어떻게 됩니까? 단원을 참조하십시오.

상태 확인에서 도메인 이름만으로 엔드포인트를 지정할 경우에는 각 엔드포인트마다 별도의 상태 확인을 생성하는 것이 좋습니다. 예를 들어, www.example.com의 콘텐츠를 제공하는 각 HTTP 서버마다 상태 확인을 생성합니다. 도메인 이름(Domain name)의 값은 레코드의 이름(example.com)이 아니라 서버의 도메인 이름(예: us-east-2-www.example.com)을 지정합니다.

> **Important**
>
> 이 구성에서 [Domain name]의 값이 레코드의 이름과 일치하는 상태 확인을 생성한 후 상태 확인을 이러한 레코드와 연결하는 경우 상태 확인 결과를 예측할 수 없습니다.

레코드 ID

IP 기반 레코드 그룹에 있는 이 레코드를 고유하게 식별하는 값을 입력합니다.

IP 기반 별칭 레코드에 특정한 값

IP 기반 별칭 레코드를 생성할 때 다음과 같은 값을 지정합니다.

> **Note**
>
> 프라이빗 호스팅 영역에서 IP 기반 별칭 레코드를 생성할 수는 있지만 지원되지 않습니다.

자세한 내용은 별칭 또는 비 별칭 레코드 선택 단원을 참조하십시오.

주제

- 라우팅 정책
- 레코드 이름
- 레코드 유형
- 값/트래픽 라우팅 대상
- 위치
- 상태 확인
- 대상 상태 평가
- 레코드 ID

라우팅 정책

IP 기반(IP-based)을 선택합니다.

> **Note**
>
> 프라이빗 호스팅 영역에서 IP 기반 별칭 레코드를 생성할 수는 있지만 지원되지 않습니다.

레코드 이름

트래픽을 라우팅할 도메인 또는 하위 도메인의 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

> **Note**
>
> 호스팅 영역과 이름이 동일한 레코드를 생성할 경우 레코드 이름(Record name) 필드에 값(예: @ 기호)을 입력하지 마세요.

IP 기반 레코드 그룹의 모든 레코드에 대해 동일한 이름을 입력합니다.

CNAME 레코드

레코드 유형(Record type) 값이 CNAME인 레코드를 생성하는 경우 레코드의 이름은 호스팅 영역의 이름과 같을 수 없습니다.

CloudFront 배포 및 Amazon S3 버킷에 대한 별칭

지정하는 값은 트래픽을 라우팅하는 AWS 리소스에 따라 부분적으로 달라집니다.

- CloudFront 배포(CloudFront distribution) – 배포에 레코드 이름과 일치하는 대체 도메인 이름이 포함되어야 합니다. 예를 들어, 레코드 이름이 acme.example.com인 경우 CloudFront 배포에 acme.example.com이 대체 도메인 이름 중 하나로 포함되어야 합니다. 자세한 내용은 Amazon CloudFront 개발자 안내서에서 대체 도메인 이름(CNAME) 사용을 참조하세요.
- Amazon S3 버킷 - 레코드 이름은 Amazon S3 버킷 이름과 일치해야 합니다. 예를 들어, 버킷의 이름이 acme.example.com이면 이 레코드의 이름도 acme.example.com이어야 합니다.

  그리고 웹사이트 호스팅용 버킷을 구성해야 합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 웹 사이트 호스팅에 대한 버킷 구성을 참조하십시오.

특수 문자

a-z, 0-9, -(하이픈) 이외의 문자를 지정하는 방법과 국제 도메인 이름을 지정하는 방법은 다음(DNS 도메인 이름 형식)을 참조하십시오.

와일드카드 문자

이름에 별표(*) 문자를 사용할 수 있습니다. DNS는 이름에 표시되는 위치에 따라 * 문자를 와일드카드 또는 * 문자(ASCII 42)로 처리합니다. 자세한 내용은 호스팅 영역 및 레코드의 이름에 별표(*) 사용 단원을 참조하십시오.

레코드 유형

DNS 레코드 유형입니다. 자세한 내용은 지원되는 DNS 레코드 유형 단원을 참조하십시오.

트래픽을 라우팅할 AWS 리소스를 기반으로 해당 값을 선택합니다. IP 기반 레코드 그룹의 모든 레코드에 대해 동일한 값을 선택합니다.

API Gateway 사용자 지정 리전 API 또는 엣지 최적화 API

A - IPv4 주소(A - IPv4 address)를 선택합니다.

Amazon VPC 인터페이스 엔드포인트

A - IPv4 주소(A - IPv4 address)를 선택합니다.

CloudFront 배포

A - IPv4 주소(A - IPv4 address)를 선택합니다.

배포에 대해 IPv6가 활성화되어 있다면 두 개의 레코드를 생성합니다. 하나는 유형(Type) 값이 A - IPv4 주소(A - IPv4 address)이고 하나는 값이 AAAA - IPv6 주소(AAAA - IPv6 address)입니다.

App Runner 서비스

A - IPv4 주소(A - IPv4 address)를 선택합니다.

리전별 하위 도메인이 있는 Elastic Beanstalk 환경

A - IPv4 주소(A - IPv4 address)를 선택합니다.

ELB 로드 밸런서

A - IPv4 address(A - IPv4 주소) 또는 AAAA - IPv6 address(AAAA - IPv6 주소) 선택

Amazon S3 버킷

A - IPv4 주소(A - IPv4 address)를 선택합니다.

OpenSearch Service

A - IPv4 address(A - IPv4 주소) 또는 AAAA - IPv6 address(AAAA - IPv6 주소) 선택

호스팅 영역의 또 다른 레코드

별칭을 생성 중인 레코드 유형을 선택합니다. NS 및 SOA를 제외한 모든 유형이 지원됩니다.

> **Note**
>
> 호스팅 영역(zone apex라고도 함)과 이름이 같은 별칭 레코드를 생성한다면, 유형 값이 CNAME인 레코드로 트래픽을 라우팅할 수 없습니다. 이는 별칭 레코드가 트래픽이 라우팅되는 레코드와 동일한 형식이어야 하고, zone apex에 대한 CNAME 레코드 생성은 별칭 레코드에 대해서도 지원되지 않기 때문입니다.

값/트래픽 라우팅 대상

목록에서 선택하거나 필드에 입력하는 값은 트래픽을 라우팅하는 AWS 리소스에 따라 달라집니다.

대상으로 지정할 수 있는 AWS 리소스에 대한 자세한 내용은 값/라우팅 트래픽에 대한 별칭 레코드의 공통 값을 참조하세요.

트래픽을 특정 AWS 리소스로 라우팅하도록 Route 53를 구성하는 방법에 대한 자세한 내용은 섹션을 참조하세요AWS 리소스로 인터넷 트래픽 라우팅.

위치

쿼리를 보낸 위치를 기반으로 하는 DNS 쿼리에 응답하도록 Route 53을 구성할 때는 Route 53이 이 레코드 설정으로 응답하길 원하는 CIDR 위치를 선택합니다.

> **Important**
>
> 위치(Location)에 대한 기본(Default) 값을 갖는 하나의 IP 기반 레코드를 생성하는 것이 좋습니다. 그러면 레코드를 생성하지 않은 위치와 Route 53이 위치를 식별하지 못하는 IP 주소도 포함됩니다.

레코드 이름(Record name) 및 레코드 유형(Record type) 값이 IP 기반 레코드와 같은 IP 기반이 아닌 레코드를 생성할 수 없습니다.

자세한 내용은 IP 기반 라우팅 단원을 참조하십시오.

상태 확인

Route 53가 지정된 엔드포인트 상태를 점검하고 엔드포인트가 정상할 때만 이 레코드를 사용하여 DNS 쿼리에 응답하길 원할 경우 상태 확인을 선택합니다.

Route 53는 레코드에 지정된 엔드포인트, 예를 들어 값(Value) 필드에서 IP 주소로 지정된 엔드포인트의 상태는 점검하지 않습니다. 레코드의 상태 확인을 선택하면 Route 53가 상태 확인에서 지정한 엔드포인트의 상태를 점검합니다. Route 53가 엔드포인트가 정상인지 여부를 결정하는 방법은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 섹션을 참조하세요.

상태 확인과 레코드를 연관시키는 것은 Route 53가 둘 이상의 레코드 사이에서 DNS 쿼리에 응답할 레코드를 선택할 때 그리고 Route 53가 상태 확인 상태를 선택의 기준으로 삼을 때만 유용합니다. 다음 구성에서만 상태 확인을 사용합니다.

- 이름, 유형 및 라우팅 정책(예: 장애 조치 또는 가중치 레코드)이 동일한 레코드 그룹의 모든 레코드 상태를 확인하고 모든 레코드에 대한 상태 확인 ID를 지정하는 경우. 레코드의 상태 확인에서 양호하지 않은 엔드포인트가 지정될 경우 Route 53는 해당 레코드 값을 사용하는 쿼리에 대한 응답을 중단합니다.
- 별칭 레코드 또는 장애 조치 별칭, 지리적 위치 별칭, IP 기반 라우팅 별칭, 대기 시간 별칭 또는 가중치 기반 별칭 그룹에 속한 레코드에 대해 대상 상태 평가(Evaluate Target Health)에서 예(Yes)를 선택하는 경우. 별칭 레코드가 동일한 호스팅 영역의 별칭이 아닌 레코드를 참조하는 경우 참조된 레코드의 상태 확인도 지정해야 합니다. 상태 확인과 별칭 레코드를 연관시키고 대상 상태 평가에서 예를 선택하는 경우 둘 다 true로 평가되어야 합니다. 자세한 내용은 상태 확인을 별칭 레코드와 연결하면 어떻게 됩니까? 단원을 참조하십시오.

상태 확인에서 도메인 이름만으로 엔드포인트를 지정할 경우에는 각 엔드포인트마다 별도의 상태 확인을 생성하는 것이 좋습니다. 예를 들어, www.example.com의 콘텐츠를 제공하는 각 HTTP 서버마다 상태 확인을 생성합니다. 도메인 이름(Domain name)의 값은 레코드의 이름(example.com)이 아니라 서버의 도메인 이름(예: us-east-2-www.example.com)을 지정합니다.

> **Important**
>
> 이 구성에서 [Domain name]의 값이 레코드의 이름과 일치하는 상태 확인을 생성한 후 상태 확인을 이러한 레코드와 연결하는 경우 상태 확인 결과를 예측할 수 없습니다.

IP 기반 별칭 레코드에서 엔드포인트가 비정상적인 경우 Route 53는 더 크고 연관된 위치 내에서 레코드를 찾습니다. 예를 들어, 미국 내 주, 미국, 북미 및 전체 위치에 대한 레코드가 있다고 가정합니다(위치가 기본값임). 주 레코드의 엔드포인트가 양호하지 않을 경우 Route 53은 미국, 북미 및 전체 위치 순으로 엔드포인트가 양호한 레코드를 찾을 때까지 레코드를 확인합니다. 모든 지리적 위치에 대한 레코드를 포함하여 모든 적용 가능한 레코드가 비정상적인 경우 Route 53은 가장 작은 지리적 리전에 대한 레코드 값을 사용하여 DNS 쿼리에 응답합니다.

대상 상태 평가

엔드포인트에서 지정된 리소스의 상태를 확인하여 Route 53가 레코드를 사용해 DNS 쿼리에 응답할지 여부를 결정하게 하려는 경우 예(Yes)를 선택합니다.

다음 사항에 유의하세요.

API Gateway 사용자 지정 리전 API와 엣지 최적화 API

엔드포인트가 API Gateway 사용자 지정 리전 API 또는 엣지 최적화 API인 경우 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정하기 위한 특별한 요구 사항은 없습니다.

CloudFront 배포

엔드포인트가 CloudFront 배포인 경우 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정할 수 없습니다.

리전별 하위 도메인이 있는 Elastic Beanstalk 환경

엔드포인트(Endpoint)에 Elastic Beanstalk 환경을 지정하고 환경에 ELB 로드 밸런서가 포함된 경우, Elastic Load Balancing은 로드 밸런서에 등록된 정상 Amazon EC2 인스턴스로만 쿼리를 라우팅합니다. (하나의 환경에 한 개 이상의 Amazon EC2 인스턴스가 포함된 경우 ELB 로드 밸런서가 자동으로 포함됩니다.) 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정했는데 정상인 Amazon EC2 인스턴스가 없거나 로드 밸런서 자체가 비정상인 경우 Route 53는 양호한 다른 리소스로 쿼리를 라우팅합니다.

환경에 하나의 Amazon EC2 인스턴스가 포함된 경우에는 특별한 요구 사항이 없습니다.

ELB 로드 밸런서

상태 확인 동작은 로드 밸런서의 유형에 따라 달랍니다.

- Classic Load Balancer: 엔드포인트(Endpoint)에 ELB Classic Load Balancer를 지정한 경우, Elastic Load Balancing은 로드 밸런서에 등록된 정상 Amazon EC2 인스턴스로만 쿼리를 라우팅합니다. 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정하고 EC2 인스턴스가 정상 상태가 아니거나 로드 밸런서 자체가 비정상인 경우 Route 53는 쿼리를 다른 리소스로 라우팅합니다.
- Application Load Balancer 및 Network Load Balancer - ELB Application Load Balancer 또는 Network Load Balancer를 지정하고 대상 상태 평가(Evaluate Target Health)를 예(Yes)로 설정한 경우 Route 53는 로드 밸런서와 연결된 대상 그룹의 상태에 따라 쿼리를 로드 밸런서로 라우팅합니다.
  - Application 또는 Network Load Balancer가 정상 상태로 간주되려면 대상을 포함하는 모든 대상 그룹에 정상 상태 대상이 하나 이상 포함되어야 합니다. 대상 그룹에 정상이 아닌 대상만 포함되는 경우 로드 밸런서는 정상이 아닌 상태로 간주되고 Route 53는 쿼리를 다른 리소스로 라우팅합니다.
  - 등록된 대상이 없는 대상 그룹은 정상이 아닌 상태로 간주됩니다.

> **Note**
>
> 로드 밸런서를 생성할 때 Elastic Load Balancing 상태 확인에 대한 설정을 구성하게 되는데, 이러한 확인은 Route 53 상태 확인은 아니지만 비슷한 기능을 수행합니다. ELB 로드 밸런서에 등록하는 EC2 인스턴스에 대해 Route 53 상태 확인을 생성하지 마십시오.

S3 버킷

엔드포인트가 S3 버킷인 경우 대상 상태 평가(Evaluate Target Health)를 예(Yes)로 설정하는 데 필요한 특정 요건은 없습니다.

Amazon VPC 인터페이스 엔드포인트

엔드포인트가 Amazon VPC 인터페이스 엔드포인트인 경우 대상 상태 평가(Evaluate Target Health)를 예(Yes)로 설정하는 데 필요한 특별한 요구 사항이 없습니다.

동일 호스팅 영역 내 다른 레코드

엔드포인트에서 지정하는 AWS 리소스가 레코드 또는 레코드 그룹(예: 가중치 기반 레코드 그룹)이지만 다른 별칭 레코드가 아닌 경우 상태 확인을 엔드포인트의 모든 레코드와 연결하는 것이 좋습니다. 자세한 내용은 상태 확인을 생략하면 어떻게 됩니까? 단원을 참조하십시오.

레코드 ID

IP 기반 레코드 그룹에 있는 이 레코드를 고유하게 식별하는 값을 입력합니다.

다중값 응답 레코드에 특정한 값

다중값 응답 레코드를 생성할 때, 다음과 같은 값을 지정합니다.

> **Note**
>
> 다중값 응답 별칭 레코드 생성은 지원되지 않습니다.

주제

- 라우팅 정책
- 레코드 이름
- 레코드 유형
- TTL(초)
- 값/트래픽 라우팅 대상
- 상태 확인
- 레코드 ID

라우팅 정책

다중값 응답(Multivalue answer)을 선택합니다.

레코드 이름

트래픽을 라우팅할 도메인 또는 하위 도메인의 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

> **Note**
>
> 호스팅 영역과 이름이 동일한 레코드를 생성할 경우 레코드 이름(Record name) 필드에 값(예: @ 기호)을 입력하지 마세요.

다중 값 레코드 그룹의 모든 레코드에 대해 동일한 이름을 입력합니다.

레코드 이름에 대한 자세한 내용은 레코드 이름 섹션을 참조하십시오.

레코드 유형

DNS 레코드 유형입니다. 자세한 내용은 지원되는 DNS 레코드 유형 단원을 참조하십시오.

NS 또는 CNAME을 제외한 값을 선택합니다.

다중값 응답 레코드 그룹의 모든 레코드에 대해 동일 값을 선택합니다.

TTL(초)

DNS recursive resolver가 이 레코드에 관한 정보를 캐싱할 시간(초)입니다. 더 긴 값(예: 172800초 또는 2일)을 지정한 경우, 이 레코드의 최신 정보를 얻으려면 DNS recursive resolver의 Route 53에 대한 호출 수를 줄여야 합니다. 이렇게 하면 지연 시간을 줄이고 Route 53 서비스 비용을 줄이는 효과가 있습니다. 자세한 내용은 Amazon Route 53가 도메인의 트래픽을 라우팅하는 방법 단원을 참조하십시오.

그러나 TTL에 더 긴 값을 지정하면 recursive resolver가 Route 53에 최신 정보를 요청하기 전에 기간이 더 긴 캐시 값을 사용하므로 레코드(예: 새 IP 주소) 변경이 적용되는 데 걸리는 시간이 길어집니다. 이미 사용 중인 도메인이나 하위 도메인의 설정을 변경하는 경우 처음에는 더 짧은 값(예: 300초)을 지정하고 새 설정이 올바른지 확인한 후 값을 늘리는 것이 좋습니다.

이 레코드를 상태 점검과 연관시킬 경우에는 클라이언트가 상태 변경에 빠르게 응답하도록 TTL을 60초 이하로 지정하는 것이 좋습니다.

> **Note**
>
> 이름 및 유형이 동일한 두 개 이상의 다중값 응답 레코드를 생성하며 콘솔을 사용하고 TTL에 대해 다른 값을 지정하는 경우, Route 53은 모든 레코드의 TTL을 지정한 마지막 값으로 변경합니다.

값/트래픽 라우팅 대상

IP 주소 또는 레코드 유형에 따라 다른 값(IP address or another value depending on the record type)을 선택합니다. 레코드 유형(Record type) 값에 해당하는 값을 입력합니다. 2개 이상의 값을 입력하는 경우 각 값을 별도의 행에 입력합니다.

트래픽을 라우팅하거나 다음 값을 지정할 수 있습니다.

- A – IPv4 주소
- AAAA - IPv6 주소
- CAA - 인증 기관 인증
- MX - 메일 교환

- NAPTR - 이름 권한 포인터
- PTR - 포인터
- SPF - 발신자 정책 프레임워크
- SRV - 서비스 로케이터
- TXT - 텍스트

위의 값에 대한 자세한 내용은 값/트래픽 라우팅 대상에 일반적인 값을 참조하세요.

상태 확인

Route 53가 지정된 엔드포인트 상태를 점검하고 엔드포인트가 정상할 때만 이 레코드를 사용하여 DNS 쿼리에 응답하길 원할 경우 상태 확인을 선택합니다.

Route 53는 레코드에 지정된 엔드포인트, 예를 들어 값(Value) 필드에서 IP 주소로 지정된 엔드포인트의 상태는 점검하지 않습니다. 레코드의 상태 확인을 선택하면 Route 53가 상태 확인에서 지정한 엔드포인트의 상태를 점검합니다. Route 53가 엔드포인트가 정상인지 여부를 결정하는 방법은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 섹션을 참조하세요.

상태 확인과 레코드를 연관시키는 것은 Route 53가 둘 이상의 레코드 사이에서 DNS 쿼리에 응답할 레코드를 선택할 때 그리고 Route 53가 상태 확인 상태를 선택의 기준으로 삼을 때만 유용합니다. 다음 구성에서만 상태 확인을 사용합니다.

- 이름, 유형 및 라우팅 정책(예: 장애 조치 또는 가중치 레코드)이 동일한 레코드 그룹의 모든 레코드 상태를 확인하고 모든 레코드에 대한 상태 확인 ID를 지정하는 경우. 레코드의 상태 확인에서 양호하지 않은 엔드포인트가 지정될 경우 Route 53은 해당 레코드 값을 사용하는 쿼리에 대한 응답을 중단합니다.
- 별칭 레코드 또는 장애 조치 별칭, 지리적 위치 별칭, 대기 시간 별칭 또는 가중치 기반 별칭의 그룹 레코드에 대한 대상 상태 평가(Evaluate Target Health)에 예(Yes)를 선택합니다. 별칭 레코드가 동일한 호스팅 영역의 별칭이 아닌 레코드를 참조하는 경우 참조된 레코드의 상태 확인도 지정해야 합니다. 상태 확인과 별칭 레코드를 연관시키고 대상 상태 평가에서 예를 선택하는 경우 둘 다 true로 평가되어야 합니다. 자세한 내용은 상태 확인을 별칭 레코드와 연결하면 어떻게 됩니까? 단원을 참조하십시오.

상태 확인에서 도메인 이름만으로 엔드포인트를 지정할 경우에는 각 엔드포인트마다 별도의 상태 확인을 생성하는 것이 좋습니다. 예를 들어, www.example.com의 콘텐츠를 제공하는 각 HTTP 서버마다 상태 확인을 생성합니다. 도메인 이름(Domain name)의 값은 레코드의 이름(example.com)이 아니라 서버의 도메인 이름(예: us-east-2-www.example.com)을 지정합니다.

> **Important**
>
> 이 구성에서 [Domain name]의 값이 레코드의 이름과 일치하는 상태 확인을 생성한 후 상태 확인을 이러한 레코드와 연결하는 경우 상태 확인 결과를 예측할 수 없습니다.

레코드 ID

다중값 응답 레코드 그룹에 있는 이 레코드를 고유하게 식별하는 값을 선택합니다.

가중치 기반 레코드에 특정한 값

가중치 기반 레코드를 생성할 때 다음과 같은 값을 지정합니다.

주제

- 라우팅 정책
- 레코드 이름
- 레코드 유형
- TTL(초)
- 값/트래픽 라우팅 대상
- 가중치
- 상태 확인
- 레코드 ID

라우팅 정책

Weighted(가중치)를 선택합니다.

레코드 이름

트래픽을 라우팅할 도메인 또는 하위 도메인의 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

> **Note**
>
> 호스팅 영역과 이름이 동일한 레코드를 생성할 경우 레코드 이름(Record name) 필드에 값(예: @ 기호)을 입력하지 마세요.

가중 레코드 그룹의 모든 레코드에 대해 동일한 이름을 입력합니다.

레코드 이름에 대한 자세한 내용은 레코드 이름 섹션을 참조하십시오.

레코드 유형

DNS 레코드 유형입니다. 자세한 내용은 지원되는 DNS 레코드 유형 단원을 참조하십시오.

가중 레코드 그룹의 모든 레코드에 대해 동일 값을 선택합니다.

TTL(초)

DNS recursive resolver가 이 레코드에 관한 정보를 캐싱할 시간(초)입니다. 더 긴 값(예: 172800초 또는 2일)을 지정한 경우, 이 레코드의 최신 정보를 얻으려면 DNS recursive resolver의 Route 53에 대한 호출 수를 줄여야 합니다. 이렇게 하면 지연 시간을 줄이고 Route 53 서비스 비용을 줄이는 효과가 있습니다. 자세한 내용은 Amazon Route 53가 도메인의 트래픽을 라우팅하는 방법 단원을 참조하십시오.

그러나 TTL에 더 긴 값을 지정하면 recursive resolver가 Route 53에 최신 정보를 요청하기 전에 기간이 더 긴 캐시 값을 사용하므로 레코드(예: 새 IP 주소) 변경이 적용되는 데 걸리는 시간이 길어집니다. 이미 사용 중인 도메인이나 하위 도메인의 설정을 변경하는 경우 처음에는 더 짧은 값(예: 300초)을 지정하고 새 설정이 올바른지 확인한 후 값을 늘리는 것이 좋습니다.

이 레코드를 상태 점검과 연관시킬 경우에는 클라이언트가 상태 변경에 빠르게 응답하도록 TTL을 60초 이하로 지정하는 것이 좋습니다.

이 가중 레코드 그룹의 모든 레코드에 동일한 TTL 값을 지정해야 합니다.

> **Note**
>
> 이름 및 유형이 동일한 두 개 이상의 가중 레코드를 생성하며 TTL에 대해 다른 값을 지정하는 경우 Route 53은 모든 레코드의 TTL을 지정한 마지막 값으로 변경합니다.

가중 레코드 그룹에 ELB 로드 밸런서로 트래픽을 라우팅하는 가중 별칭 레코드가 하나 이상 포함된 경우에는 이름과 유형이 동일한 모든 비-별칭 가중 레코드에 대해 TTL을 60초로 지정하는 것이 좋습니다. 60초(로드 밸런서의 TTL) 이외의 값을 지정하면 Weight(가중치)에 지정하는 값의 효과가 달라집니다.

값/트래픽 라우팅 대상

IP 주소 또는 레코드 유형에 따라 다른 값(IP address or another value depending on the record type)을 선택합니다. 레코드 유형(Record type) 값에 해당하는 값을 입력합니다. CNAME을 제외한 모든 유형은 둘 이상의 값을 입력할 수 있습니다. 각 값을 별도의 라인에 입력합니다.

트래픽을 라우팅하거나 다음 값을 지정할 수 있습니다.

- A – IPv4 주소
- AAAA - IPv6 주소
- CAA - 인증 기관 인증

- CNAME – 정식 이름
- MX - 메일 교환
- NAPTR - 이름 권한 포인터
- PTR - 포인터
- SPF - 발신자 정책 프레임워크
- SRV - 서비스 로케이터
- TXT - 텍스트

위의 값에 대한 자세한 내용은 값/트래픽 라우팅 대상에 일반적인 값을 참조하세요.

가중치

현재 레코드를 사용하여 Route 53이 응답할 DNS 쿼리의 비율을 결정하는 값입니다. Route 53은 DNS 이름과 유형 조합이 동일한 레코드의 가중치 합을 계산합니다. 이후 Route 53은 총계에 대한 리소스 가중치 비율을 토대로 질의에 응답합니다.

레코드 이름(Record name) 및 레코드 유형(Record type) 값이 가중 레코드와 같은 비-가중 레코드를 생성할 수 없습니다.

0~255 사이의 정수를 입력합니다. 리소스 라우팅을 해제하려면 Weight(가중치)를 0으로 설정합니다. 그룹 내 모든 레코드의 Weight(가중치)를 0으로 설정하면 확률이 동일한 모든 리소스로 트래픽이 라우팅됩니다. 따라서 가중 레코드 그룹에 대한 라우팅이 우발적으로 해제되는 일이 없습니다.

Weight(가중치)를 0으로 설정할 때의 효과는 상태 확인을 레코드와 연관시킬 때와 다릅니다. 자세한 내용은 상태 확인 구성 시 Amazon Route 53의 레코드 선택 방식 단원을 참조하십시오.

상태 확인

Route 53가 지정된 엔드포인트 상태를 점검하고 엔드포인트가 정상할 때만 이 레코드를 사용하여 DNS 쿼리에 응답하길 원할 경우 상태 확인을 선택합니다.

Route 53는 레코드에 지정된 엔드포인트, 예를 들어 값(Value) 필드에서 IP 주소로 지정된 엔드포인트의 상태는 점검하지 않습니다. 레코드의 상태 확인을 선택하면 Route 53가 상태 확인에서 지정한 엔드포인트의 상태를 점검합니다. Route 53가 엔드포인트가 정상인지 여부를 결정하는 방법은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 섹션을 참조하세요.

상태 확인과 레코드를 연관시키는 것은 Route 53가 둘 이상의 레코드 사이에서 DNS 쿼리에 응답할 레코드를 선택할 때 그리고 Route 53가 상태 확인 상태를 선택의 기준으로 삼을 때만 유용합니다. 다음 구성에서만 상태 확인을 사용합니다.

- 이름, 유형 및 라우팅 정책(예: 장애 조치 또는 가중치 레코드)이 동일한 레코드 그룹의 모든 레코드 상태를 확인하고 모든 레코드에 대한 상태 확인 ID를 지정하는 경우. 레코드의 상태 확인에서 양호하지 않은 엔드포인트가 지정될 경우 Route 53는 해당 레코드 값을 사용하는 쿼리에 대한 응답을 중단합니다.
- 별칭 레코드 또는 장애 조치 별칭, 지리적 위치 별칭, 대기 시간 별칭, IP 기반 별칭 또는 가중치 기반 별칭 그룹에 속한 레코드에 대해 대상 상태 평가(Evaluate Target Health)에서 예(Yes)를 선택하는 경우. 별칭 레코드가 동일한 호스팅 영역의 별칭이 아닌 레코드를 참조하는 경우 참조된 레코드의 상태 확인도 지정해야 합니다. 상태 확인과 별칭 레코드를 연관시키고 대상 상태 평가에서 예를 선택하는 경우 둘 다 true로 평가되어야 합니다. 자세한 내용은 상태 확인을 별칭 레코드와 연결하면 어떻게 됩니까? 단원을 참조하십시오.

상태 확인에서 도메인 이름만으로 엔드포인트를 지정할 경우에는 각 엔드포인트마다 별도의 상태 확인을 생성하는 것이 좋습니다. 예를 들어, www.example.com의 콘텐츠를 제공하는 각 HTTP 서버마다 상태 확인을 생성합니다. 도메인 이름(Domain name)의 값은 레코드의 이름(example.com)이 아니라 서버의 도메인 이름(예: us-east-2-www.example.com)을 지정합니다.

> **Important**
>
> 이 구성에서 [Domain name]의 값이 레코드의 이름과 일치하는 상태 확인을 생성한 후 상태 확인을 이러한 레코드와 연결하는 경우 상태 확인 결과를 예측할 수 없습니다.

레코드 ID

가중 레코드 그룹에 있는 이 레코드를 고유하게 식별하는 값을 선택합니다.

가중치 기반 별칭 레코드에 특정한 값

가중치 기반 별칭 레코드를 생성할 때 다음과 같은 값을 지정합니다. 자세한 내용은 별칭 또는 비 별칭 레코드 선택 단원을 참조하십시오.

주제

- 라우팅 정책
- 레코드 이름
- 레코드 유형
- 값/트래픽 라우팅 대상
- 가중치
- 상태 확인
- 대상 상태 평가
- 레코드 ID

라우팅 정책

가중치 기반을 선택합니다.

레코드 이름

트래픽을 라우팅할 도메인 또는 하위 도메인의 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

> **Note**
>
> 호스팅 영역과 이름이 동일한 레코드를 생성할 경우 이름 필드에 값(예: @ 기호)을 입력하지 마십시오.

가중 레코드 그룹의 모든 레코드에 대해 동일한 이름을 입력합니다.

레코드 이름에 대한 자세한 내용은 레코드 이름 단원을 참조하십시오.

레코드 유형

DNS 레코드 유형입니다. 자세한 내용은 지원되는 DNS 레코드 유형 단원을 참조하십시오.

트래픽을 라우팅할 AWS 리소스를 기반으로 해당 값을 선택합니다.

API Gateway 사용자 지정 리전 API 또는 엣지 최적화 API

A - IPv4 주소(A - IPv4 address)를 선택합니다.

Amazon VPC 인터페이스 엔드포인트

A - IPv4 주소(A - IPv4 address)를 선택합니다.

CloudFront 배포

A - IPv4 주소(A - IPv4 address)를 선택합니다.

배포에 대해 IPv6가 활성화되어 있다면 두 개의 레코드를 생성합니다. 하나는 유형(Type) 값이 A - IPv4 주소(A - IPv4 address)이고 하나는 값이 AAAA - IPv6 주소(AAAA - IPv6 address)입니다.

App Runner 서비스

A - IPv4 주소(A - IPv4 address)를 선택합니다.

리전별 하위 도메인이 있는 Elastic Beanstalk 환경

A - IPv4 주소(A - IPv4 address)를 선택합니다.

ELB 로드 밸런서

A - IPv4 address(A - IPv4 주소) 또는 AAAA - IPv6 address(AAAA - IPv6 주소) 선택

Amazon S3 버킷

A - IPv4 주소(A - IPv4 address)를 선택합니다.

OpenSearch Service

A - IPv4 address(A - IPv4 주소) 또는 AAAA - IPv6 address(AAAA - IPv6 주소) 선택

호스팅 영역의 또 다른 레코드

별칭을 생성 중인 레코드 유형을 선택합니다. NS 및 SOA를 제외한 모든 유형이 지원됩니다.

> **Note**
>
> 호스팅 영역(zone apex라고도 함)과 이름이 같은 별칭 레코드를 생성한다면, 유형 값이 CNAME인 레코드로 트래픽을 라우팅할 수 없습니다. 이는 별칭 레코드가 트래픽이 라우팅되는 레코드와 동일한 형식이어야 하고, zone apex에 대한 CNAME 레코드 생성은 별칭 레코드에 대해서도 지원되지 않기 때문입니다.

가중 레코드 그룹의 모든 레코드에 대해 동일 값을 선택합니다.

값/트래픽 라우팅 대상

목록에서 선택하거나 필드에 입력하는 값은 트래픽을 라우팅하는 AWS 리소스에 따라 달라집니다.

대상으로 지정할 수 있는 AWS 리소스에 대한 자세한 내용은 값/라우팅 트래픽에 대한 별칭 레코드의 공통 값을 참조하세요.

트래픽을 특정 AWS 리소스로 라우팅하도록 Route 53를 구성하는 방법에 대한 자세한 내용은 섹션을 참조하세요AWS 리소스로 인터넷 트래픽 라우팅.

가중치

현재 레코드를 사용하여 Route 53이 응답할 DNS 쿼리의 비율을 결정하는 값입니다. Route 53은 DNS 이름과 유형 조합이 동일한 레코드의 가중치 합을 계산합니다. 이후 Route 53은 총계에 대한 리소스 가중치 비율을 토대로 질의에 응답합니다.

레코드 이름(Record name) 및 레코드 유형(Record type) 값이 가중 레코드와 같은 비-가중 레코드를 생성할 수 없습니다.

0~255 사이의 정수를 입력합니다. 리소스 라우팅을 해제하려면 Weight(가중치)를 0으로 설정합니다. 그룹 내 모든 레코드의 Weight(가중치)를 0으로 설정하면 확률이 동일한 모든 리소스로 트래픽이 라우팅됩니다. 따라서 가중 레코드 그룹에 대한 라우팅이 우발적으로 해제되는 일이 없습니다.

Weight(가중치)를 0으로 설정할 때의 효과는 상태 확인을 레코드와 연관시킬 때와 다릅니다. 자세한 내용은 상태 확인 구성 시 Amazon Route 53의 레코드 선택 방식 단원을 참조하십시오.

상태 확인

Route 53가 지정된 엔드포인트 상태를 점검하고 엔드포인트가 정상할 때만 이 레코드를 사용하여 DNS 쿼리에 응답하길 원할 경우 상태 확인을 선택합니다.

Route 53는 레코드에 지정된 엔드포인트, 예를 들어 값(Value) 필드에서 IP 주소로 지정된 엔드포인트의 상태는 점검하지 않습니다. 레코드의 상태 확인을 선택하면 Route 53가 상태 확인에서 지정한 엔드포인트의 상태를 점검합니다. Route 53가 엔드포인트가 정상인지 여부를 결정하는 방법은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 섹션을 참조하세요.

상태 확인과 레코드를 연관시키는 것은 Route 53가 둘 이상의 레코드 사이에서 DNS 쿼리에 응답할 레코드를 선택할 때 그리고 Route 53가 상태 확인 상태를 선택의 기준으로 삼을 때만 유용합니다. 다음 구성에서만 상태 확인을 사용합니다.

- 이름, 유형 및 라우팅 정책(예: 장애 조치 또는 가중치 레코드)이 동일한 레코드 그룹의 모든 레코드 상태를 확인하고 모든 레코드에 대한 상태 확인 ID를 지정하는 경우. 레코드의 상태 확인에서 양호하

지 않은 엔드포인트가 지정될 경우 Route 53는 해당 레코드 값을 사용하는 쿼리에 대한 응답을 중단합니다.

- 별칭 레코드 또는 장애 조치 별칭, 지리적 위치 별칭, 대기 시간 별칭, IP 기반 별칭 또는 가중치 기반 별칭 그룹에 속한 레코드에 대해 대상 상태 평가(Evaluate Target Health)에서 예(Yes)를 선택하는 경우. 별칭 레코드가 동일한 호스팅 영역의 별칭이 아닌 레코드를 참조하는 경우 참조된 레코드의 상태 확인도 지정해야 합니다. 상태 확인과 별칭 레코드를 연관시키고 대상 상태 평가에서 예를 선택하는 경우 둘 다 true로 평가되어야 합니다. 자세한 내용은 상태 확인을 별칭 레코드와 연결하면 어떻게 됩니까? 단원을 참조하십시오.

상태 확인에서 도메인 이름만으로 엔드포인트를 지정할 경우에는 각 엔드포인트마다 별도의 상태 확인을 생성하는 것이 좋습니다. 예를 들어, www.example.com의 콘텐츠를 제공하는 각 HTTP 서버마다 상태 확인을 생성합니다. 도메인 이름(Domain name)의 값은 레코드의 이름(example.com)이 아니라 서버의 도메인 이름(예: us-east-2-www.example.com)을 지정합니다.

> **Important**
>
> 이 구성에서 [Domain name]의 값이 레코드의 이름과 일치하는 상태 확인을 생성한 후 상태 확인을 이러한 레코드와 연결하는 경우 상태 확인 결과를 예측할 수 없습니다.

대상 상태 평가

엔드포인트에서 지정된 리소스의 상태를 확인하여 Route 53가 레코드를 사용해 DNS 쿼리에 응답할지 여부를 결정하게 하려는 경우 예(Yes)를 선택합니다.

다음 사항에 유의하세요.

API Gateway 사용자 지정 리전 API와 엣지 최적화 API

엔드포인트가 API Gateway 사용자 지정 리전 API 또는 엣지 최적화 API인 경우 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정하기 위한 특별한 요구 사항은 없습니다.

CloudFront 배포

엔드포인트가 CloudFront 배포인 경우 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정할 수 없습니다.

리전별 하위 도메인이 있는 Elastic Beanstalk 환경

엔드포인트(Endpoint)에 Elastic Beanstalk 환경을 지정하고 환경에 ELB 로드 밸런서가 포함된 경우, Elastic Load Balancing은 로드 밸런서에 등록된 정상 Amazon EC2 인스턴스로만 쿼리를 라

우팅합니다. (하나의 환경에 한 개 이상의 Amazon EC2 인스턴스가 포함된 경우 ELB 로드 밸런서가 자동으로 포함됩니다.) 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정했는데 정상인 Amazon EC2 인스턴스가 없거나 로드 밸런서 자체가 비정상인 경우 Route 53는 양호한 다른 리소스로 쿼리를 라우팅합니다.

환경에 하나의 Amazon EC2 인스턴스가 포함된 경우에는 특별한 요구 사항이 없습니다.

ELB 로드 밸런서

상태 확인 동작은 로드 밸런서의 유형에 따라 달랍니다.

- Classic Load Balancer: 엔드포인트(Endpoint)에 ELB Classic Load Balancer를 지정한 경우, Elastic Load Balancing은 로드 밸런서에 등록된 정상 Amazon EC2 인스턴스로만 쿼리를 라우팅합니다. 대상 상태 평가(Evaluate target health)를 예(Yes)로 설정하고 EC2 인스턴스가 정상 상태가 아니거나 로드 밸런서 자체가 비정상인 경우 Route 53은 쿼리를 다른 리소스로 라우팅합니다.
- Application Load Balancer 및 Network Load Balancer - ELB Application Load Balancer 또는 Network Load Balancer를 지정하고 대상 상태 평가(Evaluate Target Health)를 예(Yes)로 설정한 경우 Route 53은 로드 밸런서와 연결된 대상 그룹의 상태에 따라 쿼리를 로드 밸런서로 라우팅합니다.
  - Application 또는 Network Load Balancer가 정상 상태로 간주되려면 대상을 포함하는 모든 대상 그룹에 정상 상태 대상이 하나 이상 포함되어야 합니다. 대상 그룹에 정상이 아닌 대상만 포함되는 경우 로드 밸런서는 정상이 아닌 상태로 간주되고 Route 53는 쿼리를 다른 리소스로 라우팅합니다.
  - 등록된 대상이 없는 대상 그룹은 정상이 아닌 상태로 간주됩니다.

> **Note**
>
> 로드 밸런서를 생성할 때 Elastic Load Balancing 상태 확인에 대한 설정을 구성하게 되는데, 이러한 확인은 Route 53 상태 확인은 아니지만 비슷한 기능을 수행합니다. ELB 로드 밸런서에 등록하는 EC2 인스턴스에 대해 Route 53 상태 확인을 생성하지 마십시오.

S3 버킷

엔드포인트가 S3 버킷인 경우 대상 상태 평가(Evaluate Target Health)를 예(Yes)로 설정하는 데 필요한 특정 요건은 없습니다.

Amazon VPC 인터페이스 엔드포인트

엔드포인트가 Amazon VPC 인터페이스 엔드포인트인 경우 대상 상태 평가(Evaluate Target Health)를 예(Yes)로 설정하는 데 필요한 특별한 요구 사항이 없습니다.

동일 호스팅 영역 내 다른 레코드

엔드포인트에서 지정하는 AWS 리소스가 레코드 또는 레코드 그룹(예: 가중치 기반 레코드 그룹)이지만 다른 별칭 레코드가 아닌 경우 상태 확인을 엔드포인트의 모든 레코드와 연결하는 것이 좋습니다. 자세한 내용은 상태 확인을 생략하면 어떻게 됩니까? 단원을 참조하십시오.

레코드 ID

가중 레코드 그룹에 있는 이 레코드를 고유하게 식별하는 값을 선택합니다.

영역 파일을 가져와 레코드 생성

다른 DNS 서비스 공급자로부터 마이그레이션하는 경우, 그리고 현재 DNS 서비스 공급자가 현재 DNS 설정을 영역 파일로 내보내는 것을 허용하는 경우에는, 영역 파일을 가져옴으로써 Amazon Route 53 호스팅 영역의 모든 레코드를 빠르게 생성할 수 있습니다.

> **Note**
>
> 영역 파일은 BIND라는 표준 형식을 사용해 텍스트 형식으로 레코드를 표시합니다. 영역 파일의 형식에 대한 자세한 내용은 Zone file Wikipedia 항목을 참조하십시오. 자세한 내용은 섹션 3.6.1 RFC 1034, 도메인 이름 - 개념 및 설비 및 섹션 5 RFC 1035, 도메인 이름 - 실행 및 사양에서 확인할 수 있습니다.

영역 파일을 가져와 레코드를 생성하고자 할 경우에는 다음 사항에 유의하십시오.

- 영역 파일은 반드시 RFC 규약을 준수하는 형식이어야 합니다.
- 영역 파일에 있는 레코드의 도메인 이름은 호스팅 영역의 이름과 일치해야 합니다.
- Route 53는 `$ORIGIN` 및 `$TTL` 키워드를 지원합니다. 영역 파일에 `$GENERATE` 또는 `$INCLUDE` 키워드가 포함되어 있으면, 가져오기 작업이 실패하고 Route 53는 오류를 반환합니다.
- 영역 파일을 가져올 때 Route 53는 해당 영역 파일에 있는 SOA 레코드를 무시합니다. Route 53는 호스팅 영역과 이름이 같은 NS 레코드도 모두 무시합니다.
- 레코드는 최대 1,000개까지 가져올 수 있습니다.
- 호스팅 영역에 영역 파일에 나타나는 레코드가 이미 포함되어 있으면 가져오기 프로세스가 실패하고 레코드가 생성되지 않습니다.
- 영역 파일의 내용을 검토하여 레코드 이름 뒤에 점이 적절하게 포함되는지 아니면 제외되는지 확인하는 것이 좋습니다.

- 영역 파일에 있는 레코드의 이름에 뒤에 오는 점이 포함되어 있으면(example.com.), 가져오기 프로세스는 그 이름을 전체 주소 도메인 이름으로 해석해 그 이름으로 Route 53 레코드를 생성합니다.
- 영역 파일에 있는 레코드의 이름에 뒤에 오는 점이 포함되어 있지 않으면(www), 가져오기 프로세스는 그 이름을 영역 파일의 도메인 이름(example.com)과 결합하여 결합된 이름(www.example.com)으로 Route 53 레코드를 생성합니다.

내보내기 프로세스가 레코드의 전체 주소 도메인 이름 뒤에 점을 추가하지 않는 경우 Route 53 가져오기 프로세스는 레코드의 이름에 도메인 이름을 추가합니다. 예를 들어, 호스팅 영역 example.com으로 레코드를 가져오고, 영역 파일에 있는 MX 레코드의 이름이 뒤에 오는 점이 없는mail.example.com이라고 가정해봅시다. Route 53 가져오기 프로세스는 mail.example.com.example.com이라는 이름의 MX 레코드를 생성합니다.

> **Important**
>
> CNAME, MX, PTR, 및 SRV 레코드의 경우에 이러한 작동은 RDATA 값에 포함된 도메인 이름에도 적용됩니다. 예를 들어 example.com에 대한 영역 파일이 있다고 가정해봅시다. 영역 파일에 있는 CNAME 레코드(뒤에 오는 점이 없는 support)가 www.example.com(역시 뒤에 오는 점이 없음)이라는 RDATA 값을 갖고 있다면, 가져오기 프로세스는 트래픽을 www.example.com.example.com로 라우팅하는 support.example.com이라는 이름의 Route 53 레코드를 생성합니다. 영역 파일을 가져오기 전에 RDATA 값을 검토하고 필요할 경우 업데이트합니다.

Route 53는 영역 파일로 레코드 내보내기를 지원하지 않습니다.

> **Note**
>
> 호스팅 영역과 이름이 동일한 레코드를 생성할 경우 이름 필드에 값(예: @ 기호)을 입력하지 마십시오.

영역 파일을 가져와 레코드를 생성하려면

1. 현재 도메인을 서비스하는 DNS 서비스 공급자로부터 영역 파일을 가져옵니다. 프로세스와 용어는 서비스 공급자에 따라 다릅니다. 영역 파일 또는 BIND 파일에 레코드를 보내거나 저장하는 작업에 관한 공급자의 인터페이스 및 문서를 참조하십시오.

프로세스가 명확하지 않은 경우에는 현재 DNS 서비스 공급자의 고객 지원 부서에 레코드 목록 또는 영역 파일 정보를 요청하십시오.

2. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
3. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
4. 호스팅 영역(Hosted Zones) 페이지에서 다음과 같이 새 호스팅 영역을 생성합니다.
   a. Create Hosted Zone(호스팅 영역 생성)을 선택합니다.
   b. 도메인 이름을 입력합니다. 옵션 사항으로 코멘트를 입력할 수 있습니다.
   c. 생성(Create)을 선택합니다.
5. 영역 파일 가져오기(Import Zone File)를 선택합니다.
6. 영역 파일 가져오기(Import Zone File) 창에서 영역 파일의 콘텐츠를 영역 파일(Zone File) 텍스트 상자로 붙여넣기 합니다.
7. 가져오기를 선택합니다.

> **Note**
>
> 영역 파일의 레코드 수에 따라 레코드가 생성될 때까지 몇 분 동안 기다려야 할 수도 있습니다.

8. 도메인을 위해 다른 DNS 서비스를 사용한다면(다른 등록 기관을 통해 도메인을 등록한 경우 이는 흔한 일입니다), DNS 서비스를 Route 53으로 마이그레이션합니다. 그 단계가 완료되면 등록 기관은 도메인에 대한 DNS 쿼리에 반응하여 Route 53를 DNS 서비스로 인식하기 시작하고 쿼리는 Route 53 DNS 서비스로 전송되기 시작할 것입니다 (일반적으로 이전 DNS 서비스에 대한 정보가 DNS 해석기에 캐시되는 하루 또는 이틀이 지나야 DNS 쿼리가 Route 53으로 라우팅되기 시작합니다). 자세한 내용은 Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정 단원을 참조하십시오.

레코드 편집

다음 절차는 Amazon Route 53 콘솔을 사용하여 레코드를 편집하는 방법을 설명합니다. Route 53 API를 사용하여 레코드를 편집하는 방법에 대한 자세한 내용은 Amazon Route 53 API 참조의 ChangeResourceRecordSets를 참조하세요.

> **Note**
>
> 레코드 변경 내용이 Route 53 DNS 서버로 전파되려면 시간이 걸립니다. 현재 변경 사항의 전파 여부를 확인하는 유일한 방법은 GetChange API 작업을 사용하는 것입니다. 변경 사항은 일반적으로 60초 이내에 모든 Route 53 이름의 서버로 전파됩니다.

Route 53 콘솔을 사용하여 레코드를 편집하려면

1. 별칭 레코드를 편집하지 않는 경우에는 2단계로 건너뜁니다.

   트래픽을 Elastic Load Balancing Classic Load Balancer, Application Load Balancer 또는 Network Load Balancers로 라우팅하는 별칭 레코드를 편집하는 경우 그리고 서로 다른 계정을 사용하여 Route 53 호스팅 영역 및 로드 밸런서를 생성한 경우에는 Elastic Load Balancing 로드 밸런서의 DNS 이름 가져오기 절차를 수행하여 로드 밸런서에 대한 DNS 이름을 가져옵니다.

   다른 AWS 리소스의 별칭 레코드를 편집하는 경우 2단계로 건너뜁니다.
2. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
3. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
4. Hosted Zones(호스팅 영역) 페이지에서 편집하려는 레코드가 포함된 호스팅 영역 행을 선택합니다.
5. 편집할 레코드의 행을 선택한 다음 레코드 편집 창에서 변경 사항을 입력합니다.
6. 관련 값들을 입력합니다. 자세한 내용은 Amazon Route 53 레코드를 생성 또는 편집할 때 지정하는 값 단원을 참조하십시오.
7. 변경 사항 저장(Save changes)을 선택합니다.
8. 레코드를 여러 개 편집하는 경우에는 5~7단계를 반복합니다.

레코드 삭제

다음 절차에서는 Route 53 콘솔을 사용하여 레코드를 삭제하는 방법을 설명합니다. Route 53 API를 사용하여 레코드를 삭제하는 방법에 대한 자세한 내용은 Amazon Route 53 API 참조의 ChangeResourceRecordSets를 참조하세요.

> **Note**
>
> 레코드 변경 내용이 Route 53 DNS 서버로 전파되려면 시간이 걸립니다. 현재 변경 사항의 전파 여부를 확인하는 유일한 방법은 GetChange API 작업을 사용하는 것입니다. 변경 사항은 일반적으로 60초 이내에 모든 Route 53 이름의 서버로 전파됩니다.

레코드를 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 호스팅 영역 페이지에서 삭제할 레코드가 포함된 호스팅 영역의 행을 선택합니다.
3. 레코드 목록에서 삭제하려는 레코드를 선택합니다.

   연속된 여러 레코드를 선택하려면 첫 번째 행을 선택한 다음 Shift 키를 누른 상태에서 마지막 행을 선택합니다. 연속되지 않는 여러 레코드를 선택하려면 첫 번째 행을 선택한 다음 Ctrl 키를 누른 상태에서 다른 행을 추가로 클릭합니다.

   유형(Type) 값이 NS 또는 SOA인 레코드는 삭제할 수 없습니다.
4. Delete(삭제)를 선택합니다.
5. 대화 상자를 닫으려면 삭제(Delete)를 선택합니다.

레코드 나열

다음 절차는 Amazon Route 53 콘솔을 사용하여 호스팅 영역의 레코드를 나열하는 방법을 설명합니다. Route 53 API를 사용하여 레코드를 나열하는 방법에 대한 자세한 내용은 Amazon Route 53 API 참조의 ListResourceRecordSets를 참조하세요.

레코드를 나열하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
3. [Hosted Zones] 페이지에서 호스팅 영역의 이름을 선택합니다.
4. 검색 모드를 변경하려면 페이지의 오른쪽 상단에서 레코드 테이블을 선택합니다. 다음 중 하나를 선택합니다.

- 자동

  이 모드에서 서비스는 레코드 수에 기반한 필터를 사용합니다. 레코드가 2000개 미만인 경우에는 전체 모드를, 레코드가 2000개 이상인 경우에는 빠른 모드를 사용합니다.

- 전체

  이 모드에서는 모든 검색 필터를 사용할 수 있지만 검색 성능이 느려질 수 있습니다.

- 빠른

  이 모드에서는 일부 고급 기능을 사용할 수 없지만 검색 성능은 더 빨라집니다.

선택한 레코드만을 표시하려면, 다음과 같이 레코드 목록 위에 해당되는 검색 기준을 입력합니다. 자동 모드에서 검색 동작은 호스팅 영역에 최대 2,000개 또는 2,000개 이상의 레코드를 포함하는지 여부에 따라 다릅니다.

레코드가 최대 2,000개인 경우 및 전체 모드

- 특정 값을 지닌 레코드를 표시하려면, 검색 창에 값을 입력하고 Enter 키를 누릅니다. 예를 들어, 192.0으로 시작하는 IP 주소를 지닌 레코드를 표시하려면, 검색 필드에 그 값을 입력하고 입력 키를 누릅니다.
- DNS 레코드 유형이 같은 레코드만을 표시하려면, 드롭다운 목록에서 레코드 유형(Record type)을 선택한 다음 레코드 유형을 입력합니다.
- 별칭 레코드만을 표시하려면 드롭다운 목록에서 별칭(Alias)을 선택하고 **`Yes`**를 입력합니다.
- 가중치 기반 레코드만을 표시하려면 드롭다운 목록에서 라우팅 정책(Routing policy)을 선택한 다음 **`WEIGHTED`**를 입력합니다.

레코드가 2,000개 이상인 경우 및 빠른 모드

- 레코드 값이 아닌 레코드 이름으로만 검색할 수 있습니다. 또한 레코드 유형 또는 별칭이나 가중치 레코드를 기반으로 필터링할 수 없습니다.

  이렇게 하려면 필터 텍스트 상자에 커서를 놓고 속성을 선택한 다음 레코드 이름을 선택합니다.

- 레이블이 3개(점으로 세 부분이 구분됨)인 레코드의 경우 검색 필드에서 값을 입력하고 Enter를 누르면 Route 53 콘솔이 레코드 이름에서 오른쪽 세 번째 레이블에서 와일드카드 검색을 자동으로 수행합니다. 예를 들어, 호스팅 영역 example.com에 record1.example.com부터 record100.example.com까지 100개의 레코드가 있습니다. (Record1이 오른쪽에서 세 번째 레이블입니다.) 다음 값으로 검색하면 다음과 같이 진행됩니다.

- record1 - Route 53 콘솔이 record1*.example.com을 검색하고 record1.example.com, record10.example.com부터 record19.example.com 그리고 record100.example.com을 반환합니다.
- record1.example.com - 이전 예제처럼 콘솔은 record1*.example.com을 검색하고 동일한 레코드를 반환합니다.
- 1 - 콘솔이 1*.example.com을 검색하고 아무런 레코드도 반환하지 않습니다.
- example - 콘솔이 example*.example.com을 검색하고 아무런 레코드도 반환하지 않습니다.
- example.com - 이 예제에서 콘솔은 와일드카드 검색을 수행하지 않습니다. 호스팅 영역의 모든 레코드를 반환합니다.
- 자동 검색 모드 - 이 검색 모드를 사용할 때는 먼저 레코드 이름과 같은 속성을 입력해야 검색할 수 있습니다.

> **Note**
>
> 오른쪽의 세 번째 레이블에 하나 이상의 하이픈(예: `third-label.example.com`)이 포함되어 있는 경우 세 번째 레이블에서 하이픈(이 예에서는 `third`) 바로 앞 부분을 검색하면 Route 53가 레코드를 반환하지 않습니다. 대신 하이픈을 포함하거나(`third-` 검색) 하이픈 바로 앞의 문자를 생략하십시오(`third` 검색).

- 레이블이 4개 이상인 레코드의 경우 동일한 레코드 이름을 지정해야 합니다. 와일드카드 검색은 지원되지 않습니다. 예를 들어, 호스팅 영역에 이름이 label4.record1.example.com인 레코드가 포함된 경우 검색 필드에서 label4.record1.example.com을 지정한 경우에만 해당 레코드를 찾을 수 있습니다.

Amazon Route 53에서 DNSSEC 서명 구성

DNSSEC(도메인 이름 시스템 보안 확장) 서명을 사용하면 DNS 해석기가 DNS 응답이 Amazon Route 53에서 왔으며 변조되지 않았는지 검증할 수 있습니다. DNSSEC 서명을 사용하면 호스팅 영역에 대한 모든 응답이 퍼블릭 키 암호화를 사용하여 서명됩니다. DNSSEC에 대한 개요는 AWS re:Invent 2021 - Amazon Route 53: A year in review의 DNSSEC 섹션을 참조하세요.

이 장에서는 Route 53에 대해 DNSSEC 서명을 사용하는 방법, KSK(키 서명 키)에서 작업하는 방법 및 문제 해결 방법에 대해 설명합니다. 에서 DNSSEC 서명을 사용하거나 API를 사용하여 AWS Management Console 프로그래밍 방식으로 작업할 수 있습니다. CLI나 SDK를 사용하여 Route 53에서 작업하는 방법에 대한 자세한 내용은 Amazon Route 53 설정 섹션을 참조하세요.

DNSSEC 서명을 사용하기 전에 다음 사항에 유의하세요.

- 영역 중단을 방지하고 도메인을 사용할 수 없게 되는 문제를 방지하려면 DNSSEC 오류를 신속하게 대응하고 해결해야 합니다. `DNSSECInternalFailure` 또는 `DNSSECKeySigningKeysNeedingAction` 오류를 감지할 때마다 알림이 전송되도록 CloudWatch 경보를 설정하는 것이 좋습니다. 자세한 내용은 Amazon CloudWatch를 사용하여 호스팅 영역 모니터링 섹션을 참조하세요.
- DNSSEC에는 KSK(키 서명 키) 와 ZSK(영역 서명 키)라는 두 가지 키가 있습니다. Route 53 DNSSEC 서명에서 각 KSK는 사용자가 소유한 AWS KMS 의 비대칭 고객 관리형 키를 기반으로 합니다. 필요한 경우 교체를 포함한 KSK 관리에 대한 책임은 사용자에게 있습니다. ZSK 관리는 Route 53에서 수행합니다.
- 호스팅 영역에 대해 DNSSEC 서명을 사용하면 Route 53가 TTL을 1주일로 제한합니다. 호스팅 영역의 레코드에 대해 TTL을 1주일보다 긴 기간으로 설정하면 오류가 발생하지 않습니다. 그러나 Route 53는 해당 레코드에 대해 1주일의 TTL을 적용합니다. TTL이 1주일 미만인 레코드와 DNSSEC 서명이 사용되지 않은 다른 호스팅 영역의 레코드는 영향을 받지 않습니다.
- DNSSEC 서명을 사용하면 다중 공급 업체 구성이 지원되지 않습니다. 화이트 레이블 이름 서버(베니티 이름 서버 또는 프라이빗 이름 서버라고도 함)를 구성한 경우, 이 이름 서버가 단일 DNS 공급자로 제공되는지 확인합니다.
- 일부 DNS 공급자는 권한 있는 DNS에 DS(Delegation Signer) 레코드를 지원하지 않습니다. DS 쿼리 응답에 AA 플래그를 설정하지 않고 DS 쿼리를 지원하지 않는 DNS 공급자가 상위 영역을 호스팅한다면, 하위 영역에서 DNSSEC를 활성화하는 경우에 하위 영역을 확인할 수 없게 됩니다. DNS 공급자가 DS 레코드를 지원하는지 확인하세요.
- 영역 소유자 외에 다른 사용자가 해당 영역에 레코드를 추가하거나 제거할 수 있도록 IAM 권한을 설정하는 것이 도움이 될 수 있습니다. 예를 들어 영역 소유자는 KSK를 추가하고 서명을 활성화할 수 있으며 키 교체를 담당할 수도 있습니다. 그러나 다른 사람에게 호스팅 영역에 대한 다른 레코드로 작업할 책임이 있을 수 있습니다. IAM 정책 예제는 도메인 레코드 소유자에 대한 사용 권한 예제 단원을 참조하세요.
- TLD에 DNSSEC 지원이 있는지 확인하려면 Amazon Route 53에 등록할 수 있는 도메인 섹션을 참조하세요.

주제

- DNSSEC 서명 활성화 및 신뢰 체인 설정
- DNSSEC 서명 비활성화
- DNSSEC용 고객 관리형 키 작업

- KSK(키 서명 키)로 작업
- Route 53에서의 KMS 키 및 ZSK 관리
- Route 53에서 존재하지 않는다는 DNSSEC 증명
- DNSSEC 서명 문제 해결

DNSSEC 서명 활성화 및 신뢰 체인 설정

증분 단계는 호스팅 영역 소유자와 상위 영역 유지 관리자에게 적용됩니다. 두 사람은 동일한 사람이 될 수 있지만, 그렇지 않은 경우 영역 소유자는 상위 영역 유지 관리자에게 알리고 협력해야 합니다.

이 문서의 단계를 따라 영역에 서명하고 신뢰 체인에 포함시키는 것이 좋습니다. 다음 단계는 DNSSEC로의 온보딩 시 위험을 최소화해 줍니다.

> **Note**
>
> 시작하기 전에 Amazon Route 53에서 DNSSEC 서명 구성에서 사전 조건을 읽어야 합니다.

DNSSEC 서명을 활성화하려면 다음 섹션에 설명된 세 가지 단계를 수행해야 합니다.

주제

- 1단계: DNSSEC 서명 활성화 준비
- 2단계: DNSSEC 서명 활성화 및 KSK 생성
- 3단계: 신뢰 체인 설정

1단계: DNSSEC 서명 활성화 준비

준비 단계는 영역 가용성을 모니터링하고 서명 활성화와 DS(Delegation Signer) 레코드 삽입 사이의 대기 시간을 줄여 DNSSEC로의 온보딩 시 위험을 최소화하는 데 도움이 됩니다.

DNSSEC 서명 활성화를 준비하려면

1. 영역 가용성을 모니터링합니다.

   영역의 도메인 이름 가용성을 모니터링할 수 있습니다. 이것은 DNSSEC 서명을 활성화한 후 한 단계 뒤로 롤백해야 하는 모든 문제를 해결하는 데 도움이 될 수 있습니다. 쿼리 로깅을 사용하여

대부분의 트래픽에서 도메인 이름을 모니터링할 수 있습니다. 쿼리 로깅 역할 설정에 대한 자세한 내용은 Amazon Route 53 모니터링 단원을 참조하세요.

모니터링은 셸 스크립트 또는 서드 파티 서비스를 통해 수행할 수 있습니다. 그러나 이것이 롤백이 필요한지 결정하기 위한 유일한 신호는 아닙니다. 도메인을 사용할 수 없는 문제로 고객으로부터 피드백을 받을 수도 있습니다.

2. 영역의 최대 TTL을 낮춥니다.

영역의 최대 TTL은 영역에서 가장 긴 TTL 레코드입니다. 다음의 영역 예에서 영역의 최대 TTL은 1일(86,400초)입니다.

명칭	TTL	레코드 클래스	레코드 유형	레코드 데이터
example.com.	900	IN	SOA	ns1.example.com. hostmaster.example.com. 2002022401 10800 15 604800 300
example.com.	900	IN	NS	ns1.example.com.
route53.example.com.	86400	IN	TXT	**some txt record**

영역의 최대 TTL을 낮추면 서명 활성화와 DS(Delegation Signer) 레코드 삽입 사이의 대기 시간을 줄이는 데 도움이 됩니다. 영역의 최대 TTL을 1시간(3,600초)으로 낮추는 것이 좋습니다. 이렇게 하면 해석기가 서명된 레코드를 캐싱하는 데 문제가 있는 경우 단 1시간 후에 롤백할 수 있습니다.

롤백: TTL 변경 사항을 실행 취소합니다.

3. SOA TTL 및 SOA 최소 필드를 낮춥니다.

SOA 최소 필드는 SOA 레코드 데이터의 마지막 필드입니다. 다음 SOA 레코드 예제에서 최소 필드는 5분(300초)의 값을 가집니다.

명칭	TTL	레코드 클래스	레코드 유형	레코드 데이터
example.com.	900	IN	SOA	ns1.example.com. hostmaster.example.com. 2002022401 10800 15 604800 300

SOA TTL 및 SOA 최소 필드는 해석기가 부정 답변을 얼마나 오래 기억할지 결정합니다. 서명을 활성화하면 Route 53 이름 서버가 부정 답변을 위한 NSEC 레코드를 반환하기 시작합니다. NSEC에는 해석기가 부정 답변을 합성하는 데 사용할 수 있는 정보가 포함되어 있습니다. NSEC 정보로 인해 해석기가 이름에 대한 부정 답변을 가정하기 때문에 롤백해야 하는 경우, 해석기가 가정을 중지하게 하려면 SOA TTL 및 SOA 최소 필드의 최댓값을 기다리기만 하면 됩니다.

롤백: SOA 변경 사항을 실행 취소합니다.

4. TTL 및 SOA 최소 필드 변경의 효과가 적용되었는지 확인합니다.

   GetChange를 사용하여 지금까지의 변경 사항이 모든 Route 53 DNS 서버에 전파되었는지 확인합니다.

2단계: DNSSEC 서명 활성화 및 KSK 생성

Route 53 콘솔에서 AWS CLI 또는를 사용하여 DNSSEC 서명을 활성화하고 키 서명 키(KSK)를 생성할 수 있습니다.

- CLI
- 콘솔

고객 관리형 KMS 키를 제공하거나 만드는 경우 몇 가지 요구 사항이 있습니다. 자세한 내용은 DNSSEC용 고객 관리형 키 작업 단원을 참조하십시오.

CLI

이미 보유하고 있는 키를 사용하거나, 고유한 요청을 만들기 위해 hostedzone_id, cmk_arn, ksk_name 및 unique_string에 대한 자체 값을 사용하는 다음과 같은 AWS CLI 명령을 실행하여 키를 생성할 수 있습니다.

```
aws --region us-east-1 route53 create-key-signing-key \
   --hosted-zone-id $hostedzone_id \
   --key-management-service-arn $cmk_arn --name $ksk_name \
   --status ACTIVE \
   --caller-reference $unique_string
```

사용자 지정 고객 관리형 키에 대한 자세한 내용은 DNSSEC용 고객 관리형 키 작업 단원을 참조하세요. CreateKeySigningKey도 참조하세요.

DNSSEC 서명을 활성화하려면에 대한 자체 값을 사용하여 hostedzone_id다음과 같은 AWS CLI 명령을 실행합니다.

```
aws --region us-east-1 route53 enable-hosted-zone-dnssec \
   --hosted-zone-id $hostedzone_id
```

자세한 내용은 enable-hosted-zone-dnssec 및 EnableHostedZoneDNSSEC을 참조하세요.

Console

DNSSEC 서명 활성화 및 KSK 생성

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역을 선택한 후 DNSSEC 서명을 활성화할 호스팅 영역을 선택합니다.
3. DNSSEC 서명 탭에서 DNSSEC 서명 활성화를 선택합니다.

> **Note**
>
> 이 섹션의 옵션이 DNSSEC 서명 비활성화인 경우 DNSSEC 서명 활성화의 첫 단계를 이미 완료한 것입니다. DNSSEC의 호스팅 영역에 대한 신뢰 체인을 설정하거나 이미 존재하는지 확인하세요. 그러면 완료됩니다. 자세한 내용은 3단계: 신뢰 체인 설정 단원을 참조하십시오.

4. KSK(키 서명 키) 생성(Key-signing key (KSK) creation) 섹션에서 새 KSK 생성(Create new KSK)을 선택하고 KSK 이름 제공(Provide KSK name)에 Route 53가 생성할 KSK의 이름을 입력합니다. 이름에는 숫자, 문자, 밑줄(_)이 포함될 수 있습니다. 이름은 고유해야 합니다.
5. 고객 관리형 CMK에서 Route 53에서 KSK를 생성할 때 사용할 고객 관리형 키를 선택합니다. DNSSEC 서명에 적용되는 기존 고객 관리형 키를 사용하거나 새 고객 관리형 키를 생성할 수 있습니다.

   고객 관리형 KMS 키를 제공하거나 만드는 경우 몇 가지 요구 사항이 있습니다. 자세한 내용은 DNSSEC용 고객 관리형 키 작업 섹션을 참조하세요.
6. 기존 고객 관리형 키의 별칭을 입력합니다. 새 고객 관리형 키를 사용하려면 고객 관리형 키의 별칭을 입력합니다. 그러면 Route 53에서 키를 생성합니다.

   > **Note**
   >
   > Route 53에서 고객 관리형 키를 만들도록 선택한 경우 고객 관리형 키마다 별도의 요금이 부과됩니다. 자세한 내용은 AWS Key Management Service 요금을 참조하세요.
7. DNSSEC 서명 활성화를 선택합니다.

영역 서명을 활성화한 후 다음 단계를 완료합니다(콘솔 또는 CLI를 사용했는지 여부에 상관 없음).

1. 영역 서명의 효과가 적용되었는지 확인합니다.

   를 사용한 경우 `EnableHostedZoneDNSSEC()` 호출 출력의 작업 ID를 사용하여 get-change 또는 GetChange를 실행하여 모든 Route 53 DNS 서버가 응답에 서명하는지 확인할 AWS CLI수 있습니다(상태 = `INSYNC`).
2. 적어도 이전 영역의 최대 TTL 동안 기다립니다.

   해석기가 서명되지 않은 모든 레코드를 캐시에서 비울 때까지 기다립니다. 이를 위해서는 적어도 이전 영역의 최대 TTL 동안 기다려야 합니다. 위의 `example.com` 영역에서는 대기 시간이 1일입니다.
3. 고객 문제에 대한 보고서를 모니터링합니다.

   영역 서명을 활성화한 후에는 고객에게 네트워크 디바이스 및 해석기와 관련된 문제가 표시되기 시작할 수 있습니다. 권장되는 모니터링 기간은 2주입니다.

   다음은 표시될 수 있는 문제의 예제니다.

- 일부 네트워크 디바이스는 DNS 응답 크기를 512바이트 미만으로 제한할 수 있으며 이는 일부 서명된 응답에 사용하기에 너무 작은 크기입니다. 이러한 네트워크 디바이스는 더 큰 DNS 응답 크기를 허용하도록 재구성되어야 합니다.
- 일부 네트워크 디바이스는 DNS 응답에 대한 세부적인 검사를 수행하여 DNSSEC에 사용된 것과 같이 디바이스가 이해하지 못하는 특정 레코드를 제거합니다. 이러한 디바이스는 재구성해야 합니다.
- 일부 고객의 해석기는 네트워크가 지원하는 것보다 더 큰 UDP 응답을 받아들일 수 있다고 주장합니다. 네트워크 역량을 테스트하고 해석기를 적절하게 구성할 수 있습니다. 자세한 내용은 DNS 응답 크기 테스트 서버를 참조하세요.

롤백: DisableHostedZoneDNSSEC를 호출한 다음 1단계: DNSSEC 서명 활성화 준비의 단계를 롤백합니다.

3단계: 신뢰 체인 설정

Route 53에서 호스팅 영역에 대해 DNSSEC 서명을 활성화한 후 호스팅 영역에 대한 신뢰 체인을 설정하여 DNSSEC 서명 설정을 완료합니다. 이렇게 하려면 Route 53에서 제공하는 정보를 사용하여 호스팅 영역에 대한 상위 호스팅 영역에서 DS(Delegation Signer) 레코드를 생성하면 됩니다. 도메인이 등록된 위치에 따라 Route 53의 상위 호스팅 영역 또는 다른 도메인 등록 기관에 레코드를 추가합니다.

DNSSEC 서명에 대한 신뢰 체인을 설정하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역을 선택한 후 DNSSEC 신뢰 체인을 설정할 호스팅 영역을 선택합니다. 먼저 DNSSEC 서명을 활성화해야 합니다.
3. DNSSEC 서명의 DNSSEC 서명 탭에서 DS 레코드를 만들기 위한 정보 보기를 선택합니다.

   > **Note**
   >
   > 이 섹션에 DS 레코드를 만들기 위한 정보 보기가 표시되지 않는 경우 신뢰 체인을 설정하기 전에 DNSSEC 서명을 활성화해야 합니다. DNSSEC 서명 활성화(Enable DNSSEC signing)를 선택하고 2단계: DNSSEC 서명 활성화 및 KSK 생성에 설명된 단계를 완료한 다음 이 단계로 돌아와 신뢰 체인을 설정합니다.

4. 신뢰 체인 설정에서 도메인이 등록된 위치에 따라 Route 53 등록 기관 또는 다른 도메인 등록 기관 중 하나를 선택합니다.

5. 3단계에서 제공된 값을 사용하여 Route 53의 상위 호스팅 영역에 대한 DS 레코드를 생성합니다. 도메인이 Route 53에서 호스팅되지 않는 경우, 제공된 값을 사용하여 도메인 등록 기관 웹 사이트에 DS 레코드를 생성합니다.

   상위 영역에 대한 신뢰 체인을 설정합니다.

   - 도메인이 Route 53를 통해 관리되는 경우 다음 단계를 따릅니다.

     올바른 서명 알고리즘(ECDSAP256SHA256 및 유형 13) 및 다이제스트 알고리즘(SHA-256 및 유형 2)을 구성했는지 확인합니다.

     Route 53가 등록 기관인 경우 Route 53 콘솔에서 다음을 수행합니다.

     1. 키 유형, 서명 알고리즘 및 퍼블릭 키 값을 참고합니다. 탐색 창에서 등록된 도메인을 선택합니다.
     2. 도메인을 선택한 다음 DNSSEC 상태 옆의 키 관리를 선택합니다.
     3. DNSSEC 키 관리(Manage DNSSEC keys) 대화 상자의 드롭다운 메뉴에서 Route 53 등록 기관(Route 53 registrar)의 적절한 키 유형(Key type) 및 알고리즘(Algorithm)을 선택합니다.
     4. Route 53 등록 기관의 퍼블릭 키를 복사합니다. DNSSEC 키 관리(Manage DNSSEC keys) 대화 상자에서 값을 퍼블릭 키(Public key) 입력란에 붙여넣습니다.
     5. 추가를 선택합니다.

        Route 53는 공개 키의 상위 영역에 DS 레코드를 추가합니다. 예를 들어 도메인이 `example.com`인 경우 DS 레코드는 .com DNS 영역에 추가됩니다.

   - 도메인이 다른 레지스트리에서 관리되는 경우 다른 도메인 등록 기관 섹션의 지침을 따릅니다.

     다음 단계가 원활하게 진행될 수 있도록 상위 영역에 낮은 DS TTL을 도입합니다. 변경 사항을 롤백해야 하는 경우 빠르게 복구할 수 있도록 DS TTL을 5분(300초)으로 설정하는 것이 좋습니다.

     - 하위 영역에 대한 신뢰 체인을 설정합니다.

       상위 영역을 다른 레지스트리에서 관리하는 경우 등록 기관에 연락하여 해당 영역에 대한 DS 레코드를 도입하도록 합니다. 일반적으로 DS 레코드의 TTL은 조정할 수 없습니다.

     - 상위 영역이 Route 53에서 호스팅되는 경우 상위 영역 소유자에게 연락하여 해당 영역에 대한 DS 레코드를 도입하도록 합니다.

       상위 영역 소유자에게 `$ds_record_value`를 제공합니다. 이 값은 콘솔의 DS 레코드를 생성하기 위한 정보 보기(View Information to create DS record)를 클릭하고 DS 레코드(DS

record) 필드를 복사하거나 GetDNSSEC API를 호출하고 'DSRecord' 필드의 값을 검색하여 얻을 수 있습니다.

```
aws --region us-east-1 route53 get-dnssec
            --hosted-zone-id $hostedzone_id
```

상위 영역 소유자는 Route 53 콘솔 또는 CLI를 통해 레코드를 삽입할 수 있습니다.

- 를 사용하여 DS 레코드 AWS CLI를 삽입하려면 상위 영역 소유자가 다음 예제와 유사한 JSON 파일을 생성하고 이름을 지정합니다. 상위 영역 소유자는 파일의 이름을 `inserting_ds.json`과 같이 지정할 수 있습니다.

```
{
    "HostedZoneId": "$parent_zone_id",
    "ChangeBatch": {
        "Comment": "Inserting DS for zone $zone_name",
        "Changes": [
            {
                "Action": "UPSERT",
                "ResourceRecordSet": {
                    "Name": "$zone_name",
                    "Type": "DS",
                    "TTL": 300,
                    "ResourceRecords": [
                        {
                            "Value": "$ds_record_value"
                        }
                    ]
                }
            }
        ]
    }
}
```

그런 다음, 다음 명령을 실행합니다.

```
aws --region us-east-1 route53 change-resource-record-sets
            --cli-input-json file://inserting_ds.json
```

- 콘솔을 사용하여 DS 레코드를 삽입하려면

  https://console.aws.amazon.com/route53/에서 Route 53 콘솔을 엽니다.

탐색 창의 호스팅 영역(Hosted zones)에서 호스팅 영역의 이름을 선택한 다음 레코드 생성(Create record) 버튼을 선택합니다. 라우팅 정책(Routing policy)에 단순 라우팅을 선택했는지 확인합니다.

레코드 이름(Record name) 필드에 `$zone_name`과 같은 이름을 입력하고, 레코드 유형(Record type) 드롭 다운에서 DS를 선택하고, 값(Value) 필드에 `$ds_record_value`의 값을 입력한 다음 레코드 생성(Create records)을 선택합니다.

롤백: 상위 영역에서 DS를 제거하고 DS TTL 동안 기다린 다음 신뢰를 설정하는 단계를 롤백합니다. 상위 영역이 Route 53에서 호스팅되는 경우, 상위 영역 소유자는 JSON 파일의 `Action`을 `UPSERT`에서 `DELETE`로 변경하고 위의 예제 CLI를 다시 실행할 수 있습니다.

6. 도메인 레코드의 TTL을 기반으로 업데이트가 전파될 때까지 기다립니다.

   상위 영역이 Route 53 DNS 서비스에 있는 경우, 상위 영역 소유자는 GetChange API를 통해 전파 완료를 확인할 수 있습니다.

   그렇지 않으면 DS 레코드의 상위 영역을 주기적으로 조사한 다음 DS 레코드 삽입이 완전히 전파될 확률을 높일 수 있도록 10분 더 기다릴 수 있습니다. 일부 등록 기관은 일정(예: 하루에 한 번)에 따라 DS 삽입을 수행합니다.

상위 영역에 DS(Delegation Signer) 레코드를 도입하면 DS를 선택한 검증된 해석기가 해당 영역에서 응답의 유효성을 검사하기 시작합니다.

신뢰 설정 단계가 원활하게 진행되도록 하려면 다음을 완료합니다.

1. 최대 NS TTL을 찾습니다.

   영역과 관련된 NS 레코드에는 2가지 세트가 있습니다.

   - 위임 NS 레코드 - 상위 영역이 보유한 영역에 대한 NS 레코드입니다. 이 레코드는 다음 Unix 명령을 실행하여 찾을 수 있습니다(영역이 example.com인 경우 상위 영역은 com).

     ```
     dig -t NS com
     ```

     NS 레코드 중 하나를 선택한 후 다음을 실행합니다.

     ```
     dig @one of the NS records of your parent zone -t NS example.com
     ```

     예:

```
dig @b.gtld-servers.net. -t NS example.com
```

- 영역 내 NS 레코드 - 이것은 영역에 있는 NS 레코드입니다. 이 레코드는 다음 Unix 명령을 실행하여 찾을 수 있습니다.

  ```
  dig @one of the NS records of your zone -t NS example.com
  ```

  예:

  ```
  dig @ns-0000.awsdns-00.co.uk. -t NS example.com
  ```

  두 영역 모두에 대한 최대 TTL을 확인합니다.

2. 최대 NS TTL 동안 기다립니다.

   DS 삽입 전에 해석기는 서명된 응답을 받지만 서명을 검증하지는 않습니다. DS 레코드가 삽입되면 영역의 NS 레코드가 만료되기 전까지는 해석기가 해당 레코드를 볼 수 없습니다. 해석기가 NS 레코드를 다시 가져오면 DS 레코드도 반환됩니다.

   고객이 동기화되지 않은 클럭이 있는 호스트에서 해석기를 실행하는 경우 시계가 올바른 시간에서 1시간 이내인지 확인하십시오.

   이 단계를 완료하면 모든 DNSSEC 인식 해석기가 영역을 검증합니다.

3. 이름 확인을 관찰합니다.

   해석기의 영역 검증에 문제가 없음을 확인해야 합니다. 고객이 문제를 보고하는 데 필요한 시간도 고려해야 합니다.

   최대 2주 동안 모니터링하는 것이 좋습니다.

4. (선택 사항) DS 및 NS TTL을 늘립니다.

   설정에 만족하면 TTL 및 SOA 변경 사항을 저장할 수 있습니다. Route 53는 서명된 영역에 대해 TTL을 1주로 제한합니다. 자세한 내용은 Amazon Route 53에서 DNSSEC 서명 구성 섹션을 참조하세요.

   DS TTL을 변경할 수 있는 경우, 1시간으로 설정하는 것이 좋습니다.

DNSSEC 서명 비활성화

Route 53에서 DNSSEC 서명을 비활성화하는 단계는 호스팅 영역이 속한 신뢰 체인에 따라 다릅니다.

예를 들어 호스팅 영역에 신뢰 체인의 일부로 DS(Delegation Signer) 레코드가 있는 상위 영역이 있을 수 있습니다. 호스팅 영역 자체가 신뢰 체인의 또 다른 부분인 DNSSEC 서명을 활성화한 하위 영역의 상위 영역일 수도 있습니다. DNSSEC 서명을 사용하지 않는 단계를 수행하기 전에 호스팅 영역에 대한 전체 신뢰 체인을 조사하고 확인합니다.

서명을 사용하지 않는 경우 DNSSEC 서명을 활성화하는 호스팅 영역에 대한 신뢰 체인은 주의해서 실행 취소해야 합니다. 신뢰 체인에서 호스팅 영역을 제거하려면 이 호스팅 영역을 포함하는 신뢰 체인의 위치에 있는 모든 DS 레코드를 제거합니다. 즉, 순서대로 다음을 수행해야 합니다.

1. 이 호스팅 영역에 신뢰 체인의 일부인 하위 영역으로 있는 DS 레코드를 모두 제거합니다.
2. 상위 영역에서 DS 레코드를 제거합니다. 신뢰 영역이 있는 경우(상위 영역에 DS 레코드가 없고 이 영역의 하위 영역에 대한 DS 레코드가 없는 경우) 이 단계를 건너뜁니다.
3. DS 레코드를 제거할 수 없는 경우, 신뢰 체인에서 영역을 제거하려면 상위 영역에서 NS 레코드를 제거합니다. 자세한 내용은 도메인의 글루 레코드 및 이름 서버 추가 또는 변경 단원을 참조하십시오.

다음 증분 단계를 통해 개별 단계의 효과를 모니터링하여 영역의 DNS 가용성 문제를 방지할 수 있습니다.

DNSSEC 서명을 비활성화하려면

1. 영역 가용성을 모니터링합니다.

   영역의 도메인 이름 가용성을 모니터링할 수 있습니다. 이것은 DNSSEC 서명을 활성화한 후 한 단계 뒤로 롤백해야 하는 모든 문제를 해결하는 데 도움이 될 수 있습니다. 쿼리 로깅을 사용하여 대부분의 트래픽에서 도메인 이름을 모니터링할 수 있습니다. 쿼리 로깅 역할 설정에 대한 자세한 내용은 Amazon Route 53 모니터링 단원을 참조하세요.

   모니터링은 셸 스크립트 또는 유료 서비스를 통해 수행할 수 있습니다. 그러나 이것이 롤백이 필요한지 결정하기 위한 유일한 신호는 아닙니다. 도메인을 사용할 수 없는 문제로 고객으로부터 피드백을 받을 수도 있습니다.
2. 현재 DS TTL을 찾습니다.

   DS TTL은 다음 Unix 명령을 실행하여 찾을 수 있습니다.

   ```
   dig -t DS example.com example.com
   ```
3. 최대 NS TTL을 찾습니다.

영역과 관련된 NS 레코드에는 2가지 세트가 있습니다.

- 위임 NS 레코드 - 상위 영역이 보유한 영역에 대한 NS 레코드입니다. 이 레코드는 다음 Unix 명령을 실행하여 찾을 수 있습니다.

  먼저 상위 영역의 NS를 찾습니다(영역이 example.com인 경우 상위 영역은 com).

  ```
  dig -t NS com
  ```

  NS 레코드 중 하나를 선택한 후 다음을 실행합니다.

  ```
  dig @one of the NS records of your parent zone -t NS example.com
  ```

  예:

  ```
  dig @b.gtld-servers.net. -t NS example.com
  ```

- 영역 내 NS 레코드 - 이것은 영역에 있는 NS 레코드입니다. 이 레코드는 다음 Unix 명령을 실행하여 찾을 수 있습니다.

  ```
  dig @one of the NS records of your zone -t NS example.com
  ```

  예:

  ```
  dig @ns-0000.awsdns-00.co.uk. -t NS example.com
  ```

  두 영역 모두에 대한 최대 TTL을 확인합니다.

4. 상위 영역에서 DS 레코드를 제거합니다.

   상위 영역 소유자에게 연락하여 DS 레코드를 제거하도록 합니다.

   롤백: DS 레코드를 다시 삽입하고 DS 삽입이 효과가 있는지 확인한 다음 모든 해석기가 다시 검증을 시작할 때까지 최대 NS(DS가 아님) TTL 동안 기다립니다.

5. DS 제거의 효과가 적용되었는지 확인합니다.

   상위 영역이 Route 53 DNS 서비스에 있는 경우, 상위 영역 소유자는 GetChange API를 통해 전파 완료를 확인할 수 있습니다.

   그렇지 않으면 DS 레코드의 상위 영역을 주기적으로 조사한 다음 DS 레코드 제거가 완전히 전파될 확률을 높일 수 있도록 10분 더 기다릴 수 있습니다. 일부 등록 기관은 일정(예: 하루에 한 번)에 따라 DS 제거를 수행합니다.

6. DS TTL 동안 기다립니다.

   모든 해석기의 캐시에서 DS 레코드가 만료될 때까지 기다립니다.

7. DNSSEC 서명을 비활성화하고 KSK(키 서명 키)를 비활성화합니다.

   - CLI
   - 콘솔

   CLI

   DisableHostedZoneDNSSEC 및 DeactivateKeySigningKey API를 호출합니다.

   예:

```
aws --region us-east-1 route53 disable-hosted-zone-dnssec \
            --hosted-zone-id $hostedzone_id

aws --region us-east-1 route53 deactivate-key-signing-key \
            --hosted-zone-id $hostedzone_id --name $ksk_name
```

   Console

   DNSSEC 서명을 비활성화하려면

   1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
   2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택한 후 DNSSEC 서명을 비활성화할 호스팅 영역을 선택합니다.
   3. DNSSEC 서명(DNSSEC signing) 탭에서 DNSSEC 서명 비활성화(Disable DNSSEC signing)를 선택합니다.
   4. DNSSEC 서명 비활성화(Disable DNSSEC signing) 페이지에서 DNSSEC 서명을 비활성화하려는 영역의 시나리오에 따라 다음 옵션 중 하나를 선택합니다.
      - 상위 영역만(Parent zone only) - 이 영역에는 DS 레코드가 있는 상위 영역이 있습니다. 이 시나리오에서는 상위 영역의 DS 레코드를 제거해야 합니다.

- 하위 영역만(Child zones only) - 이 영역에는 하나 이상의 하위 영역이 있는 신뢰 체인에 대한 DS 레코드가 있습니다. 이 시나리오에서는 해당 영역의 DS 레코드를 제거해야 합니다.
- 상위 및 하위 영역(Parent and child zones) - 이 영역에는 하나 이상의 하위 영역이 있는 신뢰 체인에 대한 DS 레코드 및 DS 레코드가 있는 상위 영역 모두 다 있습니다. 이 시나리오의 경우 다음을 순서대로 수행합니다.

  a. 해당 영역의 DS 레코드를 제거합니다.

  b. 상위 영역의 DS 레코드를 제거합니다.

  신뢰 영역이 있는 경우 이 단계를 건너뛰어도 됩니다.

5. 4단계에서 제거한 각 DS 레코드에 대해 TTL이 무엇인지 확인하고, 가장 긴 TTL 기간이 만료되었는지 확인합니다.
6. 단계를 순서대로 수행했음을 확인하는 확인란을 선택합니다.
7. 표시된 대로 필드에 disable을 입력한 다음 비활성화(Disable)를 선택합니다.

KSK(키 서명 키)를 비활성화하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택한 후 KSK(키 서명 키)를 비활성화할 호스팅 영역을 선택합니다.
3. KSK(키 서명 키)(Key-signing keys (KSKs)) 섹션에서 비활성화할 KSK를 선택한 다음 작업(Actions)에서 KSK 편집(Edit KSK)을 선택하고 KSK 상태(KSK status)를 비활성(Inactive)로 설정한 다음 KSK 저장(Save KSK)을 선택합니다.

롤백: ActivateKeySigningKey 및 EnableHostedZoneDNSSEC API를 호출합니다.

예:

```
aws --region us-east-1 route53 activate-key-signing-key \
            --hosted-zone-id $hostedzone_id --name $ksk_name

aws --region us-east-1 route53 enable-hosted-zone-dnssec \
            --hosted-zone-id $hostedzone_id
```

8. 영역 서명 비활성화의 효과가 적용되었는지 확인합니다.

   GetChange 실행을 위한 `EnableHostedZoneDNSSEC()` 호출의 ID를 사용하여 모든 Route 53 DNS 서버가 응답 서명을 중지했는지 확인합니다(상태 =`INSYNC`).

9. 이름 확인을 관찰합니다.

   해석기가 영역의 유효성을 검사하는 데 문제가 없음을 확인해야 합니다. 고객이 문제를 보고하는 데 필요한 시간도 고려하도록 1~2주의 시간을 허용합니다.

10. (선택 사항) 정리.

    서명을 다시 활성화하지 않을 것이라면 DeleteKeySigningKey를 통해 KSK를 정리하고 해당 고객 관리형 키를 삭제하여 비용을 절감할 수 있습니다.

DNSSEC용 고객 관리형 키 작업

Amazon Route 53에서 DNSSEC 서명을 활성화하면 Route 53에서 키 서명 키(KSK)를 생성합니다. KSK를 생성하려면 Route 53에서 DNSSEC를 지원하는의 고객 관리 AWS Key Management Service 형 키를 사용해야 합니다. 이 섹션에서는 DNSSEC로 작업할 때 도움이 되는 고객 관리형 키의 세부 사항 및 요구 사항에 대해 설명합니다.

DNSSEC에 대한 고객 관리형 키로 작업하는 경우 다음 사항에 유의하세요.

- DNSSEC 서명에서 사용하는 고객 관리형 키는 미국 동부 (버지니아 북부) 리전에 있어야 합니다.
- 고객 관리형 키는 ECC_NIST_P256 키 사양의 비대칭 관리형 키여야 합니다. 이러한 고객 관리형 키는 서명 및 확인에만 사용됩니다. 비대칭 고객 관리형 키를 생성하는 데 도움이 필요하면 AWS Key Management Service 개발자 안내서의 비대칭 고객 관리형 키 생성을 참조하세요. 기존 고객 관리형 키의 암호화 구성을 찾는 데 도움이 필요하면 AWS Key Management Service 개발자 안내서의 고객 관리형 키의 암호화 구성 보기를 참조하세요.
- Route 53에서 DNSSEC와 함께 사용할 고객 관리형 키를 직접 생성하는 경우 Route 53에 필요한 권한을 부여하는 특정 키 정책 설명을 포함해야 합니다. Route 53는 고객 관리형 키에 액세스할 수 있어야 KSK를 생성할 수 있습니다. 자세한 내용은 DNSSEC 서명에 필요한 Route 53 고객 관리형 키 권한 단원을 참조하십시오.
- Route 53는 추가 AWS KMS 권한 없이 DNSSEC 서명과 함께 사용할 수 AWS KMS 있는 고객 관리형 키를 생성할 수 있습니다. 그러나 키를 만든 후 편집하려면 특정 권한이 있어야 합니다. 필요한 특

정 사용 권한은 `kms:UpdateKeyDescription`, `kms:UpdateAlias` 및 `kms:PutKeyPolicy`와 같습니다.

- 고객 관리형 키를 직접 생성하든 Route 53에서 생성하든 관계없이 보유한 각 고객 관리형 키에 대해 별도의 요금이 부과됩니다. 자세한 내용은 AWS Key Management Service 요금을 참조하세요.

KSK(키 서명 키)로 작업

DNSSEC 서명을 활성화하면 Route 53에서 KSK(키 서명 키)를 생성합니다. Route 53에는 호스팅 영역당 최대 2개의 KSK가 있을 수 있습니다. DNSSEC 서명을 활성화한 후 KSK를 추가, 제거 또는 편집할 수 있습니다.

KSK로 작업할 때는 다음 사항에 유의하세요.

- KSK를 삭제하려면 먼저 KSK를 편집하여 KSK 상태를 비활성으로 설정해야 합니다.
- 호스팅 영역에 대해 DNSSEC 서명을 사용하면 Route 53가 TTL을 1주일로 제한합니다. 호스팅 영역의 레코드에 대해 TTL을 1주일 이상으로 설정하면 오류가 발생하지 않지만 Route 53에서는 TTL을 1주일로 실행합니다.
- 영역 중단을 방지하고 도메인을 사용할 수 없게 되는 문제를 방지하려면 DNSSEC 오류에 신속하게 대응하고 해결해야 합니다. `DNSSECInternalFailure` 또는 `DNSSECKeySigningKeysNeedingAction` 오류를 감지할 때마다 알림이 전송되도록 CloudWatch 경보를 설정하는 것이 좋습니다. 자세한 내용은 Amazon CloudWatch를 사용하여 호스팅 영역 모니터링 섹션을 참조하세요.
- 이 섹션에서 설명하는 KSK 작업을 통해 영역의 KSK를 대체할 수 있습니다. 자세한 내용 및 단계별 예제에 대해서는 블로그 게시물 Amazon Route 53로 DNSSEC 서명 및 유효성 검사 구성에서 DNSSEC 키 교체를 참조하세요.

에서 KSKs를 사용하려면 다음 섹션의 지침을 AWS Management Console따르세요.

KSK(키 서명 키) 추가

DNSSEC 서명을 활성화하면 Route 53에서 KSK(키 서명 키)를 생성합니다. KSK를 별도로 추가할 수도 있습니다. Route 53에는 호스팅 영역당 최대 2개의 KSK가 있을 수 있습니다.

KSK를 생성하는 경우 KSK와 함께 사용할 고객 관리 고객 관리형 키를 만들려면 Route 53를 제공하거나 요청해야 합니다. 고객 관리형 키를 제공하거나 만드는 경우 몇 가지 요구 사항이 있습니다. 자세한 내용은 DNSSEC용 고객 관리형 키 작업 단원을 참조하십시오.

AWS Management Console에 KSK를 추가하려면 다음 단계를 따르세요.

KSK를 추가하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역을 선택한 후 호스팅 영역을 선택합니다.
3. KSK(키 서명 키)(Key-signing keys (KSKs))의 DNSSEC 서명(DNSSEC signing) 탭에서 고급 보기로 전환(Switch to advanced view)을 선택한 다음 작업(Actions)에서 KSK 추가(Add KSK)를 선택합니다.
4. KSK에 Route 53에서 생성할 KSK의 이름을 입력합니다. 이름에는 숫자, 문자, 밑줄(_)이 포함될 수 있습니다. 이름은 고유해야 합니다.
5. DNSSEC 서명에 적용되는 고객 관리형 키의 별칭을 입력하거나 Route 53에서 생성할 새 고객 관리형 키의 별칭을 입력합니다.

   > **Note**
   >
   > Route 53에서 고객 관리형 키를 만들도록 선택한 경우 고객 관리형 키마다 별도의 요금이 부과됩니다. 자세한 내용은 AWS Key Management Service 요금을 참조하세요.

6. KSK 생성을 선택합니다.

KSK(키 서명 키) 편집

KSK의 상태를 활성 또는 비활성으로 편집할 수 있습니다. KSK가 활성화되면 Route 53에서는 DNSSEC 서명에 해당 KSK를 사용합니다. KSK를 삭제하려면 먼저 KSK를 편집하여 KSK 상태를 비활성으로 설정해야 합니다.

AWS Management Console에 KSK를 추가하려면 다음 단계를 따르세요.

태그를 편집하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역을 선택한 후 호스팅 영역을 선택합니다.
3. DNSSEC 서명(DNSSEC signing) 탭의 KSK(키 서명 키)(Key-signing keys (KSKs))에서 고급 보기로 전환(Switch to advanced view)을 선택한 다음, 작업(Actions)에서 KSK 편집(Edit KSK)을 선택합니다.
4. KSK를 원하는 대로 업데이트한 다음 저장을 선택합니다.

KSK(키 서명 키) 삭제

KSK를 삭제하려면 먼저 KSK를 편집하여 KSK 상태를 비활성으로 설정해야 합니다.

KSK를 삭제할 수 있는 이유 중 하나는 일상적인 키 교체의 일부이기 때문입니다. 암호화 키를 주기적으로 교체하는 것이 가장 좋습니다. 조직에 키를 교체하는 빈도에 대한 표준 지침이 있을 수 있습니다.

AWS Management Console에서 KSK를 삭제하려면 다음 단계를 따르세요.

KSK를 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역을 선택한 후 호스팅 영역을 선택합니다.
3. KSK(키 서명 키)(Key-signing keys (KSKs))의 DNSSEC 서명(DNSSEC signing) 탭에서 고급 보기로 전환(Switch to advanced view)을 선택한 다음, 작업(Actions)에서 KSK 삭제(Delete KSK)을 선택합니다.
4. 지침에 따라 KSK 삭제를 확인합니다.

Route 53에서의 KMS 키 및 ZSK 관리

이 섹션에서는 DNSSEC 서명 활성화 영역에 대해 Route 53가 사용하는 현재 방법을 설명합니다.

> **Note**
>
> Route 53는 변경될 수 있는 다음 규칙을 사용합니다. 향후 변경으로 인해 영역 또는 Route 53의 보안 태세가 줄어들지 않습니다.

Route 53가 KSK와 AWS KMS 연결된를 사용하는 방법

DNSSEC에서 KSK는 DNSSKEY 리소스 레코드 세트에 대한 리소스 레코드 서명(RRSIG)을 생성하는 데 사용됩니다. 모든 `ACTIVE` KSK는 RRSIG 세대에서 사용됩니다. Route 53는 연결된 KMS 키에서 `Sign` AWS KMS API를 호출하여 RRSIG를 생성합니다. 자세한 내용은 AWS KMS API 가이드의 서명을 참조하세요. 이러한 RRSIG는 영역의 리소스 레코드 세트 제한에 포함되지 않습니다.

RRSIG가 만료되었습니다. RRSIG가 만료되는 것을 방지하기 위해 RRSIG를 1일에서 7일마다 다시 생성하여 정기적으로 새로 고칩니다.

또한 다음 API를 호출할 때마다 RRSIG가 새로 고쳐집니다.

- ActivateKeySigningKey
- CreateKeySigningKey
- DeactivateKeySigningKey
- DeleteKeySigningKey
- DisableHostedZoneDNSSEC
- EnableHostedZoneDNSSEC

Route 53가 새로 고침을 수행할 때마다 관련 KMS 키에 액세스할 수 없게 되는 경우를 대비하여 향후 며칠을 처리하기 위해 15개의 RRSIG를 생성합니다. KMS 키 비용 추정을 위해 하루에 한 번 정기적으로 새로 고침한다고 가정할 수 있습니다. KMS 키 정책을 실수로 변경하면 KMS 키에 액세스하는 것이 어려울 수 있습니다. 액세스할 수 없는 KMS 키는 연결된 KSK의 상태를 `ACTION_NEEDED`로 설정합니다. 마지막 RRSIG가 만료된 후 검증 확인자가 조회에 실패하기 때문에 `DNSSECKeySigningKeysNeedingAction` 오류가 감지될 때에는 CloudWatch 경보를 설정하여 이 상태를 모니터링하는 것이 좋습니다. 자세한 내용은 Amazon CloudWatch를 사용하여 호스팅 영역 모니터링 단원을 참조하십시오.

Route 53가 영역의 ZSK를 관리하는 방법

DNSSEC 서명이 활성화된 각 새 호스팅 영역에는 하나의 `ACTIVE` 영역 서명 키(ZSK)가 있습니다. ZSK는 각 호스팅 영역에 대해 별도로 생성되며 Route 53가 소유합니다. 현재 키 알고리즘은 ECDSAP256SHA256입니다.

서명 시작 후 7~30일 이내에 영역에서 정기적으로 ZSK 회전을 수행하기 시작합니다. 현재 Route 53는 사전 게시 키 롤오버 방법을 사용합니다. 자세한 내용은 사전 게시 영역 서명 키 롤오버 단원을 참조하세요. 이 방법은 영역에 다른 ZSK를 도입합니다. 회전은 7~30일마다 반복됩니다.

Route 53는 영역의 ZSK의 변경 사항을 설명하기 위해 DNSKEY 리소스 레코드 세트에 대한 RRSIG를 다시 생성할 수 없기 때문에 영역의 KSK가 `ACTION_NEEDED` 상태인 경우 Route 53는 ZSK 회전을 일시 중단합니다. 조건이 지워지면 ZSK 회전이 자동으로 재개됩니다.

Route 53에서 존재하지 않는다는 DNSSEC 증명

> **Note**
>
> Route 53는 변경될 수 있는 다음 규칙을 사용합니다. 향후 변경으로 인해 영역 또는 Route 53의 보안 태세가 줄어들지 않습니다.

DNSSEC에는 세 가지 종류의 존재하지 않는다는 증거가 있습니다.

- 쿼리 이름과 일치하는 레코드가 존재하지 않는다는 증거.
- 쿼리 유형과 일치하는 유형이 존재하지 않는다는 증거.
- 응답으로 레코드를 생성하는 데 사용되는 와일드카드 레코드가 존재하지 않는다는 증거.

Route 53는 BL 메서드를 사용하여 쿼리 이름과 일치하는 레코드가 존재하지 않는다는 증거를 구현합니다. 자세한 내용은 BL 단원을 참조하세요. 이는 증거를 컴팩트하게 표현하고 영역 둘러보기를 방지하는 방법입니다.

쿼리 유형이 아닌 쿼리 이름과 일치하는 레코드가 있는 경우(예: web.example.com/AAAA에 대해 쿼리하지만 web.example.com/A만 있는 경우) 지원되는 모든 리소스 레코드 유형을 포함하는 최소 NSEC(다음 보안) 레코드를 반환합니다.

Route 53가 와일드카드 레코드의 응답을 합성할 경우, 응답은 다음 보안 레코드인 와일드카드에 대한 NSEC 레코드와 함께 제공되지 않습니다. 이러한 NSEC 레코드는 응답의 리소스 레코드 서명(RRSIG)이 다른 응답을 스푸핑하는 데 재사용되는 것을 방지하기 위해 일반적으로 오프라인 서명을 수행하는 일부 구현에서 사용됩니다. Route 53는 non-DNSKEY 레코드의 온라인 서명을 사용하여 다른 응답에 재사용할 수 없는 응답으로 특정된 RRSIG를 생성합니다.

DNSSEC 서명 문제 해결

이 섹션의 정보는 활성화, 비활성화, KSK(키 서명 키)를 포함하여 DNSSEC 서명 문제를 해결하는 데 도움이 될 수 있습니다.

DNSSEC 활성화

DNSSEC 서명을 활성화하기 전에 Amazon Route 53에서 DNSSEC 서명 구성에서 사전 조건을 읽어야 합니다.

DNSSEC 비활성화

DNSSEC를 안전하게 비활성화하기 위해 Route 53는 대상 영역이 신뢰 체인에 속하는지 확인합니다. 대상 영역의 상위 영역에 대상 영역의 NS 레코드와 대상 영역의 DS 레코드가 있는지 확인합니다. 대상 영역을 공개적으로 확인할 수 없는 경우(예: NS 및 DS를 쿼리할 때 SERVFAIL 응답을 받음) Route 53는 DNSSEC를 비활성화해도 안전한지 여부를 판단할 수 없습니다. 상위 영역에 확인하여 해결한 다음에 DNSSEC를 다시 비활성화해 볼 수 있습니다.

KSK 상태가 Action needed(작업 필요)인 경우

Route 53 DNSSEC가 해당 ACTION_NEEDED에 대한 액세스 권한을 잃을 때(권한 변경 또는 AWS KMS key 삭제로 인해) KSK의 상태를 필요한 작업 AWS KMS key (또는 KeySigningKey 상태)으로 변경할 수 있습니다.

KSK의 상태가 작업 필요(Action needed)인 경우는 DNSSEC 검증 해석기를 사용하는 클라이언트에 영역 가동 중단이 발생함을 의미하므로 프로덕션 영역을 확인되지 않는 상황을 방지할 수 있도록 신속하게 조치를 취해야 합니다.

이 문제를 해결하려면 KSK가 기반으로 하는 고객 관리형 키가 활성화되었으며 올바른 권한이 있는지 확인하세요. 필요한 권한에 대한 자세한 정보는 DNSSEC 서명에 필요한 Route 53 고객 관리형 키 권한 단원을 참조하세요.

KSK를 수정한 후에 설명된 AWS CLI대로 콘솔 또는를 사용하여 다시 활성화합니다2단계: DNSSEC 서명 활성화 및 KSK 생성.

향후이 문제를 방지하려면 Amazon CloudWatch 에 제안된 대로 지표를 추가하여 KSK의 상태를 추적하는 것이 좋습니다Amazon Route 53에서 DNSSEC 서명 구성.

KSK 상태가 내부 오류(Internal failure)인 경우

KSK의 상태가 내부 오류(Internal failure)(또는 KeySigningKey 상태가 INTERNAL_FAILURE)인 경우, 문제가 해결될 때까지 다른 DNSSEC 엔터티에서 작업할 수 없습니다. 이 KSK 또는 다른 KSK로 작업하는 것을 포함하여 DNSSEC 서명으로 작업하려면 먼저 조치를 취해야 합니다.

문제를 해결하려면 KSK를 다시 활성화하거나 비활성화합니다.

문제를 해결하려면 API로 작업할 때 서명 활성화(EnableHostedZoneDNSSEC) 또는 서명 비활성화(DisableHostedZoneDNSSEC)를 시도합니다.

내부 오류(Internal failure) 문제는 신속하게 해결해야 합니다. 문제를 해결하기 전까지는 호스팅 영역을 변경할 수 없습니다. 단, 내부 오류(Internal failure) 수정 작업은 예외로 합니다.

AWS Cloud Map 를 사용하여 레코드 및 상태 확인 생성

인터넷 트래픽이나 Amazon VPC 내부의 트래픽을 애플리케이션 구성 요소 또는 마이크로서비스로 라우팅하려면 AWS Cloud Map 을 사용하여 레코드를 자동으로 생성하고 선택적으로 상태 확인을 생성할 수 있습니다. 자세한 내용은 AWS Cloud Map 개발자 안내서를 참조하세요.

DNS 제한 및 동작

DNS 메시징은 호스팅 영역 및 레코드를 생성하고 사용하는 방식에 영향을 미치는 요인들에 의해 제한을 받습니다. 이 섹션에서는 이러한 요인들에 대해 알아봅니다.

최대 응답 크기

DNS 표준을 따르기 위해, UDP를 거쳐 전송되는 응답의 크기는 512바이트를 넘지 않습니다. 512바이트를 초과하는 응답들은 중간에 잘리게 되므로 해석기가 반드시 TCP를 거쳐 요청을 재발행해야 합니다. RFC 2671에 정의된 대로 Resolver가 EDNS0을 지원하고 EDNS0 옵션을 Amazon Route 53에 알린다면, Route 53는 잘림 없이 UDP를 거쳐 4,096바이트까지 응답을 허용합니다.

권한 섹션 처리

성공적인 쿼리를 위해 Route 53는 DNS 응답의 권한 섹션에 해당 호스팅 영역에 대한 이름 서버(NS) 레코드를 추가합니다. 찾을 수 없는 이름(NXDOMAIN 응답)의 경우 Route 53는 DNS 응답의 권한 섹션에 해당 호스팅 영역에 대한 권한 시작(SOA) 레코드(RFC 1035에 정의됨)를 추가합니다.

추가 섹션 처리

Route 53는 추가 섹션에 레코드를 추가합니다. 레코드가 알려져 있고 적절하다면, 서비스는 응답 섹션에 인용된 MX, CNAME, NS, 또는 SRV 레코드의 어떤 대상에 대해서라도 A 또는 AAAA 레코드를 추가합니다. 이 DNS 레코드 유형에 대한 자세한 내용은 다음(지원되는 DNS 레코드 유형)을 참조하십시오.

트래픽 흐름을 사용하여 DNS 트래픽 라우팅

트래픽 흐름은 크고 복잡한 구성에서 레코드를 생성하고 유지 관리하는 프로세스를 대폭 간소화합니다.

호스팅 영역에서 관련 레코드를 관리하는 것은 다음과 같은 상황에서 어려울 수 있습니다.

- 동일한 도메인에 대한 트래픽을 제공하는 웹 서버와 같이 동일한 작업을 수행하는 리소스가 많이 있습니다.
- 별칭 레코드와 Route 53 라우팅 정책 조합(예: 지연 시간, 장애 조치 및 가중치 기반)을 사용하여 복잡한 레코드 트리를 생성하려고 합니다.

트래픽 흐름의 이점

레코드와 해당 관계를 더 쉽게 추적할 수 있도록 트래픽 흐름은 다음 기능을 사용하여 DNS 레코드 생성을 간소화합니다.

Visual editor(시각적 편집기)

트래픽 흐름 시각적 편집기를 사용하면 레코드의 복잡한 트리를 생성하고 레코드 간의 관계를 볼 수 있습니다. 예를 들어 지연 시간 별칭 레코드가 가중치 기반 레코드를 참조하고 가중치 기반 레코드가 여러 AWS 리전의 리소스를 참조하는 구성을 생성할 수 있습니다. 각 구성을 트래픽 정책이라고 합니다. 트래픽 정책은 원하는 만큼 무료로 생성할 수 있습니다.

버전 관리

여러 버전의 트래픽 정책을 만들 수 있으므로 구성이 변경될 때 처음부터 다시 시작할 필요가 없습니다. 이전 버전은 삭제할 때까지 계속 존재합니다. 트래픽 정책당 버전 1000까지 기본 제한이 있습니다. 선택적으로 각 버전에 설명을 지정할 수 있습니다.

자동 레코드 생성 및 업데이트

트래픽 정책은 수십 개 또는 수백 개의 레코드를 나타낼 수 있습니다. 트래픽 흐름을 사용하면 트래픽 정책 레코드를 생성하여 이러한 모든 레코드를 자동으로 생성할 수 있습니다. 트리의 루트에 호스팅 영역과 레코드 이름(예: example.com 또는 www.example.com)을 지정하면 Route 53가 트리에 다른 모든 레코드를 자동으로 생성합니다. 루트 레코드(트래픽 정책 레코드)는 호스팅 영역에 대한 레코드 목록에 표시되며, 다른 레코드는 모두 숨겨집니다.

새 버전의 트래픽 정책을 만들 때 이전 트래픽 정책 버전을 사용하여 생성한 트래픽 정책 레코드를 선택적으로 업데이트할 수 있습니다. 트래픽 정책 레코드를 업데이트하면 Route 53는 트리의 다른

모든 레코드를 자동으로 업데이트합니다. 또한 이전 버전의 트래픽 정책을 사용하려면 트래픽 정책 레코드를 다시 업데이트하여 변경 내용을 신속하게 롤백할 수 있습니다.

> **Note**
>
> 트래픽 흐름을 사용하여 퍼블릭 호스팅 영역에서만 레코드를 생성할 수 있습니다.

지리 근접 라우팅 정책

트래픽 흐름을 사용할 때 트래픽 흐름 시각적 캔버스의 지리 근접성 맵을 사용하여 트래픽이 각 글로벌 엔드포인트로 라우팅되는 방법을 보다 직관적으로 이해할 수 있습니다. 자세한 내용은 지리 근접 라우팅 단원을 참조하십시오.

서로 다른 호스팅 영역에서 여러 레코드에 재사용

트래픽 정책을 사용하여 여러 퍼블릭 호스팅 영역에서 레코드를 자동으로 생성할 수 있습니다. 예를 들어 여러 도메인 이름에 동일한 웹 서버를 사용하는 경우, 동일한 트래픽 정책을 사용하여 호스팅 영역에서 example.com, example.org 및 example.net에 대한 트래픽 정책 레코드를 생성할 수 있습니다.

클라이언트가 example.com 또는 www.example.com과 같은 루트 레코드의 이름에 대한 쿼리를 제출하면 Route 53는 해당 트래픽 정책 레코드를 생성하는 데 사용한 트래픽 정책의 구성을 기반으로 쿼리에 응답합니다.

각 트래픽 정책 레코드에 대해 월별 요금이 발생합니다. 자세한 내용은 Amazon Route 53 요금의 “트래픽 흐름” 섹션을 참조하십시오.

이러한 요금을 최소화하기 위해 호스팅 영역에서 해당 호스팅 영역의 트래픽 정책 레코드를 참조하는 하나 이상의 별칭 레코드를 생성할 수 있습니다. 예를 들어 example.com에 대한 트래픽 정책 레코드를 생성한 다음 트래픽 정책 레코드를 참조하는 www.example.com에 대한 별칭 레코드를 생성할 수 있습니다.

트래픽 정책 만들기 및 관리

주제

- 트래픽 정책 만들기
- 트래픽 정책을 만들 때 지정하는 값

- 지리 근접 설정의 효과를 볼 수 있는 지도 보기
- 트래픽 정책의 추가 버전 만들기
- JSON 문서를 가져와서 트래픽 정책 만들기
- 트래픽 정책 버전 및 연결된 정책 레코드 보기
- 트래픽 정책 버전 및 트래픽 정책 삭제

트래픽 정책 만들기

트래픽 정책을 만들려면 다음 절차를 수행하십시오.

트래픽 정책을 만들려면

1. 구성을 설계합니다. 복잡한 DNS 라우팅 구성이 작동하는 방법에 대한 자세한 내용은 DNS 장애 조치 구성 in Amazon Route 53 상태 확인 생성 단원을 참조하십시오.
2. 구성에 대한 설계를 기반으로 엔드포인트에 대해 사용할 상태 확인을 만듭니다.
3. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
4. 탐색 창에서 [Traffic policies]를 선택합니다.
5. [Create traffic policy]를 선택합니다.
6. [Name policy] 페이지에서 해당 값을 지정합니다. 자세한 내용은 트래픽 정책을 만들 때 지정하는 값 단원을 참조하십시오.
7. Next(다음)를 선택합니다.
8. Create traffic policy(트래픽 정책 생성) 정책 이름 v1 페이지에서 해당 값을 지정합니다. 자세한 내용은 트래픽 정책을 만들 때 지정하는 값 단원을 참조하십시오.

   다음과 같은 방법으로 트래픽 정책의 규칙, 엔드포인트 및 분기를 삭제할 수 있습니다.

   - 규칙 또는 엔드포인트를 삭제하려면 상자의 오른쪽 상단 모서리에서 [x]를 클릭합니다.

     > **Important**
     >
     > 하위 규칙 및 엔드포인트가 있는 규칙을 삭제할 경우 Amazon Route 53에서는 모든 하위 항목도 함께 삭제합니다.

   - 두 개의 규칙을 동일한 하위 규칙 또는 엔드포인트에 연결하고 연결 중 하나를 삭제하려면 삭제하려는 연결에 커서를 놓고 해당 연결에 대한 [x]를 클릭합니다.

9. [Create traffic policy]를 선택합니다.
10. 선택 사항: Create policy records with traffic policy(트래픽 정책으로 정책 레코드 생성) 페이지에서 새 트래픽 정책을 사용하여 하나의 호스팅 영역에서 하나 이상의 정책 레코드를 생성합니다. 자세한 내용은 정책 레코드의 생성 또는 업데이트 시 지정하는 값 단원을 참조하십시오. 나중에 동일 호스팅 영역 또는 추가 호스팅 영역에서 정책 레코드를 만들 수도 있습니다.

    지금 정책 레코드를 생성하지 않으려면 이 단계 건너뛰기를 선택하면 콘솔에 현재 AWS 계정을 사용하여 생성한 트래픽 정책 및 정책 레코드 목록이 표시됩니다.
11. 이전 단계에서 정책 레코드에 대한 설정을 지정한 경우 [Create policy record]를 선택합니다.

트래픽 정책을 만들 때 지정하는 값

트래픽 정책을 만들 때 다음 값을 지정합니다.

-
-
-
-
-
-
-

정책 이름

트래픽 정책을 설명하는 이름을 입력합니다. 이 값은 콘솔의 트래픽 정책 목록에 표시됩니다. 트래픽 정책을 만든 후에는 해당 이름을 변경할 수 없습니다.

버전

이 값은 트래픽 정책이나 기존 정책의 새 버전을 생성할 때 Amazon Route 53에서 자동으로 할당됩니다.

버전 설명

이 버전의 트래픽 정책에 적용되는 설명을 입력합니다. 이 값은 콘솔의 트래픽 정책 버전 목록에 표시됩니다.

DNS 유형

이 트래픽 정책 버전을 사용하여 정책 레코드를 생성할 때 Amazon Route 53에서 모든 레코드에 할당하게 할 DNS 유형을 선택합니다. 지원되는 유형 목록은 지원되는 DNS 레코드 유형 단원을 참조하십시오.

> **Important**
>
> 기존 트래픽 정책의 새 버전을 만들 경우 DNS 유형을 변경할 수 있습니다. 하지만 정책 레코드를 편집하고 정책 레코드를 만드는 데 사용한 트래픽 정책 버전과 다른 DNS 유형을 가진 트래픽 정책 버전을 선택할 수 없습니다. 예를 들어, [DNS type]이 A인 트래픽 정책 버전을 사용하여 정책 레코드를 만든 경우 정책 레코드를 편집하여 다른 [DNS type] 값을 가진 트래픽 정책 버전을 선택할 수 없습니다.

트래픽을 다음 AWS 리소스로 라우팅하려면 해당 값을 선택합니다.

- CloudFront 배포 — A: IPv4 형식의 IP 주소 또는 AAAA: IPv6 형식의 IP 주소)를 선택합니다.
- ELB Application Load Balancer - A: IPv4 형식의 IP 주소 또는 AAAA: IPv6 형식의 IP 주소를 선택합니다.
- ELB Classic Load Balancer - A: IPv4 형식의 IP 주소 또는 AAAA: IPv6 형식의 IP 주소를 선택합니다.
- ELB Network Load Balancer - A: IPv4 형식의 IP 주소 또는 AAAA: IPv6 형식의 IP 주소를 선택합니다.
- Elastic Beanstalk 환경: A: IPv4 형식의 IP 주소를 선택합니다.
- 웹 사이트 엔드포인트로 구성된 Amazon S3 버킷: A: IPv4 형식의 IP 주소(A: IP address in IPv4 format)를 선택합니다.

연결 대상

구성에 대한 설계를 기반으로 해당 규칙 또는 엔드포인트를 선택합니다.

장애 조치 규칙

가능한 경우 하나의 리소스가 모든 트래픽을 수용하고 첫 번째 리소스를 사용할 수 없을 때는 다른 리소스들이 모든 트래픽을 수용하는 액티브-패시브 장애 조치를 구성하고자 하는 경우에 이 옵션을 선택합니다.

자세한 내용은 액티브-패시브 장애 조치 단원을 참조하십시오.

지리 위치 규칙

Amazon Route 53가 사용자의 위치에 기반한 DNS 쿼리에 응답하기를 원하는 경우에 이 옵션을 선택합니다.

자세한 내용은 지리적 라우팅 단원을 참조하십시오.

[Geolocation rule]을 선택할 때는 요청이 시작되는 미국의 주 또는 국가도 선택합니다.

지연 규칙

여러 곳의 Amazon EC2 데이터 센터에 같은 기능을 수행하는 리소스들이 있고 Route 53가 최상의 지연 시간을 제공하는 리소스들로 DNS 쿼리에 응답하기를 원하는 경우에 이 옵션을 선택합니다.

지연 규칙을 선택할 때는 AWS 리전도 선택합니다.

자세한 내용은 지연 시간 기반 라우팅 단원을 참조하십시오.

지리 근접 규칙

Route 53가 리소스의 위치와 선택적으로 지정하는 바이어스를 기반으로 DNS 쿼리에 응답하도록 하려면 이 옵션을 선택합니다. 바이어스를 사용하면 더 많은 트래픽을 리소스와 주고 받을 수 있습니다.

[Geoproximity rule]을 선택하면 다음 값을 입력합니다.

엔드포인트 위치

해당되는 값을 선택합니다.

- 사용자 지정(좌표 입력) - 엔드포인트가 AWS 리소스가 아닌 경우 사용자 지정(좌표 입력)을 선택합니다.
- AWS 리전 - 엔드포인트가 AWS 리소스인 경우 리소스를 AWS 리전 생성한를 선택합니다.
- AWS 로컬 영역 - 엔드포인트가 AWS 리소스인 경우 리소스를 생성한 AWS 로컬 영역을 선택합니다.

AWS 로컬 영역을 사용하는 경우 먼저 활성화해야 합니다. 자세한 내용은 AWS Local Zones User Guide의 Getting started with Local Zones를 참조하세요.

사용 가능한 로컬 영역에 대해서는 AWS 로컬 영역 로케이션을 참조하세요.

AWS 리전 및 로컬 영역의 차이점에 대해 알아보려면 Amazon EC2 사용 설명서의 리전 및 영역을 참조하세요.

> **Important**
>
> 단일 지리 근접 라우팅 정책에는 동일한 대도시 지역 내에 지리적으로 위치한 두 개 이상의 위치가 포함될 수 없습니다.
> 또한 미국 서부(오레곤) AWS 리전 및 미국 포틀랜드와 같은 일부 및 로컬 영역은 동일한 지리 근접성 라우팅 정책 내에서 사용하기에는 서로 너무 가까운 위치에 있습니다.
> 동일한 대도시 지역 내 둘 이상의 위치로 트래픽을 라우팅해야 하는 경우 지역 내 서로 다른 두 엔드포인트에 대해 50/50 가중치 라우팅 규칙 (WRR) 을 적용하는 지리적 근접성 라우팅 정책을 정의하여 해당 엔드포인트 간에 트래픽을 균등하게 분배하세요.

Coordinates

엔드포인트 위치(Endpoint location)에 사용자 지정(좌표 입력)(Custom(enter coordinates))을 선택한 경우 리소스 위치의 위도와 경도를 입력합니다. 다음 사항에 유의하세요.

- 위도는 적도의 남쪽(음수) 또는 북쪽(양수) 위치를 나타냅니다. 유효한 값은 -90도 ~ 90도입니다.
- 경도는 본초 자오선의 서쪽(음수) 또는 동쪽(양수) 위치를 나타냅니다. 유효한 값은 -180도 ~ 180도입니다.
- 일부 온라인 매핑 애플리케이션에서 위도와 경도를 얻을 수 있습니다. 예를 들어 Google Maps에서 위치의 URL은 위도와 경도를 지정합니다.

  https://www.google.com/maps/@47.6086111,-122.3409953,20z
- 최대 두 자리 정밀도의 소수를 입력할 수 있습니다(예: 47.63). 더 정밀하게 값을 지정하는 경우 Route 53는 값을 소수점 이하 두 자리까지 자릅니다. 적도에서 위도와 경도의 경우 0.01도는 약 0.69마일입니다.

편향

Route 53가 트래픽을 리소스로 라우팅하는 지리적 리전의 크기를 선택적으로 변경하려면 바이어스(Bias)에 대해 해당하는 값을 지정합니다.

- Route 53가 트래픽을 리소스로 라우팅하는 지리적 리전의 크기를 확장하려면 바이어스에 대해 1~99의 양의 정수를 지정합니다. Route 53는 인접 리전의 크기를 축소합니다.
- Route 53가 트래픽을 리소스로 라우팅하는 지리적 리전의 크기를 축소하려면 바이어스에 대해 1~99의 음의 바이어스를 지정합니다. Route 53는 인접 리전의 크기를 확장합니다.

> **Important**
>
> 바이어스 값의 변동 효과는 거리를 기준으로 할 때처럼 절대적인 것이 아니라 다른 리소스의 위치를 기준으로 하기 때문에 상대적입니다. 그 결과, 변경 효과는 예측하기 어렵습니다. 예를 들어 리소스의 위치에 따라 바이어스를 10에서 15로 변경하면 뉴욕 대도시 구역에서 상당량의 트래픽을 늘리거나 빼는 것의 차이를 파악할 수 있습니다. 바이어스를 조금씩 일정하게 변경하고 결과를 평가한 다음 해당하는 경우 추가로 변경하는 것이 좋습니다.

자세한 내용은 지리 근접 라우팅 단원을 참조하십시오.

다중 응답 규칙

Route 53가 거의 무작위로 선택된 최대 8개의 정상 응답으로 DNS 쿼리에 응답하도록 하려면 이 옵션을 선택합니다.

자세한 내용은 다중값 응답 라우팅 단원을 참조하십시오.

가중치 기반 규칙

같은 기능을 수행하는 리소스가 여러 개(예: 같은 웹 사이트를 지원하는 여러 개의 웹 서버)이고 Route 53가 트래픽을 지정된 비율(예: 한 서버의 1/3 및 다른 서버의 2/3)에 따라 리소스에 라우팅할 경우에 이 옵션을 선택합니다.

가중치 법칙을 선택하면 이 규칙에 적용할 가중치를 입력합니다.

자세한 내용은 가중치 기반 라우팅 단원을 참조하십시오.

엔드포인트

DNS 쿼리를 라우팅할 리소스(예: CloudFront 배포 또는 Elastic Load Balancing 로드 밸런서)를 지정하려면 이 옵션을 선택합니다.

기존 규칙

이 트래픽 정책의 기존 규칙에 DNS 쿼리를 라우팅하려면 이 옵션을 선택합니다. 예를 들어, 서로 다른 여러 국가에 대한 쿼리를 동일한 장애 조치 규칙에 라우팅하는 두 개 이상의 지리 위치 규칙을 만들 수 있습니다. 그러면 장애 조치 규칙에서 쿼리를 두 개의 Elastic Load Balancing 로드 밸런서에 라우팅할 수 있습니다.

트래픽 정책에 포함된 규칙이 없는 경우에는 이 옵션을 사용할 수 없습니다.

기존 엔드포인트

DNS 쿼리를 기존 엔드포인트에 라우팅하려면 이 옵션을 선택합니다. 예를 들어 2개의 장애 조치 규칙이 있는 경우, On failover(장애 조치 중)(보조) 옵션 모두에 대한 DNS 쿼리를 동일한 Elastic Load Balancing 로드 밸런서로 라우팅하는 것이 좋습니다.

트래픽 정책에 포함된 엔드포인트가 없는 경우에는 이 옵션을 사용할 수 없습니다.

값 유형

다음 중 해당 옵션을 선택합니다.

CloudFront 배포

트래픽을 CloudFront 배포에 라우팅하려면 이 옵션을 선택합니다. 이 옵션은 DNS 유형에 대해 A: IPv4 형식의 IP 주소 또는 DNS 유형에 대해 AAAA: IPv6 형식의 IP 주소를 선택합니다.

ELB Application Load Balancers

트래픽을 Elastic Load Balancing Application Load Balancer로 라우팅하려면 이 옵션을 선택합니다. 이 옵션은 [A: IP address in IPv4 format] 또는 [AAAA: IP address in IPv6 format]을 [DNS type]으로 선택한 경우에만 사용할 수 있습니다.

ELB Classic Load Balancer

트래픽을 Elastic Load Balancing Classic Load Balancer로 라우팅하려면 이 옵션을 선택합니다. 이 옵션은 [A: IP address in IPv4 format] 또는 [AAAA: IP address in IPv6 format]을 [DNS type]으로 선택한 경우에만 사용할 수 있습니다.

ELB Network Load Balancer

트래픽을 Elastic Load Balancing Network Load Balancer로 라우팅하려면 이 옵션을 선택합니다. 이 옵션은 [A: IP address in IPv4 format] 또는 [AAAA: IP address in IPv6 format]을 [DNS type]으로 선택한 경우에만 사용할 수 있습니다.

Elastic Beanstalk 환경

트래픽을 Elastic Beanstalk 환경으로 라우팅하려면 이 옵션을 선택합니다. 이 옵션은 [A: IP address in IPv4 format]을 [DNS type]으로 선택한 경우에만 사용할 수 있습니다.

S3 웹 사이트 엔드포인트

웹 사이트 엔드포인트로 구성된 Amazon S3 버킷에 트래픽을 라우팅하려면 이 옵션을 선택합니다. 이 옵션은 [A: IP address in IPv4 format]을 [DNS type]으로 선택한 경우에만 사용할 수 있습니다.

유형 DNS type 값

Route 53에서 값(Value) 필드의 값을 사용하여 DNS 쿼리에 응답하게 하려면 이 옵션을 선택합니다. 예를 들어, 이 트래픽 정책을 만들 때 [A]를 [DNS type] 값으로 선택한 경우 [Value type] 목록의 이 옵션은 [Type A value]입니다. 따라서 IP 주소를 IPv4 형식으로 값(Value) 필드에 입력해야 합니다.. Route 53는 값필드의 IP 주소를 사용하여 이 엔드포인트에 라우팅되는 DNS 쿼리에 응답합니다.

값

값 입력에 대해 선택한 옵션을 기반으로 값을 선택하거나 입력합니다.

CloudFront 배포

현재 AWS 계정과 연결된 배포 목록에서 CloudFront 배포를 선택합니다.

ELB Application Load Balancers

현재 AWS 계정과 연결된 로드 밸런서 목록에서 Elastic Load Balancing Application 로드 밸런서를 선택합니다.

ELB Classic Load Balancer

현재 AWS 계정과 연결된 로드 밸런서 목록에서 Elastic Load Balancing Classic 로드 밸런서를 선택합니다.

ELB Network Load Balancer

현재 AWS 계정과 연결된 로드 밸런서 목록에서 Elastic Load Balancing Network 로드 밸런서를 선택합니다.

Elastic Beanstalk 환경

현재 AWS 계정과 연결된 환경 목록에서 Elastic Beanstalk 환경을 선택합니다.

S3 웹 사이트 엔드포인트

웹 사이트 엔드포인트로 구성되고 현재 AWS 계정과 연결된 Amazon S3 Amazon S3 버킷 목록에서 Amazon S3 버킷을 선택합니다.

> **Important**
>
> 트래픽 정책을 기반으로 정책 레코드를 생성하는 경우, 여기서 선택하는 버킷은 정책 레코드에서 Policy record DNS name에 대해 지정하는 도메인 이름(예: www.example.com)과

일치해야 합니다. 값(Value)과 정책 레코드 DNS 이름(Policy record DNS name)이 일치하지 않으면 Amazon S3는 도메인 이름에 대한 DNS 쿼리에 응답하지 않습니다.

유형 DNS type 값

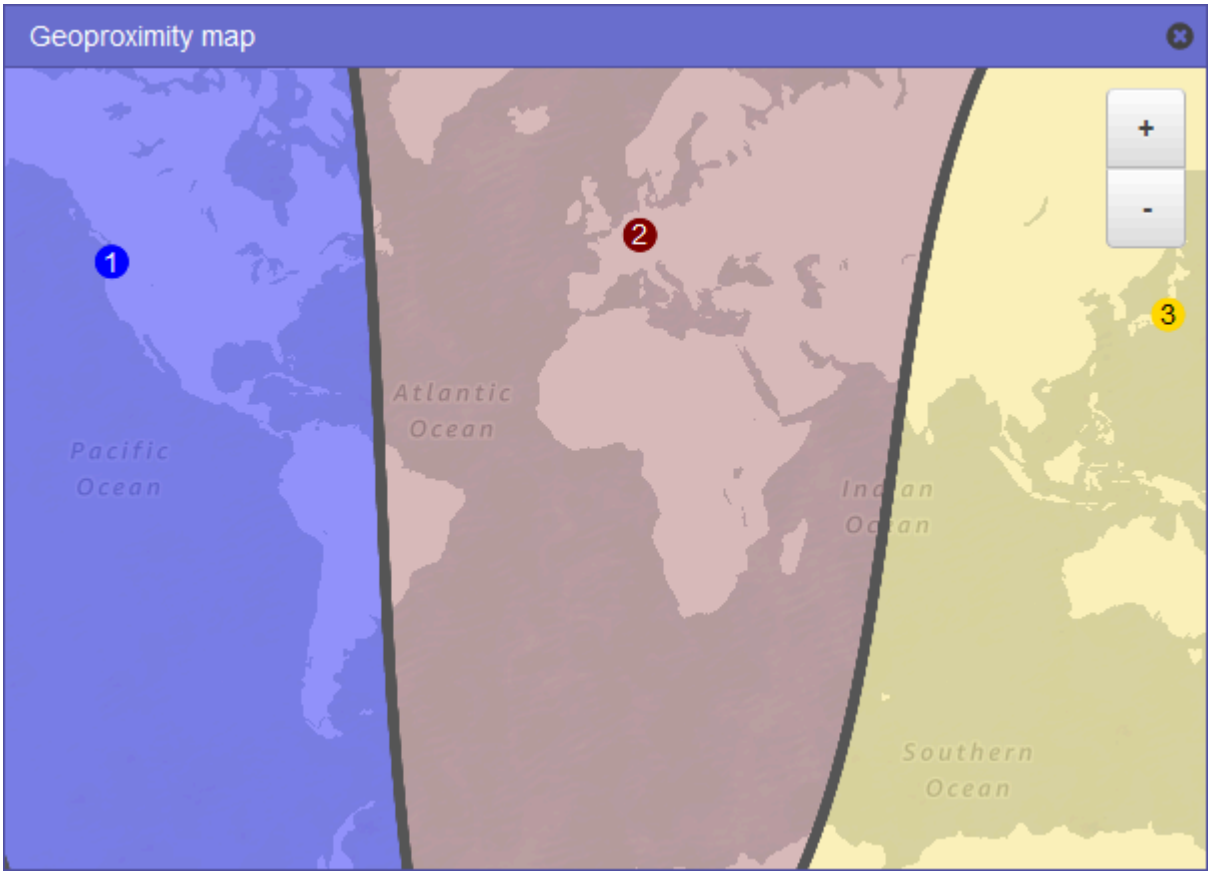
이 트래픽 정책을 시작할 때 [DNS type]에 대해 지정한 값과 일치하는 값을 입력합니다. 예를 들어, MX를 DNS 유형으로 선택한 경우 메일 서버에 할당할 우선 순위와 메일 서버의 도메인 이름(예: `10 sydney.mail.example.com`)의 두 값을 입력합니다.

지원되는 DNS 유형에 대한 자세한 내용은 지원되는 DNS 레코드 유형 단원을 참조하십시오.

지리 근접 설정의 효과를 볼 수 있는 지도 보기

지리 근접성 규칙을 사용하면 AWS 리전 또는 로컬 영역에서 리소스의 위치를 지정하고, 위도와 경도를 사용하여 위치가 아닌 곳에서 리소스의AWS 위치를 지정할 수 있습니다. 지리 근접 규칙을 생성하면 Route 53가 기본적으로 사용자와 가장 가까운 리소스로 인터넷 트래픽을 라우팅합니다. 트래픽이 리소스로 라우팅되는 지역을 확장하거나 축소하는 바이어스를 지정하여 리소스로 라우팅되는 트래픽을 늘리거나 줄일 수도 있습니다. 지리 근접 라우팅에 대한 자세한 내용은 지리 근접 라우팅 단원을 참조하십시오.

현재 지리 근접 설정의 효과를 볼 수 있는 지도를 표시할 수 있습니다. 예를 들어, 미국 서부(오레곤), 유럽(프랑크푸르트), 아시아 태평양(도쿄) 리전에 리소스가 있는데 바이어스를 지정하지 않은 경우에는 지도 모양이 다음과 같습니다.



지리 근접 규칙용 지도를 표시하려면 Show geoproximity map(지리 근접 지도 표시) 옆에 있는 그래프 아이콘을 선택합니다. (이 아이콘은 규칙 맨 위에 표시됩니다.) 지도를 숨길 때는 아이콘을 다시 선택하거나 지도의 오른쪽 상단 모서리에 있는 x를 선택합니다.

다음 사항에 유의하세요.

- 이 지도의 정확도는 약 16킬로미터(10마일)입니다.
- 리전을 추가, 편집 또는 삭제하거나 리전의 바이어스 설정을 변경하면 지도가 자동으로 조정됩니다.
- 각 규칙 정의에서 리전 번호와 색상은 지도 상의 번호와 색상에 해당합니다.
- 확대나 축소를 통해 표시되는 세부 정보를 늘리거나 줄일 수 있습니다. 지도 상의 + 및 - 버튼, 터치패드 또는 마우스 휠을 사용하여 확대/축소 수준을 변경합니다.
- 지도 창 안에서 지도를 움직여 특정 지역을 볼 수 있습니다. 터치패드를 사용하거나 마우스로 지도를 클릭 및 드래그합니다. 브라우저 창에서 지도 창을 움직일 수도 있습니다.
- 정책 안에 지리 근접 규칙이 둘 이상일 경우에는 한 번에 한 규칙의 지도만 볼 수 있습니다.

트래픽 정책의 추가 버전 만들기

트래픽 정책을 편집하면 Amazon Route 53에서 트래픽 정책의 다른 버전을 자동으로 만듭니다. 이전 버전은 삭제하도록 선택한 경우가 아니면 유지됩니다. 새 버전은 편집 중인 트래픽 정책과 이름이 동일하며, Route 53에서 자동으로 증가되는 버전 번호로 원본 버전과 구분됩니다. 동일한 이름을 가진 기존 버전의 트래픽 정책을 기반으로 새 버전의 트래픽 정책을 만들 수 있습니다.

Route 53에서는 지정된 트래픽 정책의 새 버전에 대해 버전 번호를 재사용하지 않습니다. 예를 들어, 세 버전의 [MyTrafficPolicy]를 만들고 마지막 두 버전을 삭제한 다음 다른 버전을 만들 경우 새 버전은 버전 4입니다. Route 53에서는 이전 버전을 유지하여 새 구성에서 트래픽을 원하는 대로 라우팅하지 않을 경우에 이전 구성으로 롤백할 수 있도록 해줍니다.

새 트래픽 정책 버전을 만들려면 다음 절차를 수행하십시오.

다른 버전의 트래픽 정책을 만들려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 [Traffic policies]를 선택합니다.
3. 새 버전을 만들 트래픽 정책의 이름을 선택합니다.
4. 페이지 상단에 있는 [Traffic policy versions] 테이블에서 새 트래픽 정책 버전에 대한 기반으로 사용할 트래픽 정책 버전에 대한 확인란을 선택합니다.
5. [Edit policy as new version]을 선택합니다.
6. Update description(설명 업데이트) 페이지에 새 트래픽 정책 버전에 대한 설명을 입력합니다. 이 버전을 동일한 트래픽 정책의 다른 버전과 구별하는 설명을 지정하는 것이 좋습니다. 새 정책 레코드를 만들 때 지정하는 값은 이 트래픽 정책에 대해 사용 가능한 버전 목록에 나타납니다.
7. Next(다음)를 선택합니다.
8. 해당하는 구성을 업데이트합니다. 자세한 내용은 트래픽 정책을 만들 때 지정하는 값 단원을 참조하십시오.

   다음과 같은 방법으로 트래픽 정책의 규칙, 엔드포인트 및 분기를 삭제할 수 있습니다.

   - 규칙 또는 엔드포인트를 삭제하려면 상자의 오른쪽 상단 모서리에서 [x]를 클릭합니다.

> **Important**
>
> 하위 규칙 및 엔드포인트가 있는 규칙을 삭제할 경우 Route 53에서는 모든 하위 항목도 함께 삭제합니다.

- 두 개의 규칙을 동일한 하위 규칙 또는 엔드포인트에 연결하고 연결 중 하나를 삭제하려면 삭제하려는 연결에 커서를 놓고 해당 연결에 대한 [x]를 클릭합니다.

9. 편집을 마치면 [Save as new version]을 선택합니다.
10. 선택 사항: 새 트래픽 정책 버전을 사용하여 한 호스팅 영역에서 하나 이상의 정책 레코드를 만들도록 설정을 지정합니다. 자세한 내용은 정책 레코드의 생성 또는 업데이트 시 지정하는 값 단원을 참조하십시오. 나중에 동일 호스팅 영역 또는 추가 호스팅 영역에서 정책 레코드를 만들 수도 있습니다.

    지금 정책 레코드를 생성하지 않으려면 이 단계 건너뛰기를 선택하면 콘솔에 현재 AWS 계정을 사용하여 생성한 트래픽 정책 및 정책 레코드 목록이 표시됩니다.
11. 이전 단계에서 정책 레코드에 대한 설정을 지정한 경우 [Create policy record]를 선택합니다.

JSON 문서를 가져와서 트래픽 정책 만들기

트래픽 정책에 포함할 모든 엔드포인트와 규칙을 설명하는 JSON 형식의 문서를 가져와서 새 트래픽 정책 또는 기존 트래픽 정책의 새 버전을 만들 수 있습니다. JSON 문서의 형식에 대한 자세한 내용과 복사 및 수정할 수 있는 몇 가지 예에 대해서는 Amazon Route 53 API 참조의 트래픽 정책 문서 형식을 참조하세요.

기존 트래픽 정책 버전의 JSON 형식 문서를 가져오는 가장 쉬운 방법은 AWS CLI에서 `get-traffic-policy` 명령을 사용하는 것입니다. 자세한 내용은 AWS CLI 명령 참조 안내서의 get-traffic-policy를 참조하세요.

`get-traffic-policy` 명령으로 생성된 JSON 파일에는 역방향 슬래시(\)가 이스케이프 문자로 포함됩니다. JSON 파일을 가져오기 전에 모든 역방향 슬래시를 null 문자로 교체합니다.

JSON 문서를 가져와서 트래픽 정책을 만들려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. JSON 문서를 가져와서 새 트래픽 정책을 만들려면 다음 단계를 수행하십시오.

a. 탐색 창에서 [Traffic policies]를 선택합니다.

b. [Create traffic policy]를 선택합니다.

c. [Name policy] 페이지에서 해당 값을 지정합니다. 자세한 내용은 트래픽 정책을 만들 때 지정하는 값 단원을 참조하십시오.

d. 4단계로 건너뜁니다.

3. JSON 문서를 가져와서 기존 트래픽 정책의 새 버전을 만들려면 다음 단계를 수행하십시오.

a. 탐색 창에서 [Traffic policies]를 선택합니다.

b. 새 버전의 기반으로 사용할 트래픽 정책의 이름을 선택합니다.

c. [Traffic policy versions] 테이블에서 새 버전의 기반으로 사용할 버전에 대한 확인란을 선택합니다.

d. [Edit policy as new version]을 선택합니다.

e. Update description(설명 업데이트) 페이지에 새 버전에 대한 설명을 입력합니다.

f. 4단계로 건너뜁니다.

4. Next(다음)를 선택합니다.

5. [Import traffic policy]를 선택합니다.

6. 새 트래픽 정책을 입력하고 예제 트래픽 정책 또는 기존 트래픽 정책을 붙여 넣습니다.

7. [Import traffic policy]를 선택합니다.

트래픽 정책 버전 및 연결된 정책 레코드 보기

트래픽 정책에 대해 만든 모든 버전과 각 트래픽 정책 버전을 사용하여 만든 모든 정책 레코드를 볼 수 있습니다.

트래픽 정책 버전 및 연결된 정책 레코드를 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.

2. 탐색 창에서 [Traffic policies]를 선택합니다.

3. 트래픽 정책의 이름을 선택합니다.

4. 위쪽 테이블에는 트래픽 정책에 대해 만든 모든 버전이 나열됩니다. 이 테이블에 포함되는 정보는 다음과 같습니다.

버전 번호

만든 각 트래픽 정책 버전의 번호입니다. 버전 번호를 선택하면 해당 버전에 대한 구성이 콘솔에 표시됩니다.

정책 레코드 수

이 트래픽 버전을 사용하여 만든 정책 레코드의 수입니다.

DNS 유형

트래픽 정책 버전을 만들 때 지정한 DNS 유형입니다.

버전 설명

트래픽 정책 버전을 만들 때 지정한 설명입니다.

5. 아래쪽 테이블에는 위쪽 테이블에 있는 트래픽 정책 버전을 사용하여 만든 모든 정책 레코드가 나열됩니다. 이 테이블에 포함되는 정보는 다음과 같습니다.

정책 레코드 DNS 이름

트래픽 정책과 연결된 DNS 이름입니다.

상태 표시기

가능한 값은 다음을 포함합니다.

적용됨

Route 53에서 정책 레코드와 해당 레코드의 생성 또는 업데이트를 마쳤습니다.

[생성 중]

Route 53에서 새 정책 레코드에 대한 레코드를 생성하고 있습니다.

업데이트 중

정책 레코드를 업데이트한 후 Route 53에서 지정된 DNS 이름에 대한 기존 레코드 그룹을 대체할 새 레코드 그룹을 생성하고 있습니다.

[삭제 중]

Route 53에서 정책 레코드 및 연결된 레코드를 삭제하고 있습니다.

Failed

Route 53에서 정책 레코드 및 연결된 레코드를 생성하거나 업데이트할 수 없습니다.

사용된 버전

정책 레코드를 만드는 데 사용된 트래픽 정책의 버전을 나타냅니다.

DNS 유형

Route 53에서 이 정책 레코드에 대해 생성한 모든 레코드의 DNS 유형입니다. 정책 레코드를 편집할 경우 편집 중인 정책 레코드와 동일한 DNS 유형을 가진 트래픽 정책 버전을 지정해야 합니다.

TTL(초)

DNS recursive resolver가 이 레코드에 관한 정보를 캐싱할 시간(초)입니다. 더 큰 값(예: 17만 2,800초 또는 2일)을 지정할 경우 재귀 해석기가 Route 53으로 요청을 덜 자주 보내므로 Route 53 서비스 요금이 감소합니다. 그러나 Route 53에 최신 정보를 요청하는 대신 재귀 해석기가 기간이 더 긴 캐시 값을 사용하므로 레코드(예: 새 IP 주소) 변경이 적용되는데 걸리는 시간이 길어집니다.

트래픽 정책 버전 및 트래픽 정책 삭제

트래픽 정책을 삭제하려면 해당 트래픽 정책에 대해 만든 모든 버전(원본 포함)을 삭제해야 합니다. 또한 트래픽 정책 버전을 삭제하려면 해당 트래픽 정책 버전을 사용하여 만든 모든 정책 레코드를 삭제해야 합니다.

> **Important**
>
> Amazon Route 53에서 DNS 쿼리에 응답하는 데 사용 중인 정책 레코드를 삭제할 경우 Route 53에서 해당 DNS 이름에 대한 쿼리에 대한 응답을 중지합니다. 예를 들어, Route 53에서 www.example.com에 대한 DNS 쿼리에 응답하기 위해 www.example.com에 대한 정책 레코드를 사용 중일 때 정책 레코드를 삭제하면 사용자가 www.example.com 도메인 이름을 사용하여 웹 사이트 또는 웹 애플리케이션에 액세스할 수 없습니다.

트래픽 정책 버전과 트래픽 정책(필요한 경우)을 삭제하려면 다음 절차를 수행하십시오.

트래픽 정책 버전 및 트래픽 정책을 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 [Traffic policies]를 선택합니다.

3. 트래픽 정책 버전을 삭제할(필요한 경우 완전히 삭제) 트래픽 정책의 이름을 선택합니다.
4. 위쪽 테이블에서 삭제할 트래픽 정책 버전이 아래쪽 테이블의 [Version used] 열에 표시되는 경우 아래쪽 테이블에서 해당 정책 레코드에 대한 확인란을 선택합니다.

   예를 들어, 트래픽 정책 버전 3을 삭제하려고 하지만 버전 3을 사용하여 아래쪽 테이블의 정책 레코드 중 하나를 만든 경우 해당 정책 레코드에 대한 확인란을 선택합니다.
5. [Delete policy records]를 선택합니다.
6. 삭제한 정책 레코드가 테이블에 더 이상 나타나지 않을 때까지 아래쪽 테이블에 대한 [Refresh] 버튼을 선택하여 화면을 새로 고칩니다.
7. 위쪽 테이블에서 삭제할 트래픽 정책 버전에 대한 확인란을 선택합니다.
8. [Delete version]을 선택합니다.
9. 이전 단계에서 모든 트래픽 정책 버전을 삭제한 경우 트래픽 정책을 삭제하려면 위쪽 테이블에 대한 [Refresh] 버전을 선택하여 테이블이 비워질 때까지 화면을 새로 고칩니다.
10. 탐색 창에서 [Traffic policies]를 선택합니다.
11. 트래픽 정책 목록에서 삭제할 트래픽 정책에 대한 확인란을 선택합니다.
12. [Delete traffic policy]를 선택합니다.

정책 레코드 만들기 및 관리

트래픽 정책을 생성할 때 지정한 리소스로 인터넷 트래픽을 라우팅하려면 하나 이상의 정책 레코드를 생성합니다. 각 정책 레코드는 정책 레코드를 생성하려는 호스팅 영역과 트래픽을 라우팅하려는 도메인 또는 하위 도메인 이름을 식별합니다. 예를 들어, www.example.com의 트래픽을 라우팅하려는 경우 example.com 호스팅 영역에 호스팅 영역 ID를 지정하고 Policy record DNS name(정책 레코드 DNS 이름)에 www.example.com을 지정합니다.

동일한 트래픽 정책을 사용하여 하나 이상의 도메인 또는 하위 도메인의 트래픽을 라우팅하려는 경우 다음 두 가지 옵션이 있습니다.

- 각 도메인 또는 하위 도메인 이름의 정책 레코드를 생성할 수 있습니다.
- 하나의 정책 레코드를 생성한 다음 정책 레코드를 참조하는 CNAME 또는 별칭 레코드를 생성할 수 있습니다.

예를 들어, example.com, example.net 및 example.org에 동일한 트래픽 정책을 사용하는 경우 다음 중 하나를 수행할 수 있습니다.

- 각 이름에 대해 하나의 정책 레코드를 생성합니다.
- 이름 중 하나에 대한 정책 레코드를 생성한 다음 다른 두 이름의 호스팅 영역에서 CNAME 레코드를 생성합니다. 두 개의 CNAME 레코드에서 정책 레코드를 생성한 레코드 이름을 지정합니다.

example.com 및 www.example.com과 같은 도메인과 하위 도메인에 동일한 트래픽 정책을 사용하려는 경우 한 이름에 대한 정책 레코드를 생성한 다음 나머지에 대한 별칭 레코드를 생성할 수 있습니다. 예를 들어, example.com에 대한 정책 레코드를 생성한 다음 example.com 레코드를 별칭 대상으로 하는 www.example.com에 대한 별칭 레코드를 생성할 수 있습니다.

> **Note**
>
> 생성하는 각 정책 레코드에 대해 월별 요금이 발생합니다. 여러 도메인 또는 하위 도메인 이름에 동일한 트래픽 정책을 사용하려는 경우 CNAME 또는 별칭 레코드를 사용하여 요금을 줄일 수 있습니다.
>
> - 하나의 정책 레코드와 이 정책 레코드를 참조하는 하나 이상의 CNAME 레코드를 생성하는 경우 정책 레코드에 대한 요금과 CNAME 레코드의 DNS 쿼리에 대한 요금만 지불하면 됩니다.
> - 하나의 정책 레코드와 이 정책 레코드를 참조하는 동일한 호스팅 영역 내의 별칭 레코드 하나 이상을 생성하는 경우 정책 레코드에 대한 요금과 별칭 레코드의 DNS 쿼리에 대한 요금만 지불하면 됩니다.

주제

정책 레코드 만들기

정책 레코드를 만들려면 다음 절차를 수행하십시오.

> **Important**
>
> 만드는 각 정책 레코드에 대해 월별 요금이 발생합니다. 나중에 정책 레코드를 삭제할 경우 일할 계산된 요금이 청구됩니다. 자세한 내용은 Amazon Route 53 요금의 "트래픽 흐름" 섹션을 참조하세요.

정책 레코드를 만들려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 [Policy records]를 선택합니다.
3. [Policy records] 페이지에서 [Create policy records]를 선택합니다.
4. [Create policy records] 페이지에서 해당 값을 지정합니다. 자세한 내용은 정책 레코드의 생성 또는 업데이트 시 지정하는 값 단원을 참조하십시오.
5. [Create policy records]를 선택합니다.

   생성된 정책 레코드의 상태가 적용됨으로 표시되려면 몇 분 정도 걸릴 수 있습니다.
6. 다른 호스팅 영역에서 정책 레코드를 만들려면 3~5단계를 반복합니다.

> **Note**
>
> 정책 레코드 상태가 실패인 경우 상태 옆에 있는 정보 버튼을 선택하여 실패에 대한 자세한 정보를 확인합니다. 추가 도움이 필요하고 AWS 지원에 문의하려면 에서 기술 지원을 받으려면 어떻게 해야 하나요 AWS?를 참조하세요.

정책 레코드의 생성 또는 업데이트 시 지정하는 값

정책 레코드를 만들거나 업데이트할 때 다음 값을 지정합니다.

- Traffic policy
- Version
- Hosted zone
- Policy record DNS name
- TTL

트래픽 정책

이 정책 레코드에 대해 구성을 사용할 트래픽 정책을 선택합니다.

버전

이 정책 레코드에 대해 구성을 사용할 트래픽 정책의 버전을 선택합니다.

기존 정책 레코드를 업데이트할 경우 DNS 유형이 정책 레코드의 현재 DNS 유형과 일치하는 버전을 선택해야 합니다. 예를 들어, 정책 레코드의 DNS 유형이 [A]인 경우 DNS 유형이 [A]인 버전을 선택해야 합니다.

호스팅 영역

지정된 트래픽 정책과 버전을 사용하여 정책 레코드를 만들 호스팅 영역을 선택합니다. 정책 레코드를 만든 이후에는 [Hosted zone] 값을 변경할 수 없습니다.

정책 레코드 DNS 이름

정책 레코드를 만들 때 지정된 트래픽 정책과 버전의 구성을 사용하여 Route 53에서 DNS 쿼리에 응답하게 할 도메인 이름 또는 하위 도메인 이름을 입력합니다.

지정한 호스팅 영역에서 여러 도메인 이름 또는 하위 도메인 이름에 대해 동일한 구성을 사용하려면 [Add another policy record]를 선택하고 해당 도메인 이름 또는 하위 도메인 이름과 TTL을 입력합니다.

정책 레코드를 만든 이후에는 [Policy record DNS name] 값을 변경할 수 없습니다.

TTL(초)

DNS recursive resolver가 이 레코드에 관한 정보를 캐싱할 시간(초)을 입력합니다. 더 큰 값(예: 172,800초 또는 2일)을 지정할 경우 재귀 해석기가 Route 53으로 요청을 덜 자주 보내므로 Route 53 서비스 요금이 감소합니다. 그러나 Route 53에 최신 정보를 요청하는 대신 재귀 해석기가 기간이 더 긴 캐시 값을 사용하므로 레코드(예: 새 IP 주소) 변경이 적용되는데 걸리는 시간이 길어집니다.

정책 레코드 업데이트

정책 레코드의 설정을 업데이트하려면 다음 절차를 수행하십시오.

정책 레코드를 업데이트하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.

2. 탐색 창에서 [Policy records]를 선택합니다.
3. [Policy records] 페이지에서 업데이트할 정책 레코드에 대한 확인란을 선택하고 [Edit policy record]를 선택합니다.
4. [Edit policy record] 페이지에서 해당 값을 지정합니다. 자세한 내용은 정책 레코드의 생성 또는 업데이트 시 지정하는 값 단원을 참조하십시오.
5. [Edit policy record]를 선택합니다.

   생성된 정책 레코드의 상태가 적용됨으로 표시되려면 몇 분 정도 걸릴 수 있습니다.
6. 다른 정책 레코드를 업데이트하려면 3~5단계를 반복합니다.

> **Note**
>
> 정책 레코드 상태가 실패인 경우 상태 옆에 있는 정보 버튼을 선택하여 실패에 대한 자세한 정보를 확인합니다. 추가 도움이 필요하고 AWS 지원에 문의하려면 에서 기술 지원을 받으려면 어떻게 해야 하나요 AWS?를 참조하세요.

정책 레코드 삭제

정책 레코드를 삭제하려면 다음 절차를 수행하십시오.

> **Important**
>
> Amazon Route 53에서 DNS 쿼리에 응답하는 데 사용 중인 정책 레코드를 삭제할 경우 Route 53에서 해당 DNS 이름에 대한 쿼리에 대한 응답을 중지합니다. 예를 들어, Route 53에서 www.example.com에 대한 DNS 쿼리에 응답하기 위해 www.example.com에 대한 정책 레코드를 사용 중일 때 정책 레코드를 삭제하면 사용자가 www.example.com 도메인 이름을 사용하여 웹 사이트 또는 웹 애플리케이션에 액세스할 수 없습니다.

정책 레코드를 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 [Policy records]를 선택합니다.

3. [Policy records] 페이지에서 삭제할 정책 레코드에 대한 확인란을 선택하고 [Delete policy record]를 선택합니다.

   몇 분 정도 기다린 후 페이지를 새로 고쳐 정책 레코드가 목록에서 사라지는지 확인합니다.

Amazon Route 53 Resolver란 무엇인가요?

Amazon Route 53 Resolver 는 퍼블릭 레코드, Amazon VPC별 DNS 이름 및 Amazon Route 53 프라이빗 호스팅 영역에 대한 AWS 리소스의 DNS 쿼리에 재귀적으로 응답하며 기본적으로 모든 VPCs.

> **Note**
>
> Amazon Route 53 Resolver 는 이전에 Amazon DNS 서버라고 했지만 Resolver 규칙과 인바운드 및 아웃바운드 엔드포인트가 도입될 때 이름이 변경되었습니다. 자세한 내용은 Amazon Virtual Private Cloud 사용 설명서의 Amazon DNS 서버를 참조하세요.

Amazon VPC는 VPC+2 IP 주소에서 Route 53 Resolver에 연결됩니다. 이 VPC+2 주소는 가용 영역 내의 Route 53 Resolver에 연결됩니다.

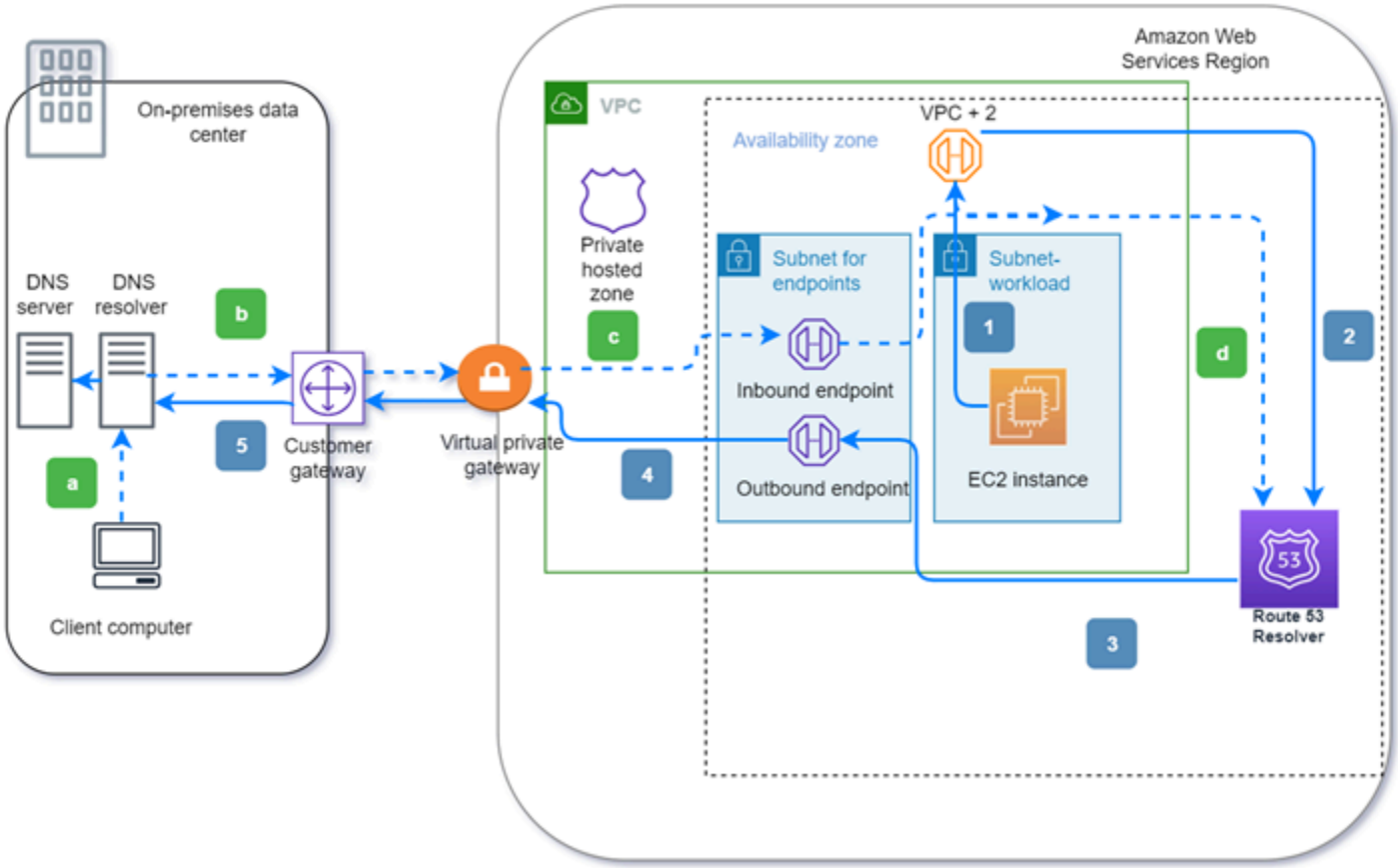
Route 53 Resolver는 다음에 대한 DNS 쿼리에 자동으로 응답합니다.

- EC2 인스턴스의 로컬 VPC 도메인 이름(예: ec2-192-0-2-44.compute-1.amazonaws.com).
- 프라이빗 호스팅 영역의 기록(예: acme.example.com).
- Route 53 Resolver는 퍼블릭 도메인 이름에 대해 인터넷에 있는 퍼블릭 이름 서버에 대해 역방향 조회를 수행합니다.

VPC와 온프레미스 리소스를 모두 활용하는 워크로드가 있는 경우 온프레미스에서 호스팅되는 DNS 레코드도 확인해야 합니다. 마찬가지로 이러한 온프레미스 리소스는에서 호스팅되는 이름을 확인해야 할 수 있습니다 AWS. Resolver 엔드포인트 및 조건부 전달 규칙을 통해 온프레미스 리소스와 VPC 간의 DNS 쿼리를 확인하여 VPN 또는 Direct Connect(DX)를 통해 하이브리드 클라우드 설정을 생성할 수 있습니다. 구체적으로 설명하면 다음과 같습니다.

- 인바운드 Resolver 엔드포인트를 사용하면 온프레미스 네트워크나 다른 VPC에서 귀하의 VPC로 DNS 쿼리를 보낼 수 있습니다.
- 아웃바운드 Resolver 엔드포인트를 사용하면 귀하의 VPC에서 온프레미스 네트워크나 다른 VPC로 DNS 쿼리를 보낼 수 있습니다.
- Resolver 규칙을 사용하면 각 도메인 이름에 대해 하나의 전달 규칙을 생성하고 DNS 쿼리를 VPC에서 온프레미스 DNS 해석기로, 온프레미스에서 VPC로 전달할 도메인의 이름을 지정할 수 있습니다. 규칙은 VPC에 직접 적용되며 복수의 계정에 걸쳐 공유될 수 있습니다.

다음 다이어그램은 Resolver 엔드포인트를 사용하는 하이브리드 DNS 확인을 보여줍니다. 다이어그램은 하나의 가용 영역만 표시하도록 간소화되어 있습니다.



다이어그램은 다음 단계들을 보여줍니다.

아웃바운드(실선 화살표 1–5):

1. Amazon EC2 인스턴스는 도메인 internal.example.com에 대한 DNS 쿼리를 해결해야 합니다. 신뢰할 수 있는 DNS 서버는 온프레미스 데이터 센터에 있습니다. 이 DNS 쿼리는 Route 53 Resovler에 연결된 VPC에 있는 VPC+2로 전송됩니다.
2. Route 53 Resolver 전달 규칙은 쿼리를 온프레미스 데이터 센터의 internal.example.com으로 전달하도록 구성되어 있습니다.
3. 쿼리는 아웃바운드 엔드포인트로 전달됩니다.
4. 아웃바운드 엔드포인트는 AWS 및 데이터 센터 간의 프라이빗 연결을 통해 쿼리를 온프레미스 DNS 해석기로 전달합니다. 연결은 가상 프라이빗 게이트웨이로 AWS Site-to-Site VPN표현되는 AWS Direct Connect 또는 중 하나일 수 있습니다.
5. 온프레미스 DNS 해석기는 internal.example.com에 대한 DNS 쿼리를 해석하고 반대로 동일한 경로를 통해 Amazon EC2 인스턴스에 응답을 반환합니다.

인바운드(점선 화살표 a–d):

a. 온프레미스 데이터 센터의 클라이언트는 DNS 쿼리를 도메인 dev.example.com AWS 리소스로 확인해야 합니다. 이 항목은 쿼리를 온프레미스 DNS 해석기로 전송합니다.

b. 온프레미스 DNS 해석기에는 dev.example.com에 대한 쿼리를 인바운드 엔드포인트로 가리키는 전달 규칙이 있습니다.

c. 쿼리는 가상 게이트웨이로 AWS Site-to-Site VPN표시된 AWS Direct Connect 또는와 같은 프라이빗 연결을 통해 인바운드 엔드포인트에 도착합니다.

d. 인바운드 엔드포인트는 쿼리를 Route 53 Resolver로 보내고, Route 53 Resolver는 dev.example.com에 대한 DNS 쿼리를 확인하고 반대로 동일한 경로를 통해 클라이언트에 응답을 반환합니다.

주제

VPC와 네트워크 간 DNS 쿼리 해석

Resolver에는 온프레미스 환경에서 송수신되는 DNS 쿼리에 응답하도록 구성하는 엔드포인트가 포함되어 있습니다.

> **Note**
>
> 사용자의 온프레미스 DNS 서버에서 VPC CIDR+ 2 주소로 프라이빗 DNS 쿼리를 전달하는 것은 지원되지 않으므로 불안정한 결과가 발생할 수 있습니다. 대신 Resolver 인바운드 엔드포인트를 사용할 것을 권장합니다.

또한 전달 규칙을 구성하여 Resolver와 네트워크의 DNS 해석기 간에 DNS 해석을 통합할 수 있습니다. 네트워크에는 다음과 같이 VPC에서 연결할 수 있는 모든 네트워크가 포함될 수 있습니다.

- VPC 자체
- 피어링된 다른 VPC
- 에 연결된 온프레미스 네트워크 AWS AWS Direct Connect, VPN 또는 네트워크 주소 변환(NAT) 게이트웨이

쿼리 전달을 시작하기 전에, 연결된 VPC에 Resolver 인바운드 및/또는 아웃바운드 엔드포인트를 생성합니다. 이러한 엔드포인트는 인바운드 또는 아웃바운드 쿼리에 대한 경로를 제공합니다.

인바운드 엔드포인트: 네트워크의 DNS 해석기가 이 엔드포인트를 통해 DNS 쿼리를 Route 53 Resolver에 전달할 수 있습니다.

> 이렇게 하면 DNS 해석기가 Route 53 프라이빗 호스팅 영역의 EC2 인스턴스 또는 레코드와 같은 AWS 리소스의 도메인 이름을 쉽게 확인할 수 있습니다. 자세한 내용은 네트워크의 DNS 해석기가 Route 53 Resolver 엔드포인트로 DNS 쿼리를 전달하는 방법 단원을 참조하십시오.

아웃바운드 엔드포인트: Resolver가 이 엔드포인트를 통해 쿼리를 네트워크의 해석기에게 조건부로 전달합니다.

> 선택한 쿼리를 전달하려면 전달하려는 DNS 쿼리의 도메인 이름(예: example.com) 및 쿼리를 전달하려는 네트워크에 있는 DNS 해석기의 IP 주소를 지정하는 Resolver 규칙을 생성합니다. 쿼리가 여러 규칙(example.com, acme.example.com)과 일치하는 경우 Resolver는 가장 확실히 일치하는 규칙(acme.example.com)을 선택하고 해당 규칙에 지정한 IP 주소에 쿼리를 전달합니다. 자세한 내용은 Route 53 Resolver 엔드포인트가 DNS 쿼리를 VPC에서 네트워크로 전달하는 방법 섹션을 참조하세요.

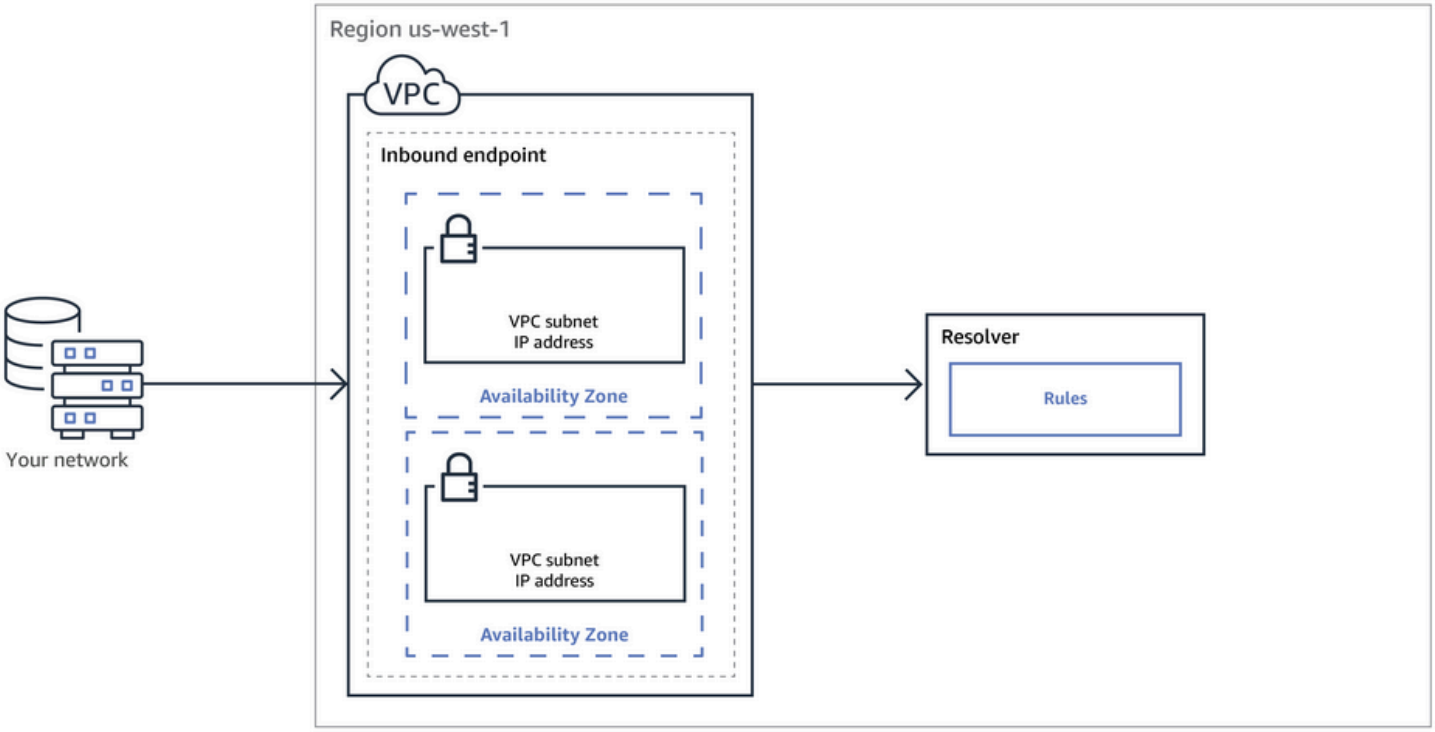
Amazon VPC와 마찬가지로 Resolver도 지역적입니다. VPC가 있는 리전마다 쿼리를 VPC에서 네트워크로 전달하거나(아웃바운드 쿼리) 네트워크에서 VPC로 전달하거나(인바운드 쿼리) 둘 다로 전달하도록 선택할 수 있습니다.

소유하지 않은 VPC에서는 해석기 엔드포인트를 생성할 수 없습니다. VPC 소유자만 인바운드 엔드포인트와 같은 VPC 수준 리소스를 생성할 수 있습니다.

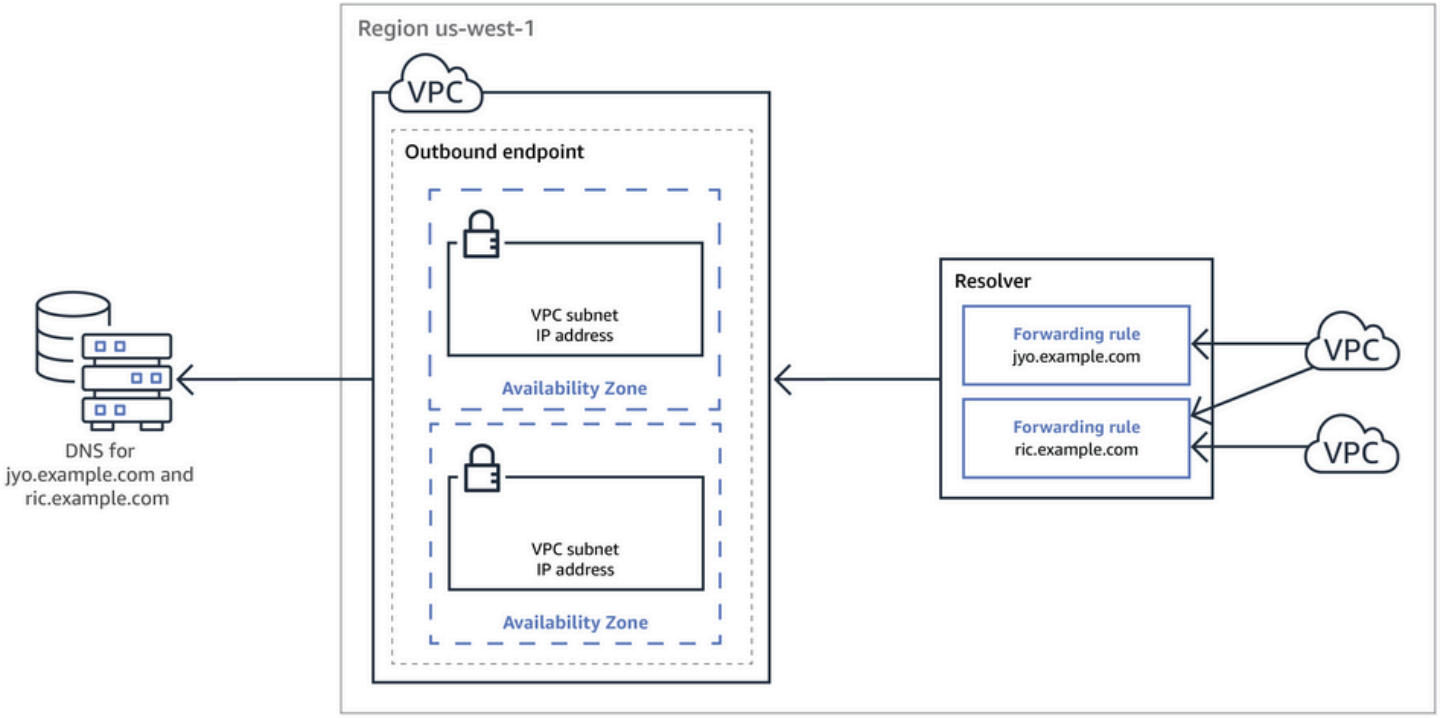
> **Note**
>
> Resolver 엔드포인트를 생성할 때 인스턴스 테넌시 속성이 `dedicated`로 설정된 VPC를 지정할 수 없습니다. 자세한 내용은 섹션을 참조하세요.

인바운드 또는 아웃바운드 전달을 사용하려면 VPC에 Resolver 엔드포인트를 만듭니다. 엔드포인트 정의의 일부로 인바운드 DNS 쿼리를 전달할 IP 주소 또는 아웃바운드 쿼리를 시작할 IP 주소를 지정합니다. 지정한 각 IP 주소에 대해 Resolver는 자동으로 VPC 탄력적 네트워크 인터페이스를 만듭니다.

다음 다이어그램은 네트워크의 DNS 해석기에서 Route 53 Resolver 엔드포인트까지의 DNS 쿼리의 경로를 보여줍니다.



다음 다이어그램은 네트워크의 VPC 중 하나의 EC2 인스턴스에서 네트워크의 DNS 해석기까지의 DNS 쿼리의 경로를 보여줍니다.



VPC 네트워크 인터페이스에 대한 개요는 Amazon VPC 사용 설명서의 탄력적 네트워크 인터페이스를 참조하세요.

주제

- 네트워크의 DNS 해석기가 Route 53 Resolver 엔드포인트로 DNS 쿼리를 전달하는 방법
- Route 53 Resolver 엔드포인트가 DNS 쿼리를 VPC에서 네트워크로 전달하는 방법
- 인바운드 및 아웃바운드 엔드포인트를 만들 때 고려 사항

네트워크의 DNS 해석기가 Route 53 Resolver 엔드포인트로 DNS 쿼리를 전달하는 방법

네트워크에서 AWS 리전의 Route 53 Resolver 엔드포인트로 DNS 쿼리를 전달하려면 다음 단계를 수행합니다.

1. VPC의 Route 53 Resolver 인바운드 엔드포인트를 생성하고 네트워크의 해석기가 DNS 쿼리를 전달하는 IP 주소를 지정합니다.

   인바운드 엔드포인트에 대해 지정한 각 IP 주소에 대해 Resolver는 인바운드 엔드포인트가 생성된 VPC에 VPC 탄력적 네트워크 인터페이스를 만듭니다.

2. 인바운드 엔드포인트에 지정한 IP 주소로 해당 도메인 이름의 DNS 쿼리를 전달하도록 네트워크의 해석기를 구성합니다. 자세한 내용은 인바운드 및 아웃바운드 엔드포인트를 만들 때 고려 사항 섹션을 참조하세요.

네트워크에서 시작되는 DNS 쿼리를 Resolver에서 해석하는 방법은 다음과 같습니다.

1. 네트워크에 있는 웹 브라우저나 다른 애플리케이션이 Resolver에 전달된 도메인 이름의 DNS 쿼리를 제출합니다.
2. 네트워크에 있는 해석기가 인바운드 엔드포인트의 IP 주소로 쿼리를 전달합니다.
3. 인바운드 엔드포인트가 Resolver로 쿼리를 전달합니다.
4. Resolver가 내부적으로 또는 퍼블릭 이름 서버에 대해 재귀 조회를 수행하여 DNS 쿼리의 도메인 이름에 해당하는 값을 가져옵니다.
5. 해석기는 인바운드 엔드포인트에 값을 반환합니다.
6. 인바운드 엔드포인트가 네트워크에 있는 해석기에 값을 반환합니다.
7. 네트워크에 있는 해석기가 애플리케이션으로 값을 반환합니다.
8. Resolver에서 반환한 값을 사용하여 애플리케이션이 HTTP 요청(예: Amazon S3 버킷의 객체에 대한 요청)을 제출합니다.

인바운드 엔드포인트를 생성해도 Resolver의 동작은 변경되지 않으며 AWS , 네트워크 외부의 위치에서 Resolver로 가는 경로만 제공합니다.

Route 53 Resolver 엔드포인트가 DNS 쿼리를 VPC에서 네트워크로 전달하는 방법

AWS 리전에 있는 하나 이상의 VPCs에 있는 EC2 인스턴스의 DNS 쿼리를 네트워크로 전달하려면 다음 단계를 수행합니다.

1. VPC에 Route 53 Resolver 아웃바운드 엔드포인트를 생성하고 다음과 같이 여러 값을 지정합니다.
   - 네트워크에 있는 해석기로 가는 도중 DNS 쿼리가 통과할 VPC
   - Resolver가 DNS 쿼리를 전달할 출처가 되는 VPC의 IP 주소입니다. 네트워크상의 호스트에게 이 주소는 DNS 쿼리가 시작되는 IP 주소입니다.
   - VPC 보안 그룹

아웃바운드 엔드포인트에 지정한 각 IP 주소에 대해 Resolver는 지정한 VPC에 Amazon VPC 탄력적 네트워크 인터페이스를 만듭니다. 자세한 내용은 인바운드 및 아웃바운드 엔드포인트를 만들 때 고려 사항 섹션을 참조하세요.

2. Resolver가 네트워크의 해석기에 전달할 DNS 쿼리의 도메인 이름을 지정하는 규칙을 하나 이상 만듭니다. 또한 해석기의 IP 주소를 지정합니다. 자세한 내용은 규칙을 사용하여 네트워크에 전달할 쿼리 제어 섹션을 참조하세요.
3. DNS 쿼리를 네트워크에 전달할 VPC에 각 규칙을 연결합니다.

주제

규칙을 사용하여 네트워크에 전달할 쿼리 제어

규칙은 Route 53 Resolver 엔드포인트가 네트워크에 있는 DNS 해석기에 전달하는 DNS 쿼리와, Resolver가 직접 응답하는 쿼리를 제어합니다.

다음 두 가지 방법으로 규칙을 분류할 수 있습니다. 한 가지 방법은 규칙을 생성하는 사람을 통한 제어입니다.

- 자동 정의 규칙 - Resolver는 자동으로 자동 정의 규칙을 만들어 VPC와 규칙을 연결합니다. 이러한 규칙의 대부분은 Resolver가 쿼리에 답변하는 AWS특정 도메인 이름에 적용됩니다. 자세한 내용은 Resolver가 자동 정의 시스템 규칙을 생성하는 도메인 이름 단원을 참조하십시오.
- 사용자 지정 규칙 - 사용자 지정 규칙을 만들어 VPC와 연결합니다. 지금은 전달 규칙이라고도 하는 조건부 전달 규칙 한 가지만 사용자 지정 규칙으로 생성할 수 있습니다. 전달 규칙을 사용하면 Resolver가 VPC에서 네트워크에 있는 DNS 해석기의 IP 주소로 DNS 쿼리를 전달합니다.

  자동 정의 규칙과 동일한 도메인에 대해 전달 규칙을 생성할 경우 Resolver가 전달 규칙의 설정에 따라 해당 도메인 이름에 대한 쿼리를 네트워크에 있는 DNS 해석기로 전달합니다.

또 다른 방법은 역할에 따라 규칙을 분류하는 것입니다.

- 조건부 전달 규칙 - 지정된 도메인 이름의 DNS 쿼리를 네트워크의 DNS 해석기로 전달하려는 경우 조건부 전달 규칙(또는 전달 규칙)을 생성합니다.
- 시스템 규칙 - 시스템 규칙을 사용하면 Resolver가 전달 규칙에 정의된 동작을 선택적으로 재정의합니다. 시스템 규칙을 생성할 때 Resolver가 지정된 하위 도메인의 DNS 쿼리를 해석합니다. 그렇지 않을 경우 네트워크의 DNS 해석기가 해석합니다.

  기본적으로 전달 규칙은 도메인 이름과 모든 하위 도메인에 적용됩니다. 도메인에 대한 쿼리를 네트워크에 있는 해석기에 전달하되 일부 하위 도메인에 대한 쿼리는 제외하려면 하위 도메인에 대한 시스템 규칙을 생성합니다. 예를 들어 example.com의 전달 규칙을 생성하고 acme.example.com에 대한 쿼리를 전달하지 않으려면 시스템 규칙을 생성하고 도메인 이름에 acme.example.com을 지정합니다.
- 재귀 규칙 - Resolver는 인터넷 해석기라는 재귀 규칙을 자동으로 만듭니다. 이 규칙은 Route 53 Resolver가 사용자 지정 규칙을 만들지 않고 Resolver가 자동 정의 규칙을 만들지 않은 모든 도메인 이름에 대해 재귀 해석기의 역할을 합니다. 이 동작을 재정의하는 방법은 이 주제 뒷부분의 "네트워크로 모든 쿼리 전달"을 참조하세요.

특정 도메인 이름(사용자 또는 대부분의 AWS 도메인 이름), 퍼블릭 도메인 이름 또는 모든 AWS 도메인 이름에 적용되는 사용자 지정 규칙을 생성할 수 있습니다.

네트워크에 특정 도메인 이름에 대한 쿼리 전달

example.com과 같은 특정 도메인 이름에 대한 쿼리를 네트워크에 전달하려면 규칙을 생성하고 도메인 이름을 지정합니다. 쿼리를 전달할 네트워크에 있는 DNS 해석기의 IP 주소도 지정합니다. 그런 다음 네트워크에 DNS 쿼리를 전달할 VPC에 각 규칙을 연결합니다. 예를 들어 example.com, example.org 및 example.net에 대해 별도의 규칙을 생성할 수 있습니다. 그런 다음 규칙을 AWS 리전의 VPCs와 어떤 조합으로든 연결할 수 있습니다.

네트워크에 amazonaws.com에 대한 쿼리 전달

도메인 이름 amazonaws.com EC2 인스턴스 및 S3 버킷과 같은 AWS 리소스의 퍼블릭 도메인 이름입니다. amazonaws.com에 대한 쿼리를 네트워크에 전달하려면 규칙을 만들고 도메인 이름에 amazonaws.com을 지정하고 규칙 유형에 전달을 지정하세요.

> **Note**
>
> amazonaws.com의 전달 규칙을 생성할 경우에도 Resolver에서는 일부 amazonaws.com 하위 도메인에 대한 DNS 쿼리를 자동으로 전달합니다. 자세한 내용은 Resolver가 자동 정

의 시스템 규칙을 생성하는 도메인 이름 섹션을 참조하세요. 이 동작을 재정의하는 방법은 바로 다음에 나오는 "네트워크로 모든 쿼리 전달"을 참조하세요.

네트워크로 모든 쿼리 전달

모든 쿼리를 네트워크로 전달하려면, 규칙을 만들고 도메인 이름에 "."(점)을 지정하고 모든 DNS 쿼리를 네트워크로 전달하기 위한 규칙을 VPC에 연결합니다. 외부에서 DNS 해석기를 사용하면 일부 기능이 AWS 중단되므로 해석기는 여전히 모든 DNS 쿼리를 네트워크에 전달하지 않습니다. 예를 들어 일부 내부 AWS 도메인 이름에는 외부에서 액세스할 수 없는 내부 IP 주소 범위가 있습니다 AWS. "."에 대한 규칙을 만들 때 쿼리가 네트워크로 전달되지 않는 도메인 이름 목록은 Resolver가 자동 정의 시스템 규칙을 생성하는 도메인 이름를 참조하세요.

그러나 역방향 DNS에 대한 자동 정의 시스템 규칙을 비활성화할 수 있으므로 “.” 규칙이 모든 역방향 DNS 쿼리를 네트워크로 전달할 수 있습니다. 자동 정의 규칙을 해제하는 방법에 대한 자세한 내용은 해석기의 역방향 DNS 쿼리에 대한 전달 규칙 단원을 참조하십시오.

기본적으로 전달에서 제외되는 도메인 이름을 포함하여 모든 도메인 이름에 대한 DNS 쿼리를 네트워크로 전달하려면 "." 규칙을 생성하고 다음 중 하나를 수행하면 됩니다.

- VPC의 `enableDnsHostnames` 플래그를 `false`로 설정
- Resolver가 자동 정의 시스템 규칙을 생성하는 도메인 이름에 나온 도메인 이름의 규칙 생성

> **Important**
>
> "." 규칙을 생성할 때 Resolver가 제외하는 도메인 이름을 포함한 모든 도메인 이름을 네트워크로 전달할 경우 일부 기능이 중단될 수 있습니다.

Resolver가 쿼리의 도메인 이름이 규칙과 일치하는지 확인하는 방법

Route 53 Resolver에서는 DNS 쿼리에 있는 도메인 이름을 쿼리가 시작된 VPC에 연결된 규칙의 도메인 이름과 비교합니다. Resolver는 다음과 같은 경우에 도메인 이름이 일치한다고 간주합니다.

- 도메인 이름이 정확히 일치합니다.
- 쿼리에 있는 도메인 이름이 규칙에 있는 도메인 이름의 하위 도메인입니다.

예를 들어 규칙에 있는 도메인 이름이 acme.example.com일 경우 Resolver에서는 DNS 쿼리에 있는 다음 도메인 이름이 일치한다고 간주합니다.

- acme.example.com
- zenith.acme.example.com

다음 도메인 이름은 일치하지 않습니다.

- example.com
- nadir.example.com

쿼리에 있는 도메인 이름이 2개 이상의 규칙에 있는 도메인 이름과 일치하는 경우(예: example.com 및 www.example.com) Resolver는 가장 구체적인 도메인 이름(www.example.com)이 포함된 규칙을 사용하여 아웃바운드 DNS 쿼리를 라우팅합니다.

Resolver가 DNS 쿼리를 전달할 대상을 결정하는 방법

VPC의 EC2 인스턴스에서 실행되는 애플리케이션이 DNS 쿼리를 제출할 때 Route 53 Resolver는 다음과 같은 단계를 수행합니다.

1. Resolver가 규칙에 도메인 이름이 있는지 확인합니다.

   쿼리의 도메인 이름이 규칙의 도메인 이름과 일치하면 Resolver는 아웃바운드 엔드포인트를 생성할 때 지정한 IP 주소로 쿼리를 전달합니다. 그러면 아웃바운드 엔드포인트가 네트워크에 있는 해석기의 IP 주소로 쿼리를 전달합니다. 이 주소는 규칙을 생성할 때 지정된 주소입니다.

   자세한 내용은 Resolver가 쿼리의 도메인 이름이 규칙과 일치하는지 확인하는 방법 섹션을 참조하세요.

2. Resolver 엔드포인트가 "." 규칙의 설정에 따라 DNS 쿼리를 전달합니다.

   쿼리의 도메인 이름이 다른 규칙의 도메인 이름과 일치하지 않으면 Resolver가 자동 정의된 "."(점) 규칙의 설정에 따라 쿼리를 전달합니다. 점 규칙은 프라이빗 호스팅 영역의 일부 AWS 내부 도메인 이름 및 레코드 이름을 제외한 모든 도메인 이름에 적용됩니다. 이 규칙을 사용하면 쿼리에 있는 도메인 이름이 사용자 지정 전달 규칙에 있는 이름과 일치하지 않을 경우 Resolver가 퍼블릭 이름 서버에 DNS 쿼리를 전달합니다. 네트워크에 있는 DNS로 모든 쿼리를 전달하려면 사용자 지정 전달 규칙을 생성하고 도메인 이름에 "."을 지정하며 유형에 전달을 지정하고 해당 해석기의 IP 주소를 지정하면 됩니다.

3. Resolver가 쿼리를 제출한 애플리케이션에 응답을 반환합니다.

여러 리전에서 규칙 사용

Route 53 Resolver는 리전 서비스이므로 한 AWS 리전에서 생성한 객체는 해당 리전에서만 사용할 수 있습니다. 2개 이상 리전에서 동일한 규칙을 사용하려면 각 리전에서 규칙을 생성해야 합니다.

규칙을 생성한 AWS 계정은 규칙을 다른 AWS 계정과 공유할 수 있습니다. 자세한 내용은 Resolver 규칙을 다른 AWS 계정과 공유 및 공유 규칙 사용 단원을 참조하십시오.

Resolver가 자동 정의 시스템 규칙을 생성하는 도메인 이름

Resolver가 자동 정의 시스템 규칙을 자동으로 생성합니다. 이 규칙은 선택한 도메인의 쿼리가 기본적으로 해석되는 방법을 정의합니다.

- 프라이빗 호스팅 영역 및 Amazon EC2 특정 도메인 이름(예: compute.amazonaws.com 및 compute.internal)에 대해 자동 정의 규칙을 사용하면 "."(점) 또는 "com"과 같이 구체적이지 않은 도메인 이름에 대한 조건부 전달 규칙을 생성할 경우 프라이빗 호스팅 영역과 EC2 인스턴스를 계속 해석할 수 있습니다.
- 공개적으로 예약된 도메인 이름(예: localhost 및 10.in-addr.arpa)의 경우 DNS 모범 사례에 따라 쿼리가 퍼블릭 이름 서버로 전달되는 것이 아니라 로컬로 응답되는 것이 좋습니다. RFC 6303, Locally Served DNS Zones 섹션을 참조하세요.

> **Note**
>
> "."(점) 또는 "com"에 대해 조건부 전달 규칙을 생성하는 경우에는 amazonaws.com에서도 시스템 규칙을 생성하는 것이 좋습니다 (시스템 규칙을 사용하면 Resolver가 특정 도메인 및 하위 도메인의 DNS 쿼리를 로컬로 해석합니다.) 이러한 시스템 규칙을 생성하면 성능을 개선하고, 네트워크에 전달되는 쿼리 수를 줄이며, Resolver 요금을 줄일 수 있습니다.

자동 정의 규칙을 재정의하고 싶은 경우에는 동일한 도메인 이름에 대해 조건부 전달 규칙을 생성할 수 있습니다.

자동 정의 규칙의 일부를 비활성화할 수도 있습니다. 자세한 내용은 해석기의 역방향 DNS 쿼리에 대한 전달 규칙 단원을 참조하십시오.

해석기가 다음과 같은 자동 정의 규칙을 생성합니다.

프라이빗 호스팅 영역을 위한 규칙

VPC에 연결하는 프라이빗 호스팅 영역마다 Resolver가 규칙을 만들어 VPC에 연결합니다. 프라이빗 호스팅 영역을 여러 VPC에 연결할 경우 Resolver가 동일한 VPC에 규칙을 연결합니다.

규칙에는 전달 유형이 있습니다.

다양한 AWS 내부 도메인 이름에 대한 규칙

이 단원에 나오는 내부 도메인 이름에 대한 모든 규칙에는 전달(Forward) 유형이 있습니다. Resolver가 이 도메인 이름에 대한 DNS 쿼리를 VPC의 신뢰할 수 있는 이름 서버로 전달합니다.

> **Note**
>
> 사용자가 VPC의 `enableDnsHostnames` 플래그를 `true`로 설정할 때 Resolver가 이러한 규칙의 대부분을 만듭니다. Resolver 엔드포인트를 사용하지 않는 경우에도 Resolver가 규칙을 만듭니다.

VPC의 `enableDnsHostnames` 플래그를 `true`로 설정할 경우 Resolver가 다음과 같은 자동 정의 규칙을 생성해서 VPC에 연결합니다.

- 예를 들어 *Region-name*.compute.internal의 경우 eu-west-1.compute.internal입니다. us-east-1 리전에서는 이 도메인 이름을 사용하지 않습니다.
- 예를 들어 *Region-name*.compute.*amazon-domain-name*의 경우 eu-west-1.compute.amazonaws.com 또는 cn-north-1.compute.amazonaws.com.cn입니다. us-east-1 리전에서는 이 도메인 이름을 사용하지 않습니다.
- ec2.internal. us-east-1 리전에서만 이 도메인 이름을 사용합니다.
- compute-1.internal. us-east-1 리전에서만 이 도메인 이름을 사용합니다.
- compute-1.amazonaws.com. us-east-1 리전에서만 이 도메인 이름을 사용합니다.

다음의 자동 정의 규칙은 VPC의 `enableDnsHostnames` 플래그를 `true`로 설정할 경우 Resolver가 생성하는 규칙에 대한 역방향 DNS 조회에 사용됩니다.

- 10.in-addr.arpa
- 16.172.in-addr.arpa through 31.172.in-addr.arpa
- 168.192.in-addr.arpa
- 254.169.254.169.in-addr.arpa

- VPC의 각 CIDR 범위에 대한 규칙입니다. 예를 들어, CIDR 범위가 10.0.0.0/23인 VPC의 경우 Resolver가 다음 규칙을 생성합니다.
  - 0.0.10.in-addr.arpa
  - 1.0.10.in-addr.arpa

  또한 localhost 관련 도메인에 사용되는 다음의 자동 정의 규칙이 생성되고, VPC의 `enableDnsHostnames` 플래그를 `true`로 설정할 경우 VPC에 연결됩니다.
- localhost
- localdomain
- 127.in-addr.arpa
- 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa
- 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa

  Transit Gateway 또는 VPC 피어링을 통해 VPC를 다른 VPC와 연결하고 DNS 지원이 활성화된 경우 Resolver는 다음과 같은 자동 정의 규칙을 생성해서 VPC에 연결합니다.
- 피어 VPC의 IP 주소 범위에 대한 역방향 DNS 조회(예: 0.192.in-addr.arpa)

  IPv4 CIDR 블록을 VPC에 추가하면 Resolver가 새 IP 주소 범위의 자동 정의 규칙을 추가합니다.
- 다른 VPC가 다른 리전에 있을 경우 다음과 같은 도메인 이름이 사용됩니다.
  - *Region-name*.compute.internal. us-east-1 리전에서는 이 도메인 이름을 사용하지 않습니다.
  - *Region-name*.compute.*amazon-domain-name*. us-east-1 리전에서는 이 도메인 이름을 사용하지 않습니다.
  - ec2.internal. us-east-1 리전에서만 이 도메인 이름을 사용합니다.
  - compute-1.amazonaws.com. us-east-1 리전에서만 이 도메인 이름을 사용합니다.

다른 모든 도메인에 대한 규칙

Resolver가 이 주제 앞부분에서 지정하지 않은 모든 도메인 이름에 적용되는 "."(점) 규칙을 생성합니다. "." 규칙의 유형은 재귀(Recursive)이므로 이 규칙을 사용하면 Resolver가 재귀 해석기로 사용됩니다.

인바운드 및 아웃바운드 엔드포인트를 만들 때 고려 사항

AWS 리전에서 인바운드 및 아웃바운드 Resolver 엔드포인트를 생성하기 전에 다음 문제를 고려하세요.

주제

각 리전의 인바운드 및 아웃바운드 엔드포인트 수

AWS 리전의 VPCs에 대한 DNS를 네트워크의 DNS와 통합하려면 일반적으로 Resolver 인바운드 엔드포인트(VPCs) 하나와 아웃바운드 엔드포인트(VPC에서 네트워크 VPCs 로 전달하는 쿼리의 경우) 하나가 필요합니다. 여러 개의 인바운드 엔드포인트와 여러 개의 아웃바운드 엔드포인트를 생성할 수 있지만 하나의 인바운드 또는 아웃바운드 엔드포인트로 각 방향의 DNS 조회를 충분히 처리할 수 있습니다. 다음 사항에 유의하세요.

- 각 Resolver 엔드포인트의 경우 서로 다른 가용 영역에 두 개 이상의 IP 주소를 지정합니다. 엔드포인트의 각 IP 주소는 초당 많은 수의 DNS 쿼리를 처리할 수 있습니다. 엔드포인트의 IP 주소별 초당 최대 동시 쿼리 수는 Route 53 Resolver의 할당량 섹션을 참조하세요. Resolver가 추가 쿼리를 처리하게 하려는 경우 다른 엔드포인트를 추가하는 대신 기존 엔드포인트에 IP 주소를 추가할 수 있습니다.
- Resolver 요금은 엔드포인트의 IP 주소 수와 엔드포인트가 처리하는 DNS 쿼리 수를 기반으로 합니다. 각 엔드포인트는 최소 두 개의 IP 주소를 포함합니다. Resolver 요금에 대한 자세한 내용은 Amazon Route 53 요금을 참조하세요.
- 각 규칙은 DNS 쿼리가 전달되는 아웃바운드 엔드포인트를 지정합니다. AWS 리전에 여러 개의 아웃바운드 엔드포인트를 만들고 일부 또는 모든 Resolver 규칙을 모든 VPC와 연결하려면 이러한 규칙의 사본을 여러 개 만들어야 합니다.

인바운드 및 아웃바운드 엔드포인트에 동일한 VPC 사용

동일한 VPC 또는 동일한 리전의 다른 VPC에서 인바운드 및 아웃바운드 엔드포인트를 생성할 수 있습니다.

자세한 내용은 Amazon Route 53 모범 사례 섹션을 참조하세요.

인바운드 엔드포인트 및 프라이빗 호스팅 영역

Resolver가 프라이빗 호스팅 영역의 레코드를 사용하여 인바운드 DNS 쿼리를 해석하게 하려면 프라이빗 호스팅 영역을 인바운드 엔드포인트가 생성된 VPC와 연결합니다. 프라이빗 호스팅 영역과 VPC를 연결하는 방법에 대한 자세한 내용은 프라이빗 호스팅 영역 사용 섹션을 참조하세요.

VPC 피어링

선택한 VPC가 다른 VPC와 피어링되는지 여부에 관계없이 인바운드 또는 아웃바운드 엔드포인트에 대해 AWS 리전의 VPCs. 자세한 내용은 Amazon Virtual Private Cloud(VPC) 피어링을 참조하세요.

공유 서브넷의 IP 주소

인바운드 또는 아웃바운드 엔드포인트를 생성할 때 현재 계정에서 VPC를 생성한 경우에만 공유 서브넷에 IP 주소를 지정할 수 있습니다. 다른 계정이 VPC를 생성하고 VPC의 서브넷을 사용자 계정과 공유하는 경우 해당 서브넷에 IP 주소를 지정할 수 없습니다. 공유 서브넷에 대한 자세한 내용은 Amazon VPC 사용 설명서의 공유 VPC 작업을 참조하세요.

네트워크와 엔드포인트를 생성한 VPC 간의 연결

네트워크와 엔드포인트를 생성한 VPC 사이에 다음 연결 중 하나가 있어야 합니다.

- 인바운드 엔드포인트 - 인바운드 엔드포인트를 생성하는 각 VPC와 네트워크 사이에 AWS Direct Connect 연결 또는 VPN 연결을 설정해야 합니다.
- 아웃바운드 엔드포인트 - 아웃바운드 엔드포인트를 생성하는 각 VPC와 네트워크 사이에 AWS Direct Connect 연결, VPN 연결 또는 NAT(네트워크 주소 변환) 게이트웨이를 설정해야 합니다.

규칙을 공유하면 아웃바운드 엔드포인트도 공유됨

규칙을 생성할 때 Resolver가 DNS 쿼리를 네트워크로 전달하는 데 사용할 아웃바운드 엔드포인트를 지정합니다. 규칙을 다른 AWS 계정과 공유하는 경우 규칙에 지정한 아웃바운드 엔드포인트도 간접적으로 공유합니다. 하나 이상의 AWS 계정을 사용하여 AWS 리전에서 VPCs를 생성한 경우 다음을 수행할 수 있습니다.

- 리전에 하나의 아웃바운드 엔드포인트를 생성합니다.
- 하나의 AWS 계정을 사용하여 규칙을 생성합니다.

- 리전에서 VPCs를 생성한 모든 AWS 계정과 규칙을 공유합니다.

이렇게 하면 VPCs 경우에도 리전의 아웃바운드 엔드포인트 하나를 사용하여 여러 VPCs에서 네트워크로 DNS 쿼리를 전달할 수 있습니다. AWS

엔드포인트 프로토콜 선택

엔드포인트 프로토콜은 데이터를 인바운드 엔드포인트로 전송하는 방식과 아웃바운드 엔드포인트에서 데이터를 전송하는 방식을 결정합니다. VPC 트래픽에 대한 DNS 쿼리를 암호화할 필요는 없습니다. 네트워크의 모든 패킷 흐름은 전송 및 전달되기 전에 올바른 소스와 대상을 검증하는 규칙에 따라 개별적으로 승인되기 때문입니다. 송신 엔터티와 수신 엔터티 모두에 의해 특별히 승인되지 않은 상태에서 정보가 개체 간에 임의로 전달되는 것은 거의 불가능합니다. 일치하는 규칙 없이 패킷이 대상으로 라우팅되는 경우 패킷을 삭제합니다. 자세한 내용은 VPC 기능을 참조하세요.

사용 가능한 프로토콜은 다음과 같습니다:

- Do53: 포트 53를 통한 DNS 입니다. 데이터는 추가 암호화 없이 Route 53 Resolver를 사용하여 릴레이됩니다. 외부 당사자가 데이터를 읽을 수는 없지만 AWS 네트워크 내에서 데이터를 볼 수 있습니다. UDP 또는 TCP를 사용하여 패킷을 전송합니다. Do53는 주로 Amazon VPC 내부 및 Amazon VPC 간의 트래픽에 사용합니다.
- DoH: 데이터는 암호화된 HTTPS 세션을 통해 전송됩니다. DoH는 권한 없는 사용자가 데이터를 해독할 수 없고 의도한 수신자 외에는 누구도 읽을 수 없도록 보안 수준을 강화합니다.
- DoH-FIPS: 데이터를 FIPS 140-2 암호화 표준을 준수하는 암호화된 HTTPS 세션을 통해 전송합니다. 인바운드 엔드포인트에서만 지원됩니다. 자세한 내용은 FIPS PUB 140-2를 참조하세요.

인바운드 엔드포인트의 경우 다음과 같이 프로토콜을 적용할 수 있습니다.

- Do53과 DoH를 함께 사용합니다.
- Do53과 DoH-FIP를 함께 사용합니다.
- Do53를 단독으로 사용합니다.
- DoH를 단독으로 사용합니다.
- DoH FIPS를 단독으로 사용합니다.
- 없음. Do53으로 취급됩니다.

아웃바운드 엔드포인트의 경우 다음과 같이 프로토콜을 적용할 수 있습니다.

- Do53과 DoH를 함께 사용합니다.
- Do53를 단독으로 사용합니다.
- DoH를 단독으로 사용합니다.
- 없음. Do53으로 취급됩니다.

인바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값 및 아웃바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값도 참조하십시오.

전용 인스턴스 테넌시용으로 구성된 VPC에서 Resolver 사용

Resolver 엔드포인트를 생성하는 경우 인스턴스 테넌시 속성이 `dedicated`로 설정된 VPC는 지정할 수 없습니다. Resolver는 단일 테넌트 하드웨어에서 실행되지 않습니다.

그래도 Resolver를 사용하여 VPC에서 발생한 DNS 쿼리를 해석할 수 있습니다. 인스턴스 테넌시 속성이 `default`로 설정된 VPC를 최소한 하나 이상 생성하고, 인바운드 및 아웃바운드 엔드포인트를 생성할 때 해당 VPC를 지정합니다.

전달 규칙을 생성할 때 인스턴스 테넌시 속성 설정과 상관없이 규칙을 어떠한 VPC에든 연결할 수 있습니다.

Route 53 Resolver 가용성 및 크기 조정

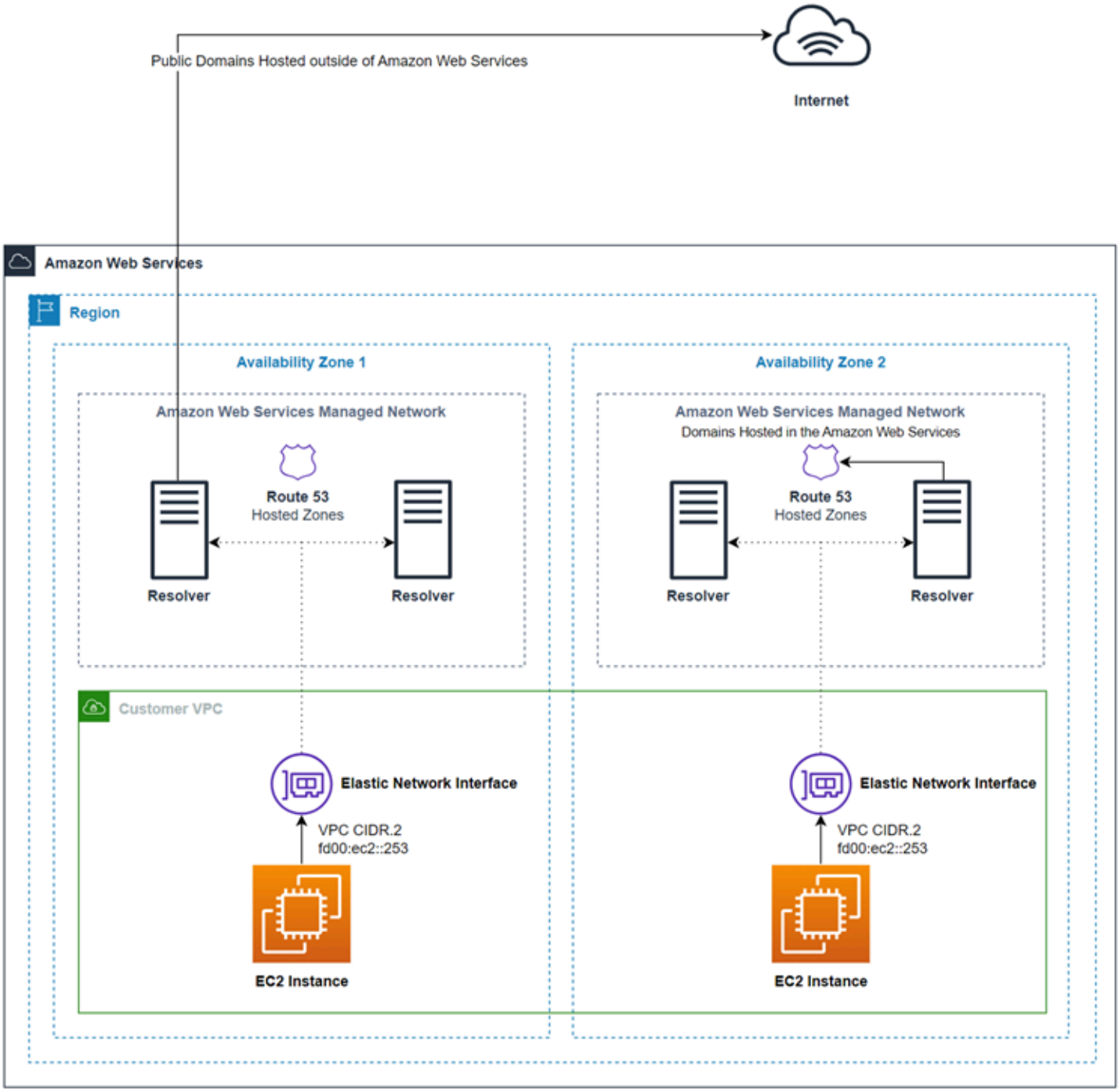
Amazon VPC CIDR + 2 주소와 fd00:ec2::253에서 실행되는Amazon Route 53 Resolver는 퍼블릭 레코드, Amazon VPC별 DNS 이름, Route 53 프라이빗 호스팅 영역에 관한 DNS 쿼리에 재귀적으로 응답하며 모든 VPC에서 기본적으로 사용할 수 있습니다. Route 53 Resolver에는 Nitro Resolver 서비스와 Zonal Resolver 플릿이라는 두 가지 고가용성 구성 요소가 있으며, 이는 사용자에게 투명합니다. Nitro Resolver 서비스는 Nitro 인스턴스의 Nitro Card와 이전 세대 인스턴스의 Dom0에서 실행되며 호스트 서버의 로컬에서 Route 53 Resolver로 전송되는 패킷을 사용하는 서비스입니다. 자세한 내용은 AWS Nitro 시스템의 보안 설계를 참조하세요.

Nitro Resolver 서비스는 인스턴스가 단기간에 수행하는 반복 쿼리에 응답하여 지연 시간을 줄이는 데 도움이 되는 로컬 캐시를 제공합니다. Nitro Resolver 서비스가 캐시된 응답이 없는 쿼리를 수신하면 일반적으로 인스턴스와 동일한 가용 영역에 있는 고가용성 Resolver 플릿인 Zonal Resolver 플릿에 쿼리를 전달합니다. 업스트림 이름 서버 또는 경로의 다른 구성 요소에 의한 쿼리를 처리하는 데 실패하는 경우 Nitro Resolver 서비스는 인스턴스에서 실행되는 워크로드에 영향을 주지 않고 이러한 실패를 투명하게 처리할 수 있는 경우가 많습니다. 또한 Resolver가 도메인 이름 서버에서 쿼리 제한 시간, 거부

된 연결 또는 SERVFAILS가 발생하는 경우 가용성을 개선하기 위해 TTL(Time-To-Live) 값을 초과하는 캐시된 응답으로 응답할 수 있습니다. Nitro Resolver 서비스와 Zonal Resolver 플릿 간의 쿼리는 고객 VPC 외부에서 엄격하게 제어되는 네트워크로 제한되며, 이는 고객이 액세스할 수 없고 엄격한 보안 제어가 적용됩니다. Nitro Resolver 서비스와 VPC 외부의 Zonal Resolver 플릿 간의 쿼리를 처리하면 고객은 VPC 내에서 DNS 쿼리를 가로채지 못합니다. 외부의 이름 서버로 향하는 쿼리 AWS 는 영역 해석기 플릿에 속한 퍼블릭 IP 주소에서 시작되는 퍼블릭 인터넷을 통과합니다. 현재 EDNS0-Client 서브넷 속성은 지원되지 않습니다. 즉, 퍼블릭 DNS 이름 서버로 향하는 모든 쿼리에는 원래 고객 IP 주소에 대한 정보가 포함되지 않습니다.

Nitro Resolver 서비스는 인스턴스의 Link-Local 서비스의 일부입니다. Link-Local 서비스에는 Route 53 Resolver, Amazon Time Service(NTP), 인스턴스 메타데이터 서비스(IMDS), Windows Licensing Service(Windows 인스턴스용)가 포함됩니다. 이 서비스는 VPC에서 생성하는 각 탄력적 네트워크 인터페이스에 따라 확장되며, 각 네트워크 인터페이스는 Link-Local 서비스로 향하는 초당 1,024개의 패킷(PPS)을 허용합니다. 이 제한을 초과하는 패킷은 거부됩니다. ethtool에서 반환한 `linklocal_allowance_exceeded` 값에서 이 제한을 초과했는지 확인할 수 있습니다. ethtool에 대한 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EC2 인스턴스의 네트워크 성능 모니터링을 참조하세요. 이 지표는 CloudWatch Agent에서 CloudWatch 지표에 보고할 수도 있습니다. Route 53 Resolver는 네트워크 인터페이스별로 구현되므로 더 많은 가용 영역에 인스턴스를 추가할수록 확장되고 안정성이 향상됩니다. 쿼리 수에는 VPC당 집계 제한이 없으므로 Route 53 Resolver는 네트워크 주소 사용량(NAU)을 기반으로 하는 VPC의 경계 내에서 조정할 수 있습니다. 자세한 내용은 Amazon Virtual Private Cloud 사용 설명서의 VPC의 네트워크 주소 사용량을 참조하세요.

다음 다이어그램은 Route 53 Resolver가 가용 영역 내에서 DNS 쿼리를 해결하는 방법에 대한 개요를 보여줍니다.



Route 53 Resolver 시작하기

Route 53 Resolver 콘솔에는 다음과 같은 Resolver 시작 단계를 안내하는 마법사가 있습니다.

- 엔드포인트 생성: 인바운드, 아웃바운드 또는 둘 다

- 아웃바운드 엔드포인트에 대해, DNS 쿼리를 네트워크로 라우팅하려는 도메인 이름을 지정하는 전달 규칙을 하나 이상 생성합니다.
- 아웃바운드 엔드포인트를 생성한 경우 규칙을 연결하려는 VPC를 선택합니다.

마법사를 사용하여 Route 53 Resolver를 구성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53resolver/ Resolver 콘솔을 엽니다.
2. Route 53 Resolver 시작 페이지에서 엔드포인트 구성을 선택합니다.
3. 탐색 모음에서 해석기 엔드포인트를 생성할 리전을 선택합니다.
4. 기본 구성에서 DNS 쿼리를 전달할 방향을 선택합니다.
   - Inbound and outbound(인바운드 및 아웃바운드): 네트워크에 있는 해석기에서 VPC의 Resolver로 DNS 쿼리를 전달하고 VPC에서 네트워크에 있는 해석기로 지정된 쿼리(예: example.com 또는 example.net)를 전달할 수 있는 설정을 마법사가 안내합니다.
   - Inbound only(인바운드 전용): 네트워크에 있는 해석기에서 VPC의 Resolver로 DNS 쿼리를 전달할 수 있는 설정을 마법사가 안내합니다.
   - Outbound only(아웃바운드 전용): VPC에서 네트워크에 있는 해석기로 지정된 쿼리를 전달할 수 있는 설정을 마법사가 안내합니다.
5. Next(다음)를 선택합니다.
6. Inbound and outbound(인바운드 및 아웃바운드)나 Inbound only(인바운드 전용)를 선택할 경우 인바운드 엔드포인트를 구성하기 위한 해당 값을 입력합니다. 그런 다음 7단계로 진행합니다. 자세한 내용은 인바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값 섹션을 참조하세요.

   Outbound only(아웃바운드 전용)를 선택할 경우 7단계로 건너뜁니다.
7. 아웃바운드 엔드포인트를 구성하기 위한 해당 값을 입력합니다. 자세한 내용은 아웃바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값 섹션을 참조하세요.
8. Inbound and outbound(인바운드 및 아웃바운드)나 Outbound only(아웃바운드 전용)를 선택할 경우 규칙을 생성하기 위한 해당 값을 입력합니다. 자세한 내용은 규칙을 생성 또는 편집할 때 지정하는 값 섹션을 참조하세요.
9. Review and create(검토 및 생성) 페이지에서 이전 단계에서 지정한 설정이 올바르다는 것을 확인합니다. 필요한 경우 해당 섹션에 대해 편집을 선택하고 설정을 업데이트합니다. 설정에 만족하면 제출을 클릭합니다.

> **Note**
>
> 아웃바운드 엔드포인트를 생성하는 데 1~2분이 걸립니다. 첫 번째 아웃바운드 엔드포인트가 생성될 때까지는 다른 아웃바운드 엔드포인트를 생성할 수 없습니다.

10. 규칙을 더 생성하려면 전달 규칙 관리 섹션을 참조하세요.
11. 인바운드 엔드포인트를 만들었으면 해당 DNS 쿼리를 인바운드 엔드포인트의 IP 주소로 전달하도록 네트워크의 DNS 해석기를 구성합니다. 자세한 내용은 DNS 애플리케이션 설명서를 참조하세요.

VPC로 인바운드 DNS 쿼리 전달

네트워크에서 Resolver로 DNS 쿼리를 전달하려면 인바운드 엔드포인트를 생성합니다. 인바운드 엔드포인트는 네트워크의 DNS 해석기가 DNS 쿼리를 전달할 IP 주소(VPC에서 사용할 수 있는 IP 주소 범위)를 지정합니다. 이러한 IP 주소는 퍼블릭 IP 주소가 아니므로 각 인바운드 엔드포인트에 대해 AWS Direct Connect 연결 또는 VPN 연결을 사용하여 VPC를 네트워크에 연결해야 합니다.

주제

- 인바운드 전달 구성
- 인바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값

인바운드 전달 구성

인바운드 엔드포인트를 생성하려면 다음 절차를 수행하세요.

인바운드 엔드포인트를 생성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 Inbound endpoints(인바운드 엔드포인트)를 선택합니다.
3. 탐색 모음에서 인바운드 엔드포인트를 생성할 리전을 선택합니다.
4. Create inbound endpoint(인바운드 엔드포인트 생성)를 선택합니다.
5. 관련 값들을 입력합니다. 자세한 내용은 인바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값 섹션을 참조하세요.
6. 생성을 선택합니다.

7. 해당 DNS 쿼리를 인바운드 엔드포인트의 IP 주소로 전달하도록 네트워크의 DNS 해석기를 구성합니다. 자세한 내용은 DNS 애플리케이션 설명서를 참조하세요.

인바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값

인바운드 엔드포인트를 생성하거나 편집할 때 다음 값을 지정합니다.

Outpost ID

AWS Outposts VPC에서 Resolver에 대한 엔드포인트를 생성하는 경우 ID입니다 AWS Outposts .

엔드포인트 이름

기억하기 쉬운 이름을 사용하면 대시보드에서 인바운드 엔드포인트를 쉽게 찾을 수 있습니다.

region-name 리전에 있는 VPC

네트워크의 모든 인바운드 DNS 쿼리가 Resolver로 가는 중에 이 VPC를 통과합니다.

이 엔드포인트에 대한 보안 그룹

이 VPC에 대한 액세스를 제어하는 데 사용할 보안 그룹 하나 이상의 ID. 지정한 보안 그룹에는 인바운드 규칙이 하나 이상 포함되어야 합니다. 인바운드 규칙은 포트 53에서 TCP 및 UDP 액세스를 허용해야 합니다. 엔드포인트를 만든 후에는 이 값을 변경할 수 없습니다.

일부 보안 그룹 규칙으로 인해 연결이 추적되고 인바운드 엔드포인트에 대한 IP 주소별 초당 최대 쿼리 수는 최소 1,500개가 될 수 있습니다. 보안 그룹으로 인한 연결 추적을 방지하려면 추적되지 않은 연결을 참조하세요.

> **Note**
>
> 여러 보안 그룹을 추가하려면 AWS CLI 명령을 사용합니다`create-resolver-endpoint`. 자세한 내용은 create-resolver-endpoint를 참조하세요.

자세한 내용은 Amazon VPC 사용 설명서의 VPC의 보안 그룹을 참조하세요.

엔드포인트 유형

엔드포인트 유형은 IPv4, IPv6 또는 듀얼 스택 IP 주소일 수 있습니다. 듀얼 스택 엔드포인트의 경우, 엔드포인트는 네트워크의 DNS 해석기가 DNS 쿼리를 전달할 수 있는 IPv4 및 IPv6 주소를 모두 갖게 됩니다.

> **Note**
>
> 보안상의 이유로 모든 듀얼 스택 및 IPv6 IP 주소에 대한 퍼블릭 인터넷의 직접 IPv6 트래픽 액세스를 거부합니다.

IP 주소

네트워크에 있는 DNS 해석기가 DNS 쿼리를 전달할 IP 주소입니다. 중복성을 위해 최소 두 개의 IP 주소를 지정해야 합니다. 다음을 참조하세요.

복수 가용 영역

최소한 2개의 가용 영역에 IP 주소를 지정하는 것이 좋습니다. 선택적으로 그러한 가용 영역 또는 다른 가용 영역에 추가 IP 주소를 지정할 수 있습니다.

IP 주소 및 Amazon VPC 탄력적 네트워크 인터페이스

지정한 가용 영역, 서브넷 및 IP 주소의 각 조합에 대해 Resolver는 Amazon VPC 탄력적 네트워크 인터페이스를 생성합니다. 엔드포인트의 IP 주소별 초당 최대 동시 DNS 쿼리 수는 Route 53 Resolver의 할당량 섹션을 참조하세요. 각 탄력적 네트워크 인터페이스의 요금에 대한 정보는 Amazon Route 53 요금 페이지의 "Amazon Route 53"을 참조하십시오.

> **Note**
>
> Resolver 엔드포인트에는 프라이빗 IP 주소가 있습니다. 이러한 IP 주소는 엔드포인트의 수명 기간 동안 변경되지 않습니다.

IP 주소마다 다음 값을 지정하세요. VPC in the region-name Region(region-name 리전에 있는 VPC)에서 지정한 VPC의 가용 영역에 각 IP 주소가 있어야 합니다.

가용 영역

DNS 쿼리가 VPC로 가는 도중 통과할 가용 영역. 지정한 가용 영역을 서브넷으로 구성해야 합니다.

서브넷

Resolver 엔드포인트 ENI에 할당하려는 IP 주소가 포함된 서브넷입니다. 이 주소로 DNS 쿼리가 전송됩니다. 서브넷에는 사용 가능한 IP 주소가 있어야 합니다.

서브넷 IP 주소는 엔드포인트 유형과 일치해야 합니다.

IP 주소

DNS 쿼리를 전달하려는 IP 주소입니다.

Resolver가 지정된 서브넷의 사용 가능한 IP 주소 중에서 자동으로 IP 주소를 선택하도록 할지, 아니면 직접 IP 주소를 지정할지 선택합니다.

IP 주소를 직접 지정하기로 선택할 경우 IPv4 주소나 IPv6 주소 또는 두 주소를 모두 입력합니다.

프로토콜

엔드포인트 프로토콜은 데이터를 인바운드 엔드포인트로 전송하는 방식을 결정합니다. 필요한 보안 수준에 따라 프로토콜을 하나 이상 선택합니다.

- Do53: (기본값) 추가 암호화 없이 Route 53 Resolver를 사용하여 데이터가 릴레이됩니다. 외부 당사자가 데이터를 읽을 수는 없지만 AWS 네트워크 내에서는 볼 수 있습니다.
- DoH: 데이터는 암호화된 HTTPS 세션을 통해 전송됩니다. DoH는 권한 없는 사용자가 데이터를 해독할 수 없고 의도한 수신자 외에는 누구도 읽을 수 없도록 보안 수준을 강화합니다.
- DoH-FIPS: 데이터를 FIPS 140-2 암호화 표준을 준수하는 암호화된 HTTPS 세션을 통해 전송합니다. 인바운드 엔드포인트에서만 지원됩니다. 자세한 내용은 FIPS PUB 140-2를 참조하세요.

> **Note**
>
> DoH/DoH-FIPS 인바운드 엔드포인트의 경우 Route 53 Resolver 쿼리 로깅에 잘못된 소스 IP가 게시되는 데 알려진 문제가 있습니다.

인바운드 엔드포인트의 경우 다음과 같이 프로토콜을 적용할 수 있습니다.

- Do53과 DoH를 함께 사용합니다.
- Do53과 DoH-FIP를 함께 사용합니다.
- Do53를 단독으로 사용합니다.
- DoH를 단독으로 사용합니다.
- DoH FIPS를 단독으로 사용합니다.
- 없음. Do53으로 취급됩니다.

> **Important**
>
> 인바운드 엔드포인트의 프로토콜을 Do53 전용에서 DoH 전용 또는 DoH-FIPS 전용으로 직접 변경할 수 없습니다. 이는 Do53를 사용하는 수신 트래픽이 갑자기 중단되는 것을 방지

하기 위한 것입니다. 프로토콜을 Do53에서 DoH 또는 DoH-FIP로 변경하려면 먼저 Do53과 DoH 또는 Do53과 DoH-FIP를 모두 활성화하여 모든 수신 트래픽이 DoH 프로토콜 또는 DoH-FIP를 사용하도록 전송되었는지 확인한 다음 Do53를 제거해야 합니다.

Tags

한 개 이상의 키와 해당 값을 지정합니다. 예를 들어 키에 Cost center를 지정하고 값에 456을 지정할 수 있습니다.

네트워크로 아웃바운드 DNS 쿼리 전달

하나 이상의 VPC에 있는 Amazon EC2 인스턴스에서 시작된 DNS 쿼리를 네트워크에 전달하려면, 하나의 아웃바운드 엔드포인트 및 하나 이상의 규칙을 생성합니다.

아웃바운드 엔드포인트

VPC에서 네트워크로 DNS 쿼리를 전달하려면 아웃바운드 엔드포인트를 생성합니다. 아웃바운드 엔드포인트는 쿼리가 시작되는 IP 주소를 지정합니다. VPC에서 사용할 수 있는 IP 주소 범위에서 선택하는 IP 주소는 퍼블릭 IP 주소가 아닙니다. 즉, 각 아웃바운드 엔드포인트에 대해 AWS Direct Connect 연결, VPC 연결 또는 NAT(네트워크 주소 변환) 게이트웨이를 사용하여 VPC를 네트워크에 연결해야 합니다. 동일한 리전에서 여러 VPC에 대해 동일한 아웃바운드 엔드포인트를 사용하거나 여러 아웃바운드 엔드포인트를 생성할 수 있습니다. 아웃바운드 엔드포인트에서 DNS64를 사용하하기를 원하는 경우, Amazon Virtual Private Cloud를 사용하여 DNS64를 활성화할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 DNS64 및 NAT64를 참조하십시오.

Route 53 Resolver 규칙의 대상 IP는 Resolver에서 무작위로 선택하며, 다른 IP보다 특정 대상 IP를 선택하는 것은 선호되지 않습니다. 대상 IP가 전달된 DNS 요청에 응답하지 않으면 Resolver는 대상 IP 중에서 무작위 IP 주소로 다시 시도합니다.

해석기 엔드포인트에서 모든 대상 IP 주소에 연결할 수 있는지 확인합니다. Resolver가 아웃바운드 DNS 쿼리를 대상 IP로 전달할 수 없는 경우 DNS 확인 시간이 길어질 수 있습니다.

규칙

네트워크에 있는 DNS 해석기에 전달할 쿼리의 도메인 이름을 지정하려면 규칙을 한 개 이상 생성합니다. 각 규칙은 도메인 이름 하나를 지정합니다. 그런 다음 쿼리를 네트워크에 전달할 VPC에 규칙을 연결합니다.

자세한 정보는 다음 주제를 참조하세요.

- Private hosted zones that have overlapping namespaces
- Private hosted zones and Route 53 Resolver rules

아웃바운드 전달 구성

VPC에서 시작된 DNS 쿼리를 네트워크에 전달하도록 Resolver를 구성하려면 다음 절차를 수행하세요.

> **Important**
>
> 아웃바운드 엔드포인트를 생성한 후 규칙을 한 개 이상 만들고 VPC 한 개 이상에 연결해야 합니다. 규칙은 네트워크에 전달할 DNS 쿼리의 도메인 이름을 지정합니다.

아웃바운드 엔드포인트를 생성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 Outbound endpoints(아웃바운드 엔드포인트)를 선택합니다.
3. 탐색 모음에서 아웃바운드 엔드포인트를 생성할 리전을 선택합니다.
4. Create outbound endpoint(아웃바운드 엔드포인트 생성)를 선택합니다.
5. 관련 값들을 입력합니다. 자세한 내용은 아웃바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값 섹션을 참조하세요.
6. 생성(Create)을 선택합니다.

   > **Note**
   >
   > 아웃바운드 엔드포인트를 생성하는 데 1~2분이 걸립니다. 첫 번째 아웃바운드 엔드포인트가 생성될 때까지는 다른 아웃바운드 엔드포인트를 생성할 수 없습니다.

7. 규칙을 한 개 이상 생성하여 네트워크에 전달할 DNS 쿼리의 도메인 이름을 지정합니다. 자세한 내용은 다음 절차를 참조하세요.

전달 규칙을 한 개 이상 생성하려면 다음 절차를 수행하세요.

전달 규칙을 생성하고 VPC 한 개 이상에 규칙을 연결하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 규칙(Rules)을 선택합니다.
3. 탐색 모음에서 규칙을 생성하려는 리전을 선택합니다.
4. 규칙 생성을 선택합니다.
5. 관련 값들을 입력합니다. 자세한 내용은 규칙을 생성 또는 편집할 때 지정하는 값 섹션을 참조하세요.
6. 저장을 선택합니다.
7. 다른 규칙을 추가하려면 4-6단계를 반복합니다.

아웃바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값

아웃바운드 엔드포인트를 생성하거나 편집할 때 다음 값을 지정합니다.

Outpost ID

AWS Outposts VPC에서 Resolver에 대한 엔드포인트를 생성하는 경우 ID입니다 AWS Outposts .

엔드포인트 이름

기억하기 쉬운 이름을 사용하면 대시보드에서 아웃바운드 엔드포인트를 쉽게 찾을 수 있습니다.

region-name 리전에 있는 VPC

모든 아웃바운드 DNS 쿼리는 네트워크로 가는 도중 이 VPC를 통과합니다.

이 엔드포인트에 대한 보안 그룹

이 VPC에 대한 액세스를 제어하는 데 사용할 보안 그룹 하나 이상의 ID. 지정한 보안 그룹에는 아웃바운드 규칙이 하나 이상 포함되어야 합니다. 아웃바운드 규칙은 네트워크에 있는 DNS 쿼리에 사용하는 포트에서 TCP 및 UDP 액세스를 허용해야 합니다. 엔드포인트를 만든 후에는 이 값을 변경할 수 없습니다.

일부 보안 그룹 규칙으로 인해 연결이 추적되고 아웃바운드 엔드포인트에서 대상 이름 서버까지 초당 최대 쿼리에 영향을 미칠 수 있습니다. 보안 그룹으로 인한 연결 추적을 방지하려면 추적되지 않은 연결을 참조하세요.

자세한 내용은 Amazon VPC 사용 설명서의 VPC의 보안 그룹을 참조하세요.

엔드포인트 유형

엔드포인트 유형은 IPv4, IPv6 또는 듀얼 스택 IP 주소일 수 있습니다. 듀얼 스택 엔드포인트의 경우, 엔드포인트는 네트워크의 DNS 해석기가 DNS 쿼리를 전달할 수 있는 IPv4 및 IPv6 주소를 모두 갖게 됩니다.

> **Note**
>
> 보안상의 이유로 모든 듀얼 스택 및 IPv6 IP 주소에 대해 퍼블릭 인터넷으로의 직접 IPv6 트래픽 액세스를 거부합니다.

IP 주소

Resolver가 네트워크에 있는 해석기로 가는 도중 DNS 쿼리를 전달할 VPC의 IP 주소입니다. 이 주소는 네트워크에 있는 DNS 해석기의 IP 주소가 아닙니다. VPC 하나 이상에 연결할 규칙을 생성할 때 해석기 IP 주소를 지정합니다. 중복성을 위해 최소 두 개의 IP 주소를 지정해야 합니다.

> **Note**
>
> Resolver 엔드포인트에는 프라이빗 IP 주소가 있습니다. 이러한 IP 주소는 엔드포인트의 수명 기간 동안 변경되지 않습니다.

다음 사항에 유의하세요.

복수 가용 영역

최소한 2개의 가용 영역에 IP 주소를 지정하는 것이 좋습니다. 선택적으로 그러한 가용 영역 또는 다른 가용 영역에 추가 IP 주소를 지정할 수 있습니다.

IP 주소 및 Amazon VPC 탄력적 네트워크 인터페이스

지정한 가용 영역, 서브넷 및 IP 주소의 각 조합에 대해 Resolver는 Amazon VPC 탄력적 네트워크 인터페이스를 생성합니다. 엔드포인트의 IP 주소별 초당 최대 동시 DNS 쿼리 수는 Route 53 Resolver의 할당량 섹션을 참조하세요. 각 탄력적 네트워크 인터페이스의 요금에 대한 정보는 Amazon Route 53 요금 페이지의 "Amazon Route 53"을 참조하십시오.

IP 주소 순서

IP 주소는 순서에 상관없이 지정할 수 있습니다. DNS 쿼리를 전달할 때 Resolver에서는 IP 주소가 나열되는 순서에 따라 IP 주소를 선택하지 않습니다.

IP 주소마다 다음 값을 지정하세요. VPC in the region-name Region(region-name 리전에 있는 VPC)에서 지정한 VPC의 가용 영역에 각 IP 주소가 있어야 합니다.

가용 영역

DNS 쿼리가 네트워크로 가는 도중 통과할 가용 영역. 지정한 가용 영역을 서브넷으로 구성해야 합니다.

서브넷

DNS 쿼리가 네트워크로 가는 도중 통과할 IP 주소가 포함된 서브넷입니다. 서브넷에는 사용 가능한 IP 주소가 있어야 합니다.

서브넷 IP 주소는 엔드포인트 유형과 일치해야 합니다.

IP 주소

네트워크로 가는 도중에 DNS 쿼리를 시작하려는 IP 주소입니다.

Resolver가 지정된 서브넷의 사용 가능한 IP 주소 중에서 자동으로 IP 주소를 선택하도록 할지, 아니면 직접 IP 주소를 지정할지 선택합니다.

IP 주소를 직접 지정하기로 선택할 경우 IPv4 주소나 IPv6 주소 또는 두 주소를 모두 입력합니다.

프로토콜

엔드포인트 프로토콜은 아웃바운드 엔드포인트에서 데이터를 전송하는 방식을 결정합니다. 필요한 보안 수준에 따라 프로토콜을 하나 이상 선택합니다.

- Do53: (기본값) 추가 암호화 없이 Route 53 Resolver를 사용하여 데이터가 릴레이됩니다. 외부 당사자가 데이터를 읽을 수는 없지만 AWS 네트워크 내에서는 볼 수 있습니다.
- DoH: 데이터는 암호화된 HTTPS 세션을 통해 전송됩니다. DoH는 권한 없는 사용자가 데이터를 해독할 수 없고 의도한 수신자 외에는 누구도 읽을 수 없도록 보안 수준을 강화합니다.

아웃바운드 엔드포인트의 경우 다음과 같이 프로토콜을 적용할 수 있습니다.

- Do53과 DoH를 함께 사용합니다.
- Do53를 단독으로 사용합니다.
- DoH를 단독으로 사용합니다.
- 없음. Do53으로 취급됩니다.

Tags

한 개 이상의 키와 해당 값을 지정합니다. 예를 들어 키에 Cost center를 지정하고 값에 456을 지정할 수 있습니다.

규칙을 생성 또는 편집할 때 지정하는 값

전달 규칙을 생성하거나 편집할 때 다음 값을 지정합니다.

규칙 이름

기억하기 쉬운 이름을 사용하면 대시보드에서 규칙을 쉽게 찾을 수 있습니다.

규칙 타입

해당되는 값을 선택합니다.

- 전달 - 지정된 도메인 이름의 DNS 쿼리를 네트워크의 해석기에 전달하려는 경우 이 옵션을 선택합니다.
- 시스템 - Resolver가 전달 규칙에 정의된 동작을 선택적으로 재정의하게 하려는 경우 이 옵션을 선택합니다. 시스템 규칙을 생성할 때 Resolver가 지정된 하위 도메인의 DNS 쿼리를 해석합니다. 그렇지 않을 경우 네트워크의 DNS 해석기가 해석합니다.

기본적으로 전달 규칙은 도메인 이름과 모든 하위 도메인에 적용됩니다. 도메인에 대한 쿼리를 네트워크에 있는 해석기에 전달하되 일부 하위 도메인에 대한 쿼리는 제외하려면 하위 도메인에 대한 시스템 규칙을 생성합니다. 예를 들어 example.com의 전달 규칙을 생성하고 acme.example.com에 대한 쿼리를 전달하지 않으려면 시스템 규칙을 생성하고 도메인 이름에 acme.example.com을 지정합니다.

이 규칙을 사용하는 VPC

이 규칙을 사용하여 지정된 도메인 이름에 대한 DNS 쿼리를 전달하는 VPC. 원하는 만큼 VPC에 규칙을 적용할 수 있습니다.

도메인 이름

이 도메인 이름에 대한 DNS 쿼리는 대상 IP 주소에 지정한 IP 주소로 전송됩니다. 자세한 내용은 Resolver가 쿼리의 도메인 이름이 규칙과 일치하는지 확인하는 방법 섹션을 참조하세요.

아웃바운드 엔드포인트

Resolver는 여기에 지정한 아웃바운드 엔드포인트를 통해 대상 IP 주소에서 지정된 IP 주소로 DNS 쿼리를 전달합니다.

대상 IP 주소

DNS 쿼리가 도메인 이름에 지정된 이름과 일치하면 아웃바운드 엔드포인트가 여기에 지정된 IP 주소로 쿼리를 전달합니다. 일반적으로 네트워크에 있는 DNS 해석기의 IP 주소입니다.

Target IP addresses(대상 IP 주소)는 규칙 유형 값이 전달일 경우에만 사용할 수 있습니다.

IPv4 또는 IPv6 주소, 프로토콜, 엔드포인트에 사용할 ServerNameIndication을 지정합니다. ServerNameIndication은 선택한 프로토콜이 DoH인 경우에만 적용됩니다.

아웃바운드 엔드포인트를 통해 네트워크에 있는 DoH Resolver FQDN의 대상 IP 주소 확인은 지원되지 않습니다. 아웃바운드 엔드포인트는 DoH 쿼리를 전달할 네트워크에 있는 DoH Resolver의 대상 IP 주소가 필요합니다. 네트워크의 DoH Resolver에서 TLS SNI 및 HTTP 호스트 헤더에 FQDN이 필요한 경우 ServerNameIndication을 제공해야 합니다.

ServerNameIndication

쿼리를 전달할 DoH 서버의 Server Name Indication입니다. 이는 프로토콜이 DoH인 경우에만 사용됩니다.

Tags

한 개 이상의 키와 해당 값을 지정합니다. 예를 들어 키에 Cost center를 지정하고 값에 456을 지정할 수 있습니다.

청구서를 구성하기 위해에서 AWS Billing and Cost Management 제공하는 태그입니다 AWS . 비용 할당 태그 사용에 대한 자세한 내용은 AWS Billing 사용 설명서의 비용 할당 태그 사용을 참조하세요.

인바운드 엔드포인트 관리

인바운드 엔드포인트를 관리하려면 해당 절차를 수행하세요.

주제

- 인바운드 엔드포인트 보기 및 편집
- 인바운드 엔드포인트의 상태 보기
- 인바운드 엔드포인트 삭제

인바운드 엔드포인트 보기 및 편집

인바운드 엔드포인트의 설정을 보고 편집하려면 다음 절차를 수행하세요.

인바운드 엔드포인트의 설정을 보고 편집하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 Inbound endpoints(인바운드 엔드포인트)를 선택합니다.
3. 탐색 모음에서 인바운드 엔드포인트를 생성한 리전을 선택합니다.
4. 설정을 보거나 편집할 엔드포인트의 옵션을 선택합니다.
5. 세부 정보 보기 또는 편집을 선택합니다.

   인바운드 엔드포인트의 값에 대한 자세한 내용은 인바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값을 참조하세요.
6. 편집을 선택한 경우 해당 값을 입력하고 저장을 선택합니다.

인바운드 엔드포인트의 상태 보기

인바운드 엔드포인트의 상태를 보려면 다음 절차를 수행합니다.

인바운드 엔드포인트의 상태를 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 Inbound endpoints(인바운드 엔드포인트)를 선택합니다.
3. 탐색 모음에서 인바운드 엔드포인트를 생성한 리전을 선택합니다. 상태 열에는 다음 값 중 하나가 포함됩니다.

   [생성 중]

   Resolver가 이 엔드포인트에 대해 하나 이상의 Amazon VPC 네트워크 인터페이스를 생성 및 구성하고 있습니다.

   Operational(작동)

   이 엔드포인트의 Amazon VPC 네트워크 인터페이스가 올바르게 구성되어 있고 네트워크와 Resolver 사이의 인바운드 또는 아웃바운드 DNS 쿼리를 전달할 수 있습니다.

   업데이트 중

   하나 이상의 네트워크 인터페이스를 이 엔드포인트와 연결 또는 연결 해제하는 중입니다.

Auto recovering(자동 복구 중)

Resolver가 이 엔드포인트와 연결된 네트워크 인터페이스 중 하나 이상을 복구하려고 합니다. 복구 프로세스 중 IP 주소당(네트워크 인터페이스당) DNS 쿼리 수의 제한 때문에 엔드포인트가 제한된 용량으로 작동합니다. 현재 제한은 Route 53 Resolver의 할당량 섹션을 참조하세요.

작업 필요

이 엔드포인트가 정상 상태가 아니므로 Resolver가 자동으로 복구할 수 없습니다. 문제를 해결하려면 엔드포인트와 연관된 각 IP 주소를 점검하는 것이 좋습니다. 사용할 수 없는 각 IP 주소에 대해 다른 IP 주소를 추가한 다음 사용할 수 없는 IP 주소를 삭제하세요. 엔드포인트에는 항상 두 개 이상의 IP 주소가 포함되어야 합니다. 작업 필요 상태에는 다양한 원인이 있을 수 있습니다. 일반적인 두 가지 원인은 다음과 같습니다.

- 엔드포인트와 연결된 하나 이상의 네트워크 인터페이스가 Amazon VPC를 사용하여 삭제되었습니다.
- Resolver의 제어를 벗어난 어떤 이유로 인해 네트워크 인터페이스를 생성할 수 없습니다.

[삭제 중]

해석기가 이 엔드포인트 및 연관된 네트워크 인터페이스를 삭제하고 있습니다.

인바운드 엔드포인트 삭제

인바운드 엔드포인트를 삭제하려면 다음 절차를 수행하세요.

> **Important**
>
> 인바운드 엔드포인트를 삭제하면 더 이상 네트워크의 DNS 쿼리가 엔드포인트에 지정된 VPC의 Resolver로 전달되지 않습니다.

인바운드 엔드포인트를 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 Inbound endpoints(인바운드 엔드포인트)를 선택합니다.
3. 탐색 모음에서 인바운드 엔드포인트를 생성한 리전을 선택합니다.
4. 삭제할 엔드포인트의 옵션을 선택합니다.

5. Delete(삭제)를 선택합니다.
6. 엔드포인트를 삭제하도록 확인하려면 엔드포인트 이름을 입력하고 제출을 선택합니다.

아웃바운드 엔드포인트 관리

아웃바운드 엔드포인트를 관리하려면 해당 절차를 수행하세요.

주제

- 아웃바운드 엔드포인트 보기 및 편집
- 아웃바운드 엔드포인트의 상태 보기
- 아웃바운드 엔드포인트 삭제

아웃바운드 엔드포인트 보기 및 편집

아웃바운드 엔드포인트의 설정을 보고 편집하려면 다음 절차를 수행하세요.

아웃바운드 엔드포인트의 설정을 보고 편집하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 Outbound endpoints(아웃바운드 엔드포인트)를 선택합니다.
3. 탐색 모음에서 아웃바운드 엔드포인트를 생성한 리전을 선택합니다.
4. 설정을 보거나 편집할 엔드포인트의 옵션을 선택합니다.
5. 세부 정보 보기 또는 편집을 선택합니다.

   아웃바운드 엔드포인트의 값에 대한 자세한 내용은 아웃바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값 섹션을 참조하세요.
6. 편집을 선택한 경우 해당 값을 입력한 후 저장을 선택합니다.

아웃바운드 엔드포인트의 상태 보기

아웃바운드 엔드포인트의 상태를 보려면 다음 절차를 수행합니다.

아웃바운드 엔드포인트의 상태를 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 Outbound endpoints(아웃바운드 엔드포인트)를 선택합니다.
3. 탐색 모음에서 아웃바운드 엔드포인트를 생성한 리전을 선택합니다. 상태 열에는 다음 값 중 하나가 포함됩니다.

   [생성 중]

   Resolver가 이 엔드포인트에 대해 하나 이상의 Amazon VPC 네트워크 인터페이스를 생성 및 구성하고 있습니다.

   Operational(작동)

   이 엔드포인트의 Amazon VPC 네트워크 인터페이스가 올바르게 구성되어 있고 네트워크와 Resolver 사이의 인바운드 또는 아웃바운드 DNS 쿼리를 전달할 수 있습니다.

   업데이트 중

   하나 이상의 네트워크 인터페이스를 이 엔드포인트와 연결 또는 연결 해제하는 중입니다.

   Auto recovering(자동 복구 중)

   Resolver가 이 엔드포인트와 연결된 네트워크 인터페이스 중 하나 이상을 복구하려고 합니다. 복구 프로세스 중 IP 주소당(네트워크 인터페이스당) DNS 쿼리 수의 제한 때문에 엔드포인트가 제한된 용량으로 작동합니다. 현재 제한은 Route 53 Resolver의 할당량 섹션을 참조하세요.

   작업 필요

   이 엔드포인트가 정상 상태가 아니므로 Resolver가 자동으로 복구할 수 없습니다. 문제를 해결하려면 엔드포인트와 연관된 각 IP 주소를 점검하는 것이 좋습니다. 사용할 수 없는 각 IP 주소에 대해 다른 IP 주소를 추가한 다음 사용할 수 없는 IP 주소를 삭제하세요. 엔드포인트에는 항상 두 개 이상의 IP 주소가 포함되어야 합니다. 작업 필요 상태에는 다양한 원인이 있을 수 있습니다. 일반적인 두 가지 원인은 다음과 같습니다.

   - 엔드포인트와 연결된 하나 이상의 네트워크 인터페이스가 Amazon VPC를 사용하여 삭제되었습니다.
   - Resolver의 제어를 벗어난 어떤 이유로 인해 네트워크 인터페이스를 생성할 수 없습니다.

   [삭제 중]

   해석기가 이 엔드포인트 및 연관된 네트워크 인터페이스를 삭제하고 있습니다.

아웃바운드 엔드포인트 삭제

엔드포인트를 삭제하려면 VPC와 연결된 모든 규칙부터 먼저 삭제해야 합니다.

아웃바운드 엔드포인트를 삭제하려면 다음 절차를 수행하세요.

> **Important**
>
> 아웃바운드 엔드포인트를 삭제하면 Resolver는 삭제된 아웃바운드 엔드포인트를 지정하는 규칙에 대해 더 이상 DNS 쿼리를 VPC에서 네트워크로 전달하지 않습니다.

아웃바운드 엔드포인트를 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 Outbound endpoints(아웃바운드 엔드포인트)를 선택합니다.
3. 탐색 모음에서 아웃바운드 엔드포인트를 생성한 리전을 선택합니다.
4. 삭제할 엔드포인트의 옵션을 선택합니다.
5. Delete(삭제)를 선택합니다.
6. 엔드포인트를 삭제하도록 확인하려면 엔드포인트 이름을 입력하고 제출을 선택합니다.

전달 규칙 관리

Resolver가 지정된 도메인 이름의 쿼리를 네트워크로 전달하게 하려면 도메인 이름마다 전달 규칙을 하나씩 생성하고 쿼리를 전달할 도메인의 이름을 지정합니다.

주제

- 전달 규칙 보기 및 편집
- 전달 규칙 생성
- 역방향 조회에 대한 규칙 추가
- VPC와 전달 규칙 연결
- VPC에서 전달 규칙 연결 해제
- Resolver 규칙을 다른 AWS 계정과 공유 및 공유 규칙 사용

- 전달 규칙 삭제
- 해석기의 역방향 DNS 쿼리에 대한 전달 규칙

전달 규칙 보기 및 편집

전달 규칙의 설정을 보고 편집하려면 다음 절차를 수행하세요.

전달 규칙에 대한 설정을 보거나 편집하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 규칙(Rules)을 선택합니다.
3. 탐색 모음에서 규칙을 생성한 리전을 선택합니다.
4. 설정을 보거나 편집할 규칙의 옵션을 선택합니다.
5. 세부 정보 보기 또는 편집을 선택합니다.

   전달 규칙의 값에 대한 자세한 내용은 규칙을 생성 또는 편집할 때 지정하는 값을 참조하세요.
6. 편집을 선택한 경우 해당 값을 입력한 후 저장을 선택합니다.

전달 규칙 생성

전달 규칙을 한 개 이상 생성하려면 다음 절차를 수행하세요.

전달 규칙을 생성하고 VPC 한 개 이상에 규칙을 연결하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 규칙(Rules)을 선택합니다.
3. 탐색 모음에서 규칙을 생성하려는 리전을 선택합니다.
4. 규칙 생성을 선택합니다.
5. 관련 값들을 입력합니다. 자세한 내용은 규칙을 생성 또는 편집할 때 지정하는 값 섹션을 참조하세요.
6. 저장을 선택합니다.
7. 다른 규칙을 추가하려면 4-6단계를 반복합니다.

역방향 조회에 대한 규칙 추가

VPC에서 역방향 조회를 제어해야 하는 경우 아웃바운드 해석기 엔드포인트에 규칙을 추가할 수 있습니다.

역방향 조회 규칙을 생성하려면

1. 이전 절차의 단계에 따라 5단계까지 수행합니다.
2. 규칙을 지정하는 경우 역방향 조회 전달 규칙을 적용할 단일 또는 복수 IP 주소에 대해 PTR 레코드를 입력합니다.

   예를 들어 10.0.0.0/23 범위의 주소에 대한 조회를 전달해야 하는 경우 다음 두 가지 규칙을 입력합니다.

   - 0.0.10.in-addr.arpa
   - 1.0.10.in-addr.arpa

   이러한 서브넷의 모든 IP 주소는 해당 PTR 레코드의 하위 도메인으로 참조됩니다. 예를 들어, 10.0.1.161은 1.0.10.in-addra.arpa의 하위 도메인인 161.1.0.10.in-addr.arpa의 역방향 조회 주소를 가집니다.
3. 이러한 조회를 전달할 서버를 지정합니다.
4. 아웃바운드 해석기 엔드포인트에 이러한 규칙을 추가합니다.

참고: VPC에 대해 `enableDNSHostNames`를 켜면 PTR 레코드가 자동으로 추가됩니다. Amazon Route 53 Resolver란 무엇인가요? 섹션을 참조하세요. 이전 절차는 지정된 IP 범위에 대해 해석기를 명시적으로 지정하려는 경우에만 필요합니다(예: Active Directory 서버에 쿼리를 전달하는 경우).

VPC와 전달 규칙 연결

전달 규칙을 생성한 후 하나 이상의 VPC에 규칙을 연결해야 합니다. 규칙은 VPC와 연결된 후에만 작동합니다. 규칙을 VPC와 연결할 때 Resolver가 규칙에 지정된 도메인 이름의 DNS 쿼리를 규칙에 지정된 DNS 해석기로 전달하기 시작합니다. 쿼리는 규칙을 만들 때 지정한 아웃바운드 엔드포인트를 통과합니다.

전달 규칙을 하나 이상의 VPC에 연결하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.

2. 탐색 창에서 규칙(Rules)을 선택합니다.
3. 탐색 모음에서 규칙을 생성한 리전을 선택합니다.
4. 하나 이상의 VPC에 연결할 규칙의 이름을 선택합니다.
5. VPC 연결을 선택합니다.
6. VPCs that use this rule(이 규칙을 사용하는 VPC)에서 규칙을 연결할 VPC를 선택합니다.
7. 추가를 선택합니다.

VPC에서 전달 규칙 연결 해제

다음과 같은 경우 VPC에서 전달 규칙의 연결을 해제합니다.

- 이 VPC에서 시작된 DNS 쿼리의 경우 Resolver가 규칙에 지정된 도메인 이름의 쿼리를 네트워크로 전달하는 작업을 중지하게 하려고 합니다.
- 전달 규칙을 삭제합니다. 규칙이 현재 하나 이상의 VPC에 연결된 경우 규칙을 삭제하기 전에 모든 VPC에서 규칙의 연결을 해제해야 합니다.

하나 이상의 VPC에서 전달 규칙의 연결을 해제하려면 다음 절차를 수행하세요.

VPC에서 전달 규칙의 연결을 해제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 규칙(Rules)을 선택합니다.
3. 탐색 모음에서 규칙을 생성한 리전을 선택합니다.
4. 하나 이상의 VPC에서 연결을 해제할 규칙의 이름을 선택합니다.
5. 규칙의 연결을 해제할 VPC의 옵션을 선택합니다.
6. 연결 해제를 선택합니다.
7. disassociate를 입력하여 확인합니다.
8. 제출을 선택합니다.

Resolver 규칙을 다른 AWS 계정과 공유 및 공유 규칙 사용

한 AWS 계정을 사용하여 생성한 Resolver 규칙을 다른 계정과 공유할 수 AWS 있습니다. 규칙을 공유하기 위해 Route 53 Resolver 콘솔은 AWS Resource Access Manager와 통합됩니다. Resource Access Manager에 대한 자세한 내용은 Resource Access Manager 사용 설명서 섹션을 참조하세요.

다음을 참조하세요.

공유된 규칙을 VPC에 연결

다른 AWS 계정이 하나 이상의 규칙을 계정과 공유한 경우, 생성한 규칙을 VPCs와 연결하는 것과 동일한 방식으로 VPCs와 규칙을 연결할 수 있습니다. 자세한 내용은 VPC와 전달 규칙 연결 단원을 참조하십시오.

규칙 삭제 또는 공유 해제

규칙을 다른 계정과 공유한 후 규칙을 삭제하거나 공유를 중지할 경우, 그리고 규칙이 하나 이상의 VPC와 연결된 경우 Route 53 Resolver가 나머지 규칙에 따라 해당 VPC의 DNS 쿼리를 처리하기 시작합니다. VPC에서 규칙을 연결 해제하는 경우와 동작은 동일합니다.

규칙을 조직 구성 단위(OU)에 공유하고 해당 OU의 계정을 다른 OU로 이동하면 계정 내 VPC 대한 공유 규칙과의 모든 연결이 삭제됩니다. 하지만 Resolver 규칙이 대상 OU와 이미 공유된 경우 VPC 연결은 그대로 유지되며 분리되지 않습니다.

최대 규칙 및 연결 수

계정이 규칙을 생성하고 하나 이상의 다른 계정과 공유하면 AWS 리전당 최대 규칙 수가 규칙을 생성한 계정에 적용됩니다.

규칙을 공유받은 계정에서 그 규칙을 하나 이상의 VPC와 연결할 때는 규칙과 VPC 사이의 리전당 최대 연결 수가 그 규칙을 공유한 계정에 적용됩니다.

현재 Resolver 할당량은 Route 53 Resolver의 할당량 섹션을 참조하세요.

권한

규칙을 다른 AWS 계정과 공유하려면 PutResolverRulePolicy 작업을 사용할 권한이 있어야 합니다.

규칙이 공유되는 AWS 계정에 대한 제한 사항

규칙이 공유되는 계정은 규칙을 변경하거나 삭제할 수 없습니다.

태그 지정

규칙을 생성한 계정만 규칙의 태그를 추가하거나 삭제하거나 볼 수 있습니다.

규칙의 현재 공유 상태를 보고(계정을 공유한 계정 또는 규칙이 공유되는 계정 포함) 규칙을 다른 계정과 공유하려면 다음 절차를 수행하세요.

공유 상태를 보고 다른 AWS 계정과 규칙을 공유하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 규칙(Rules)을 선택합니다.
3. 탐색 모음에서 규칙을 생성한 리전을 선택합니다.

   현재 계정이 생성하거나 현재 계정과 공유되는 규칙의 현재 공유 상태가 공유 상태 열에 표시됩니다.

   - 공유되지 않음: 현재 AWS 계정이 규칙을 생성했으며 규칙은 다른 계정과 공유되지 않습니다.
   - 나와 공유됨: 현재 계정이 규칙을 생성하고 하나 이상의 계정과 공유했습니다.
   - 나와 공유 상태: 다른 계정이 규칙을 생성하고 현재 계정과 공유했습니다.
4. 공유 정보를 표시하거나 다른 계정과 공유할 규칙의 이름을 선택합니다.

   규칙: **## ##** 페이지에서 소유자 아래의 값은 규칙을 생성한 계정의 ID를 나타냅니다. Sharing status(공유 상태)의 값이 나와 공유 상태가 아닐 경우 현재 계정입니다. 이 경우 소유자는 규칙을 생성하고 현재 계정과 공유한 계정입니다.
5. 공유를 선택하여 추가 정보를 보거나 규칙을 다른 계정과 공유합니다. 공유 상태 값에 따라 Resource Access Manager 콘솔의 페이지가 표시됩니다.

   - 공유하지 않음: 리소스 공유 생성 페이지가 표시됩니다. 다른 계정, OU 또는 조직과 규칙을 공유하는 방법은 보려면 6단계로 건너뜁니다.
   - 나와 공유됨: 공유 리소스 페이지에 현재 계정이 소유하고 다른 계정과 공유한 규칙 및 다른 리소스가 표시됩니다.
   - 나와 공유 상태: 공유 리소스 페이지에 ㄷ른 계정이 소유하고 현재 계정과 공유한 규칙 및 다른 리소스가 표시됩니다.
6. 규칙을 다른 AWS 계정, OU 또는 조직과 공유하려면 다음 값을 지정합니다.

> **Note**
>
> 공유 설정을 업데이트할 수 없습니다. 다음 설정 중 하나로도 변경하려면 규칙을 새로운 설정과 다시 공유한 후 이전 공유 설정을 제거해야 합니다.

설명

규칙을 공유한 이유를 기억나게 해주는 간단한 설명을 입력합니다.

리소스

공유할 규칙의 확인란을 선택합니다.

보안 주체

AWS 계정 번호, OU 이름 또는 조직 이름을 입력합니다.

Tags

한 개 이상의 키와 해당 값을 지정합니다. 예를 들어 키에 Cost center를 지정하고 값에 456을 지정할 수 있습니다.

이는에서 AWS 청구서를 구성하기 위해 AWS Billing and Cost Management 제공하는 태그입니다. 다른 용도로도 태그를 사용할 수 있습니다. 비용 할당 태그 사용에 대한 자세한 내용은 AWS Billing 사용 설명서의 비용 할당 태그 사용을 참조하세요.

전달 규칙 삭제

전달 규칙을 삭제하려면 다음 절차를 수행하세요.

다음을 참조하세요.

- 전달 규칙이 VPC와 연결되어 있으면 규칙을 삭제하기 전에 VPC에서 규칙의 연결을 해제해야 합니다. 자세한 내용은 VPC에서 전달 규칙 연결 해제 섹션을 참조하세요.
- 유형(Type) 값이 재귀(Recursive)인 기본 인터넷 해석기(Internet Resolver) 규칙은 삭제할 수 없습니다. 이 규칙을 사용하면, 사용자가 지정 규칙을 만들지 않았고 Resolver가 자동 정의 규칙을 만들지 않은 모든 도메인 이름에 대해 Route 53 Resolver가 재귀 해석기 역할을 합니다. 규칙 분류 방법에 대한 자세한 내용은 규칙을 사용하여 네트워크에 전달할 쿼리 제어 섹션을 참조하세요.

전달 규칙을 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 규칙(Rules)을 선택합니다.

3. 탐색 모음에서 규칙을 생성한 리전을 선택합니다.
4. 삭제할 규칙의 옵션을 선택합니다.
5. Delete(삭제)를 선택합니다.
6. 규칙을 삭제하도록 확인하려면 규칙 이름을 입력하고 제출을 선택합니다.

해석기의 역방향 DNS 쿼리에 대한 전달 규칙

Amazon VPC에서 Virtual Private Cloud(VPC)에 대한 `enableDnsHostnames`와 `enableDnsSupport`가 `true`로 설정되면 해석기는 역방향 DNS 쿼리에 대해 자동 정의된 시스템 규칙을 자동으로 생성합니다. 이러한 설정에 대한 자세한 내용은 Amazon VPC 개발자 가이드의 VPC의 DNS 속성을 참조하십시오.

역방향 DNS 쿼리에 대한 전달 규칙은 SSH 또는 Active Directory와 같은 서비스에 특히 유용합니다. 이러한 서비스에는 고객이 리소스에 연결을 시도하는 IP 주소에 대한 역방향 DNS 조회를 수행하여 사용자를 인증하는 옵션이 있습니다. 자동 정의된 시스템 규칙에 대한 자세한 내용은 Resolver가 자동 정의 시스템 규칙을 생성하는 도메인 이름 단원을 참조하십시오.

이러한 규칙을 끄고 모든 역방향 DNS 쿼리를 수정하여 확인을 위해 온프레미스 네임 서버로 전달되도록 할 수 있습니다.

자동 규칙을 끄고 나서 필요에 따라 온프레미스 리소스로 쿼리를 전달하는 규칙을 생성합니다. 전달 규칙을 관리하는 방법에 대한 자세한 내용은 전달 규칙 관리 단원을 참조하세요.

자동 정의 규칙을 끄려면 다음을 수행합니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창의 해석기(Resolver) 아래에서 VPC를 선택한 다음 VPC ID를 선택합니다.
3. 역방향 DNS 확인을 위한 자동 정의 규칙(Autodefined rules for reverse DNS resolution)에서 확인란을 선택 취소합니다. 확인란이 이미 선택 취소되어 있는 경우 확인란을 선택하여 자동 정의된 역방향 DNS 확인을 켤 수 있습니다.

관련 API는 해석기 구성 API를 참조하십시오.

Amazon Route 53에서 DNSSEC 검증 활성화

Amazon Route 53에서 Virtual Private Cloud(VPC)에 대해 DNSSEC 검증을 활성화하면 응답이 변조되지 않았는지 확인하기 위해 DNSSEC 서명을 암호화 방식으로 확인합니다. VPC 세부 정보 페이지에서 DNSSEC 검증을 사용합니다.

Route 53 Resolver는 재귀 DNS 확인을 수행할 때 퍼블릭 서명 이름에 DNSSEC 검증을 적용합니다.

하지만 Route 53 Resolver가 다른 DNS 해석기로 전달하는 경우 해당 해석기는 재귀적 DNS 확인을 수행하므로 DNSSEC 검증도 적용해야 합니다.

Important

DNSSEC 검증을 활성화하면 VPC에서 AWS 리소스의 퍼블릭 DNS 레코드에 대한 DNS 해석에 영향을 줄 수 있어 중단이 발생할 수 있습니다. DNSSEC 검증을 활성화 또는 비활성화하는 데 몇 분 정도 걸릴 수 있습니다.

Note

이때 VPC(AmazonProvidedDNS) Amazon Route 53 Resolver 의는 DNS 쿼리의 DO(DNSSEC OK) EDNS 헤더 비트와 CD(Checking Disabled) 비트를 무시합니다. DNSSEC을 구성한 경우 이는 Route 53 Resolver가 DNSSEC 유효성 검사를 수행하는 동안 DNSSEC 레코드를 반환하거나 응답에 AD 비트를 설정하지 않는다는 것을 의미합니다. 따라서 자체 DNSSEC 유효성 검사를 수행하는 것은 현재 Route 53 Resolver에서 지원되지 않습니다. 이 작업을 수행해야 하는 경우 자체 재귀 DNS 확인을 수행해야 합니다.

VPC 대해 DNSSEC 검증을 활성화하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창의 Resolver에서 VPC를 선택합니다.
3. DNSSEC 검증에서 확인란을 선택합니다. 확인란이 이미 선택되어 있는 경우 선택을 취소하여 DNSSEC 검증을 비활성화할 수 있습니다.

   DNSSEC 검증을 활성화 또는 비활성화하는 데 몇 분 정도 걸릴 수 있습니다.

AWS 리소스로 인터넷 트래픽 라우팅

Amazon Route 53를 사용하여 트래픽을 다양한 AWS 리소스로 라우팅할 수 있습니다.

- 도메인 이름을 사용하여 Amazon API Gateway API로 트래픽 라우팅
- 도메인 이름을 사용하여 Amazon CloudFront 배포로 트래픽 라우팅
- Amazon EC2 인스턴스로 트래픽 라우팅
- AWS App Runner 서비스로 트래픽 라우팅
- AWS Elastic Beanstalk 환경으로 트래픽 라우팅
- ELB 로드 밸런서로 트래픽 라우팅
- Amazon S3 버킷에서 호스팅하는 웹 사이트로 트래픽 라우팅
- 도메인 이름을 사용하여 Amazon Virtual Private Cloud 인터페이스 엔드포인트로 트래픽 라우팅
- Amazon WorkMail로 트래픽 라우팅
- Amazon OpenSearch Service 도메인 엔드포인트로 트래픽 라우팅
- 트래픽을 다른 AWS 리소스로 라우팅
- 를 사용하여 Amazon Route 53 및 Amazon Route 53 Resolver 리소스 생성 AWS CloudFormation

도메인 이름을 사용하여 Amazon API Gateway API로 트래픽 라우팅

Amazon API Gateway를 사용해 API를 생성, 게시, 유지 관리, 모니터링, 보호할 수 있습니다. AWS 클라우드에 저장된 데이터 외에도 AWS 서비스 또는 기타 웹 서비스에 액세스하는 APIs를 생성할 수 있습니다.

API Gateway API로 도메인 트래픽을 라우팅하는 데 사용하는 방법은 리전 API Gateway 엔드포인트를 생성했든 아니면 엣지 최적화 API Gateway 엔드포인트를 생성했든 관계없이동일합니다. 프라이빗 API Gateway 엔드포인트를 생성하는 경우 프로세스가 약간 다릅니다.

- 리전 API 엔드포인트(Regional API endpoint): 리전 API 엔드포인트로 트래픽을 라우팅하는 Route 53 별칭 레코드를 생성합니다.
- 엣지 최적화 API 엔드포인트(Edge-optimized API endpoint): 트래픽을 엣지 최적화 API로 라우팅하는 Route 53 별칭 레코드를 생성합니다. 그러면 트래픽이 엣지 최적화 API와 연결된 CloudFront 배포로 라우팅됩니다.

- 프라이빗 API 엔드포인트: 프라이빗 호스팅 영역의 API Gateway용 인터페이스 VPC 엔드포인트를 사용하여 트래픽을 프라이빗 API 엔드포인트로 라우팅하는 Route 53 별칭 레코드를 생성합니다.

별칭 레코드는 CNAME 레코드와 유사한 DNS에 대한 Route 53 확장입니다. 별칭 레코드와 CNAME 레코드의 비교는 별칭 또는 비 별칭 레코드 선택 단원을 참조하십시오.

> **Note**
>
> Route 53는 API Gateway APIs 또는 기타 AWS 리소스에 대한 별칭 쿼리에 대해 요금을 부과하지 않습니다.

주제

사전 조건

시작하기 전에 다음을 준비해야 합니다.

- api.example.com과 같이 생성하려는 Route 53 레코드의 이름과 일치하는 사용자 지정 도메인 이름이 있는 API Gateway API입니다.

  자세한 정보는 다음의 주제를 참조하세요.

  - Amazon API Gateway 개발자 가이드의 HTTP API에 대한 사용자 지정 도메인 이름 설정
  - Amazon API Gateway 개발자 가이드의 REST API에 대한 사용자 지정 도메인 이름 설정
  - Amazon API Gateway 개발자 가이드의 WebSocket API에 대한 사용자 지정 도메인 이름 설정
  - Amazon API Gateway APIs에서 프라이빗 API의 사용자 지정 도메인 이름입니다.
- 등록된 도메인 이름. Amazon Route 53를 도메인 등록 기관으로 사용하거나 다른 등록 기관을 사용할 수 있습니다.
- 도메인의 DNS 서비스가 될 Route 53입니다. Route 53를 사용하여 도메인 이름을 등록하면 Route 53가 해당 도메인의 DNS 서비스로 자동 구성됩니다.

  Route 53를 도메인의 DNS 서비스 공급자로 사용하는 방법에 대한 자세한 내용은 Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정 섹션을 참조하세요.

트래픽을 API Gateway 엔드포인트로 라우팅하도록 Route 53 구성

API Gateway 엔드포인트로 트래픽을 라우팅하도록 Route 53를 구성하려면 다음 절차를 수행합니다.

Custom domain names for public APIs

다음 절차에서는 퍼블릭 API의 사용자 지정 도메인 이름에 대한 APIs Gateway 엔드포인트로 트래픽을 라우팅하는 방법을 설명합니다.

API Gateway 엔드포인트로 트래픽을 라우팅하려면

1. 동일한 계정을 사용하여 Route 53 호스팅 영역과 엔드포인트를 생성한 경우, 2단계로 건너뜁니다.

   서로 다른 계정을 사용하여 호스팅 영역과 엔드포인트를 생성한 경우, 사용하려는 사용자 지정 도메인 이름의 대상 도메인 이름을 가져옵니다.

   a. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/apigateway/ API Gateway 콘솔을 엽니다.
   b. 탐색 창에서 사용자 지정 도메인 이름을 선택합니다.
   c. 사용하려는 사용자 지정 도메인 이름을 선택하고 API Gateway 도메인 이름의 값을 가져옵니다.
2. https://console.aws.amazon.com/route53/에서 Route 53 콘솔을 엽니다.
3. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
4. 트래픽을 API로 라우팅하는 데 사용할 도메인 이름이 있는 호스팅 영역 이름을 선택합니다.
5. 레코드 세트 생성을 선택합니다.
6. 다음 값을 지정하세요.

> **Important**
>
> 별칭을 활성화하는 것이 좋습니다. Route 53 별칭 레코드를 사용하지 않는 도메인 이름의 경우 프라이빗 DNS가 활성화된 VPC를 사용하여 프라이빗 API를 간접 호출하면 문제가 발생할 수 있습니다. 프라이빗 DNS는 VPC 내의 기본 DNS 확인 동작을 재정의하므로 외부 DNS 레코드와 충돌할 수 있습니다.

라우팅 정책

해당 라우팅 정책을 선택합니다. 자세한 내용은 라우팅 정책 선택 단원을 참조하십시오.

레코드 이름

트래픽을 API로 라우팅하는 데 사용할 도메인 이름을 입력합니다.

트래픽을 라우팅하려는 API에는 api.example.com과 같이 Route 53 레코드의 이름과 일치하는 사용자 지정 도메인 이름이 포함되어야 합니다.

별칭

빠른 생성(Quick create)레코드 생성 방법을 사용하는 경우, 별칭(Alias)을 켭니다.

값/트래픽 라우팅 대상

API Gateway API에 대한 별칭(Alias to API Gateway API)을 선택한 다음 엔드포인트의 출처인 리전을 선택합니다.

엔드포인트 값을 지정하는 방법은 동일한 AWS 계정을 사용하여 호스팅 영역과 API를 생성했는지 아니면 다른 계정을 사용하여 생성했는지에 따라 달라집니다.

- 동일한 계정(Same account) - 대상 도메인 이름의 목록에는 레코드 이름(Record name)에 대해 지정한 값과 일치하는 사용자 지정 도메인 이름이 있는 API만 포함됩니다. 해당되는 값을 선택합니다.
- 서로 다른 계정(Different accounts) - 이 절차의 1단계에서 가져온 값을 입력합니다.

레코드 유형

A - IPv4 주소(A – IPv4 address)를 선택합니다.

대상 상태 평가

DNS 장애 조치를 관리하려면 사용자 지정 상태 확인을 구성하십시오. 예제는 API Gateway 사용 설명서의 DNS 장애 조치를 위한 사용자 지정 상태 점검 구성을 참조하십시오.

7. 레코드 생성을 선택합니다.

변경 사항은 일반적으로 60초 이내에 모든 Route 53 서버로 전파됩니다. 전파가 완료되면 이 절차에서 생성한 별칭 레코드의 이름을 사용하여 트래픽을 API로 라우팅할 수 있습니다.

Custom domain names for private APIs

다음 절차에서는 프라이빗 API의 사용자 지정 도메인 이름에 대해 APIs Gateway 엔드포인트로 트래픽을 라우팅하는 방법을 설명합니다.

API Gateway 엔드포인트로 트래픽을 라우팅하려면

1. https://console.aws.amazon.com/route53/에서 Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
3. 트래픽을 API로 라우팅하는 데 사용할 도메인 이름이 있는 프라이빗 호스팅 영역의 이름을 선택합니다.
4. 레코드 세트 생성을 선택합니다.
5. 다음 값을 지정하세요.

   라우팅 정책

   해당 라우팅 정책을 선택합니다. 자세한 내용은 라우팅 정책 선택 단원을 참조하십시오.

   레코드 이름

   트래픽을 API로 라우팅하는 데 사용할 도메인 이름을 입력합니다.

   트래픽을 라우팅하려는 API에는 api.example.com과 같이 Route 53 레코드의 이름과 일치하는 사용자 지정 도메인 이름이 포함되어야 합니다.

   별칭

   별칭을 켭니다.

   값/트래픽 라우팅 대상

   VPC 엔드포인트에 대한 별칭을 선택합니다. 엔드포인트가 속한 리전을 선택한 다음 VPC 엔드포인트를 선택합니다.

   레코드 유형

   VPC 엔드포인트에 IPv6를 사용하는 경우 AAAA 레코드 유형을 생성합니다. VPC 엔드포인트에 듀얼 스택을 사용하는 경우 AAAA 및 A 레코드 유형을 모두 생성합니다.

   대상 상태 평가

   DNS 장애 조치를 관리하려면 사용자 지정 상태 확인을 구성하십시오. 예제는 API Gateway 사용 설명서의 DNS 장애 조치를 위한 사용자 지정 상태 점검 구성을 참조하십시오.

6. 레코드 생성을 선택합니다.

   변경 사항은 일반적으로 60초 이내에 모든 Route 53 서버로 전파됩니다. 전파가 완료되면 이 절차에서 생성한 별칭 레코드의 이름을 사용하여 트래픽을 API로 라우팅할 수 있습니다.

도메인 이름을 사용하여 Amazon CloudFront 배포로 트래픽 라우팅

AWS 콘텐츠 전송 네트워크(CDN)인 Amazon CloudFront를 웹 콘텐츠 전송 속도를 높이는 한 가지 방법으로 사용할 수 있습니다. CloudFront에서는 엣지 로케이션의 글로벌 네트워크를 통해 동적, 정적, 스트리밍 및 대화형 콘텐츠를 포함하는 전체 웹 사이트를 전송할 수 있습니다. 귀사의 콘텐츠를 요청하는 사용자는 지연 시간이 가장 낮은 엣지 로케이션으로 자동으로 라우팅됩니다.

> **Note**
>
> 퍼블릭 호스팅 영역에 대해서만 트래픽을 CloudFront 배포로 라우팅할 수 있습니다.

CloudFront를 사용하여 웹 사이트 콘텐츠를 배포하려면 배포를 생성하고 이에 대한 설정을 지정합니다. 예를 들어 선택한 사용자에게만 콘텐츠에 대한 액세스 권한을 부여할 것인지 여부와 사용자에게 HTTPS를 사용하게 하려는지 여부에 따라 CloudFront에서 콘텐츠를 가져올 HTTP 서버 또는 Amazon S3 버킷과 같은 설정을 지정합니다.

배포를 만들 때 배포에 도메인 이름을 할당합니다(예: d111111abcdef8.cloudfront.net). 예를 들어, 다음과 같이 콘텐츠에 대한 URL에 이 도메인 이름을 사용할 수 있습니다.

```
http://d111111abcdef8.cloudfront.net/logo.jpg
```

또는 다음과 같이 URL에 고유한 도메인 이름을 사용할 수 있습니다.

```
http://example.com/logo.jpg
```

Amazon CloudFront 개발자 안내서의 단계에 따라 CloudFront에서 배포에 할당한 도메인 이름 대신 CloudFront 배포의 파일 URL에 있는 고유한 도메인 이름을 사용합니다. CloudFront 배포에서 고유한 도메인 이름 사용에 대한 자세한 내용은 대체 도메인 이름(CNAME)을 추가하여 파일에 대해 사용자 지정 URL 사용을 참조하세요.

Route 53 도메인 이름을 CloudFront 배포에 사용하는 경우 Amazon Route 53를 사용하여 CloudFront 배포를 가리키는 별칭 레코드를 생성합니다. 별칭 레코드는 DNS에 대한 Route 53 확장입니다. 이는

루트 도메인(예: example.com)과 하위 도메인(예: www.example.com)에 대해 모두 별칭 레코드를 만들 수 있다는 점을 제외하고, CNAME 레코드와 유사합니다. (CNAME 레코드는 하위 도메인에 대해서만 생성할 수 있습니다.) Route 53가 별칭 레코드의 이름과 유형이 일치하는 DNS 쿼리를 수신하면, Route 53가 배포와 연결되어 있는 도메인 이름으로 응답합니다.

> **Note**
>
> Route 53는 CloudFront 배포 또는 기타 AWS 리소스에 대한 별칭 쿼리에 대해 요금을 부과하지 않습니다.

사전 조건

시작하기 전에 다음을 준비해야 합니다.

1. 등록된 도메인 이름. Amazon Route 53를 도메인 등록 기관으로 사용하거나 다른 등록 기관을 사용할 수 있습니다.
2. 도메인의 DNS 서비스가 될 Route 53입니다. Route 53를 사용하여 도메인 이름을 등록하면 Route 53가 해당 도메인의 DNS 서비스로 자동 구성됩니다.

   Route 53를 도메인의 DNS 서비스 공급자로 사용하는 방법에 대한 자세한 내용은 Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정 섹션을 참조하세요.
3. Amazon CloudFront 배포에 HTTPS가 필요하도록 공인 인증서를 요청합니다. 자세한 내용을 알아보려면 AWS Certificate Manager 사용 설명서에서 2단계: 공인 인증서 요청 및 AWS Certificate Manager에서의 DNS 검증 단원을 참조하세요.
4. CloudFront 배포 CloudFront에서 배포에 할당한 도메인 이름 대신 URL에 사용할 도메인 이름과 일치하는 대체 도메인 이름을 배포에 포함해야 합니다.

   예를 들어, 콘텐츠의 URL에 [example.com] 도메인 이름을 포함하려는 경우 배포에 대한 [Alternate Domain Name] 필드에 [example.com]을 포함해야 합니다.

   자세한 내용은 Amazon CloudFront 개발자 안내서의 다음 설명서를 참조하세요.

   - 배포 생성을 위한 태스크 목록
   - CloudFront 콘솔을 사용하여 배포 생성 또는 업데이트

Amazon Route 53를 구성하여 CloudFront 배포로 트래픽을 라우팅합니다.

CloudFront 배포로 트래픽을 라우팅하도록 Amazon Route 53를 구성하려면 다음 절차를 수행합니다. CloudFront 배포에서 고유한 도메인 이름 사용에 대한 자세한 내용은 Amazon CloudFront 개발자 안내서의 대체 도메인 이름(CNAME)을 추가하여 파일에 대해 사용자 지정 URL 사용을 참조합니다.

> **Note**
>
> 변경 사항은 일반적으로 60초 이내에 모든 Route 53 서버로 전파됩니다. 변경 사항을 전파하는 경우 이 절차에서 생성한 별칭 레코드의 이름을 사용하여 트래픽을 CloudFront 배포로 라우팅할 수 있습니다.

트래픽을 CloudFront 웹 배포로 라우팅하려면

1. CloudFront에서 배포에 할당한 도메인 이름을 가져오고 IPv6가 활성화되어 있는지 확인합니다.

   a. 에 로그인 AWS Management Console 하고에서 CloudFront 콘솔을 엽니다https://console.aws.amazon.com/cloudfront/v4/home.

   b. ID열에서 트래픽을 라우팅할 배포의 연결된 이름을 선택합니다(확인란이 아님).

   c. 일반(General) 탭에서 배포 도메인 이름(Distribution domain Name) 필드의 값을 가져옵니다.

   d. 일반(General) 탭의 설정(Settings) 섹션에서 편집을 선택하고 스크롤하여 IPv6 필드를 확인하여 배포에 IPv6가 활성화되어 있는지 확인합니다. IPv6가 활성화되어 있으면 배포를 위해 2개의 별칭 레코드를 만들어야 합니다. 하나는 IPv4 트래픽을 배포로 라우팅하고, 하나는 IPv6 트래픽을 라우팅하기 위한 것입니다. 취소를 선택합니다.

      자세한 내용은 Amazon CloudFront 개발자 안내서에서 배포의 생성 또는 업데이트 시 지정하는 값 주제의 IPv6 활성화를 참조하세요.

2. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
3. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
4. 트래픽을 CloudFront 배포로 라우팅하는 데 사용할 도메인의 호스팅 영역의 연결된 이름을 선택합니다.
5. 레코드 세트 생성을 선택합니다.

   마법사를 사용하여 레코드를 생성하거나 빠른 생성으로 전환(Switch to quick create)을 선택합니다.

6. 다음 값을 지정하세요.

   라우팅 정책

   해당 라우팅 정책을 선택합니다. 자세한 내용은 라우팅 정책 선택 단원을 참조하십시오.

   레코드 이름

   트래픽을 CloudFront 배포로 라우팅하는 데 사용할 도메인 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

   예를 들어, 호스팅 영역의 이름이 example.com이고 acme.example.com을 사용하여 트래픽을 배포로 라우팅하려면 acme를 입력합니다.

   별칭

   빠른 생성(Quick create) 레코드 생성 방법을 사용하는 경우, 별칭(Alias)을 켭니다.

   > **Important**
   >
   > CloudFront 배포가 작동하려면 별칭 레코드를 생성해야 합니다.

   값/트래픽 라우팅 대상

   CloudFront 배포에 대한 별칭(Alias to CloudFront distributions)을 선택합니다. us-east-1 리전이 기본으로 선택됩니다. 배포를 생성할 때 CloudFront가 배포에 할당한 도메인 이름을 선택합니다. 이 이름은 1단계에서 생성한 값입니다.

   레코드 유형

   A - IPv4 주소(A – IPv4 address)를 선택합니다.

   배포에 대해 IPv6가 활성화되어 있고 두 번째 레코드를 생성하는 경우, AAAA - IPv6 address를 선택합니다.

   대상 상태 평가

   기본값인 [No]를 수락합니다.

7. 레코드 생성을 선택합니다.
8. 배포에 대해 IPv6가 활성화되어 있다면 5~7단계를 반복합니다. 6단계에서 설명된 것처럼 레코드 유형 필드를 제외하고 동일한 설정을 지정합니다.

Amazon EC2 인스턴스로 트래픽 라우팅

Amazon EC2는 AWS 클라우드에서 확장 가능한 컴퓨팅 용량을 제공합니다. 사전 구성된 템플릿(Amazon Machine Image(AMI))를 사용하여 EC2 가상 컴퓨팅 환경(인스턴스)을 시작할 수 있습니다. EC2 인스턴스를 시작하면 EC2가 운영 체제(Linux 또는 Microsoft Windows) 및 AMI에 포함된 추가 소프트웨어(예: 웹 서버 또는 데이터베이스 소프트웨어)를 자동으로 설치합니다.

웹 사이트를 호스팅하거나 EC2 인스턴스에서 웹 애플리케이션을 실행하는 경우 Amazon Route 53를 사용하여 example.com 등 도메인에 대한 트래픽을 서버로 라우팅할 수 있습니다.

사전 조건

시작하기 전에 다음을 준비해야 합니다.

- Amazon EC2 인스턴스 EC2 인스턴스 시작에 대한 자세한 내용은 다음 문서를 참조하십시오.
  - Linux - Amazon EC2 사용 설명서의 Amazon EC2 Linux 인스턴스 시작하기 참조
  - Microsoft Windows - Amazon EC2 사용 설명서의 Amazon EC2 Windows 인스턴스 시작하기 참조

  > **Important**
  >
  > 탄력적 IP 주소를 생성하고 이를 EC2 인스턴스에 연결하는 것이 좋습니다. 탄력적 IP 주소를 생성하면 Amazon EC2 인스턴스의 IP 주소가 절대로 달라지지 않습니다. 요금 관련 자세한 내용은 탄력적 IP 주소에 대한 요금 섹션을 참조하세요.

- 등록된 도메인 이름. Amazon Route 53를 도메인 등록 기관으로 사용하거나 다른 등록 기관을 사용할 수 있습니다.
- 도메인의 DNS 서비스가 될 Route 53입니다. Route 53를 사용하여 도메인 이름을 등록하면 Route 53가 해당 도메인의 DNS 서비스로 자동 구성됩니다.

  Route 53를 도메인의 DNS 서비스 공급자로 사용하는 방법에 대한 자세한 내용은 Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정 섹션을 참조하세요.

Amazon Route 53를 구성하여 Amazon EC2 인스턴스로 트래픽을 라우팅합니다.

EC2 인스턴스로 트래픽을 라우팅하도록 Amazon Route 53를 구성하려면 다음 절차를 수행합니다.

Amazon EC2 인스턴스로 트래픽을 라우팅하려면

1. Amazon EC2 인스턴스의 IP 주소를 가져옵니다.

   a. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/ec2/ Amazon EC2 콘솔을 엽니다.

   b. 콘솔의 오른쪽 상단에 있는 리전 목록에서 인스턴스를 시작한 리전을 선택합니다.

   c. 탐색 창에서 Instances(인스턴스)를 선택합니다.

   d. 테이블에서 트래픽을 라우팅할 인스턴스를 선택합니다.

   e. 하단 창에 있는 [Description] 탭에서 [Elastic IPs] 값을 가져옵니다.

      인스턴스와 탄력적 IP를 연결하지 않은 경우 IPv4 퍼블릭 IP 값을 가져옵니다.

2. https://console.aws.amazon.com/route53/에서 Route 53 콘솔을 엽니다.
3. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
4. 트래픽을 라우팅할 도메인의 이름과 일치하는 호스팅 영역 이름을 선택합니다.
5. 레코드 세트 생성을 선택합니다.
6. 다음 값을 지정하세요.

   라우팅 정책

      해당 라우팅 정책을 선택합니다. 자세한 내용은 라우팅 정책 선택 단원을 참조하십시오.

   레코드 이름

      트래픽을 EC2 인스턴스로 라우팅하는 데 사용할 도메인 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

      예를 들어, 호스팅 영역의 이름이 example.com이고 acme.example.com을 사용하여 트래픽을 EC2 인스턴스로 라우팅하려면 acme를 입력합니다.

   값/트래픽 라우팅 대상

      IP 주소 또는 레코드 유형에 따라 다른 값을 선택합니다. 1단계에서 얻은 IP 주소를 입력합니다.

   레코드 유형

      A - IPv4 주소(A – IPv4 address)를 선택합니다.

TTL(초)

기본값 [300]을 수락합니다.

7. 레코드 생성을 선택합니다.

변경 사항은 일반적으로 60초 이내에 모든 Route 53 서버로 전파됩니다. 전파가 완료되면 이 절차에서 생성한 레코드의 이름을 사용하여 트래픽을 EC2 인스턴스로 라우팅할 수 있게 됩니다.

> **Important**
>
> 탄력적 IP를 릴리스하는 경우 탄력적 IP를 가리키는 DNS 레코드도 삭제해야 합니다. 그렇지 않으면 DNS 레코드가 손상되어 권한 없는 사용자가 레코드를 조작하게 될 수 있습니다.

AWS App Runner 서비스로 트래픽 라우팅

AWS App Runner 는 개발자가 컨테이너화된 웹 애플리케이션 및 APIs 대규모로 쉽게 배포할 수 있는 완전 관리형 서비스입니다. 소스 코드 또는 컨테이너 이미지로 시작하세요. App Runner는 웹 애플리케이션을 자동으로 빌드 및 배포하고, 암호화를 통해 트래픽을 로드 밸런싱하고, 트래픽 요구 사항에 맞게 확장하고, 서비스가 프라이빗 Amazon VPC에서 실행되는 다른 AWS 서비스 및 애플리케이션과 쉽게 통신할 수 있도록 합니다. App Runner를 사용하면 서버나 확장을 고려하는 대신 애플리케이션에 집중할 수 있는 시간이 늘어납니다. 자세한 내용은 AWS App Runner 개발자 가이드의 AWS App Runner 이란 무엇입니까?를 참조하세요.

> **Important**
>
> Amazon Route 53는 현재 2022년 8월 1일 이후에 생성된 AWS App Runner 서비스에 대한 별칭 레코드를 지원합니다.

도메인 트래픽을 App Runner 서비스로 라우팅하려면 Amazon Route 53를 사용하여 App Runner 서비스를 가리키는 별칭 레코드(alias record)를 생성합니다. 별칭 레코드는 DNS에 대한 Route 53 확장입니다. 이는 example.com과 같은 루트 도메인과, www.example.com(http://www.example.com/)과 같은 하위 도메인에 대해 모두 별칭 레코드를 만들 수 있다는 점을 제외하면 CNAME 레코드와 유사합니다. 하위 도메인에 대한 CNAME 레코드만 생성할 수 있습니다.

> **Note**
>
> Route 53는 App Runner 서비스 또는 기타 AWS 리소스에 대한 별칭 쿼리에 대해서는 요금을 부과하지 않습니다.

사전 조건

시작하기 전에 다음을 준비해야 합니다.

- App Runner 서비스. App Runner 서비스 생성에 대한 자세한 내용은 App Runner 시작하기 단원을 참조하세요.
- 등록된 도메인 이름. Amazon Route 53를 도메인 등록 기관으로 사용하거나 다른 등록 기관을 사용할 수 있습니다.
- 도메인의 DNS 서비스가 될 Route 53입니다. Route 53를 사용하여 도메인 이름을 등록하면 Route 53가 해당 도메인의 DNS 서비스로 자동 구성됩니다.

  Route 53를 도메인의 DNS 서비스 공급자로 사용하는 방법에 대한 자세한 내용은 Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정 섹션을 참조하세요.
- App Runner 서비스에 사용자 지정 도메인을 연결해둡니다. 자세한 내용은 App Runner의 사용자 지정 도메인 이름 관리를 참조하세요.
- Route 53 호스팅 영역에 App Runner에서 반환한 인증서 검증 레코드를 구성하여 도메인 검증 프로세스를 시작합니다. 자세한 내용은 AWS Certificate Manager 사용 설명서의 AWS Certificate Manager에서의 DNS 검증 단원을 참조하세요.

Amazon Route 53를 구성하여 App Runner 서비스로 트래픽 라우팅

App Runner 서비스로 트래픽을 라우팅하도록 Amazon Route 53를 구성하려면 다음 절차를 수행합니다.

App Runner 서비스로 트래픽 라우팅

1. https://console.aws.amazon.com/route53/에서 Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
3. 트래픽을 라우팅할 도메인의 이름과 일치하는 호스팅 영역 이름을 선택합니다.
4. 레코드 세트 생성을 선택합니다.

5. 다음 값을 지정하세요.

   라우팅 정책

   해당 라우팅 정책을 선택합니다. 자세한 내용은 라우팅 정책 선택 단원을 참조하십시오.

   레코드 이름

   App Runner 서비스로 트래픽을 라우팅하는 데 사용할 도메인 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

   예를 들어, 호스팅 영역의 이름이 example.com이고 acme.example.com을 사용하여 트래픽을 App Runner 서비스로 라우팅하려면 acme를 입력합니다.

   값/트래픽 라우팅 대상

   App Runner 서비스에 대한 별칭(Alias to App Runner Service)을 선택한 다음 AWS 리전을 선택합니다. 트래픽을 라우팅할 환경의 도메인 이름을 선택합니다.

   레코드 유형

   기본값 A – IPv4 address(A – IPv4 주소)를 수락합니다.

   대상 상태 평가

   기본값인 예(Yes)를 수락합니다.

6. 레코드 생성을 선택합니다.

   변경 사항은 일반적으로 60초 이내에 모든 Route 53 서버로 전파됩니다. 전파가 완료되면 이 절차에서 생성한 별칭 레코드의 이름을 사용하여 트래픽을 App Runner 서비스로 라우팅할 수 있습니다.

AWS Elastic Beanstalk 환경으로 트래픽 라우팅

AWS Elastic Beanstalk 를 사용하여 AWS 클라우드에서 애플리케이션을 배포하고 관리하는 경우 Amazon Route 53을 사용하여 example.com 같은 도메인의 DNS 트래픽을 새 또는 기존 Elastic Beanstalk 환경으로 라우팅할 수 있습니다.

Elastic Beanstalk 환경으로 DNS 트래픽을 라우팅하는 방법은 다음 주제의 절차를 참조하세요.

> **Note**
>
> 이 절차에서는 이미 Route 53를 도메인의 DNS 서비스로 사용하고 있다고 가정합니다. 다른 DNS 서비스를 사용하는 경우, Route 53를 DNS 서비스 공급자로 사용하는 방법에 대한 자세한 내용은 Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정 섹션을 참조하세요.

주제

- Elastic Beanstalk 환경에 애플리케이션 배포
- Elastic Beanstalk 환경의 도메인 이름 가져오기
- Elastic Beanstalk 환경으로 트래픽을 라우팅하는 Amazon Route 53 레코드 생성

Elastic Beanstalk 환경에 애플리케이션 배포

트래픽을 라우팅할 Elastic Beanstalk 환경이 이미 있다면 Elastic Beanstalk 환경의 도메인 이름 가져오기 섹션으로 건너뛰세요.

애플리케이션을 생성하여 Elastic Beanstalk 환경에 배포하려면

- 애플리케이션을 생성하여 Elastic Beanstalk 환경에 배포하는 방법에 대한 자세한 내용은 AWS Elastic Beanstalk 개발자 안내서의 Elastic Beanstalk 사용 시작하기를 참조하세요.

Elastic Beanstalk 환경의 도메인 이름 가져오기

Elastic Beanstalk 환경의 도메인 이름을 이미 알고 있다면 Elastic Beanstalk 환경으로 트래픽을 라우팅하는 Amazon Route 53 레코드 생성 단원으로 건너뛰십시오.

Elastic Beanstalk 환경의 도메인 이름을 가져오려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/elasticbeanstalk/ Elastic Beanstalk 콘솔을 엽니다.
2. 애플리케이션 목록에서 트래픽을 라우팅할 애플리케이션을 찾아 URL 값을 가져옵니다. 애플리케이션 목록이 표시되지 않으면 탐색 창에서 Applications(애플리케이션)를 선택합니다.

   URL에 대한 자세한 내용은 Elastic Beanstalk 개발자 가이드의 Elastic Beanstalk 환경의 도메인 이름을 참조하세요.

Elastic Beanstalk 환경으로 트래픽을 라우팅하는 Amazon Route 53 레코드 생성

Amazon Route 53 레코드에는 Elastic Beanstalk 환경으로 트래픽을 라우팅하는 방법을 제어하는 설정이 포함되어 있습니다. 환경을 배포한 us-east-2 같은 리전이 환경의 도메인 이름에 포함되는지 여부에 따라 CNAME 레코드 또는 별칭 레코드 중 하나를 만듭니다. 새 환경에는 도메인 이름의 리전이 포함되어 있고, 2016년 초 이전에 생성한 환경에는 포함되어 있지 않습니다. CNAME 레코드와 별칭 레코드를 비교하는 내용은 별칭 또는 비 별칭 레코드 선택 단원을 참조하십시오.

도메인 이름에 리전이 포함되지 않은 경우

CNAME 레코드를 생성해야 합니다. 하지만 DNS의 제한 때문에 CNAME 레코드는 루트 도메인 이름이 아니라 하위 도메인에 대해서만 생성할 수 있습니다. 예를 들어 도메인 이름이 example.com이라면 acme.example.com에 대한 트래픽을 Elastic Beanstalk 환경으로 라우팅하는 레코드를 생성할 수 있습니다. 그러나 example.com에 대한 트래픽을 Elastic Beanstalk 환경으로 라우팅하는 레코드는 생성할 수 없습니다.

Elastic Beanstalk 환경으로 트래픽을 라우팅하는 CNAME 레코드를 생성하려면 절차를 참조하십시오.

도메인 이름에 리전이 포함된 경우

별칭 레코드를 생성할 수 있습니다. 별칭 레코드는 Route 53에만 사용할 수 있으며, CNAME 레코드에 비해 다음 두 가지 중요한 장점이 있습니다.

- 루트 도메인 이름 또는 하위 도메인에 대한 별칭 레코드를 생성할 수 있습니다. 예를 들어 도메인 이름이 example.com이라면 example.com 또는 acme.example.com에 대한 요청을 Elastic Beanstalk 환경으로 라우팅하는 레코드를 생성할 수 있습니다.
- Route 53는 별칭 레코드를 사용하여 트래픽을 라우팅하는 요청에 대해서는 요금을 부과하지 않습니다.

Elastic Beanstalk 환경으로 트래픽을 라우팅하는 Amazon Route 53 별칭 레코드를 생성하려면 절차를 참조하십시오.

Elastic Beanstalk 환경으로 트래픽을 라우팅하는 CNAME 레코드를 생성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.

3. Elastic Beanstalk 환경으로 트래픽을 라우팅하는 데 사용할 호스팅 영역의 이름을 선택합니다.
4. 레코드 세트 생성을 선택합니다.
5. 빠른 생성으로 전환 선택
6. 다음 값을 지정하세요.

   라우팅 정책

   해당 라우팅 정책을 선택합니다. 자세한 내용은 라우팅 정책 선택 단원을 참조하십시오.

   레코드 이름

   Elastic Beanstalk 환경으로 트래픽을 라우팅하는 데 사용할 도메인 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

   예를 들어, 호스팅 영역의 이름이 example.com이고 acme.example.com을 사용하여 트래픽을 사용 중인 환경으로 라우팅하려면 acme를 입력합니다.

   > **Important**
   > 호스팅 영역과 이름이 동일한 CNAME 레코드는 만들 수 없습니다.

   별칭

   빠른 생성(Quick create)레코드 생성 방법을 사용하는 경우, 별칭(Alias)을 켭니다.

   값/트래픽 라우팅 대상

   IP 주소 또는 레코드 유형에 따라 다른 값(IP address or another value depending on the record type)을 선택하고 Elastic Beanstalk 환경의 도메인 이름 가져오기 주제의 절차를 수행할 때 얻을 수 있는 값을 입력합니다. 서로 다른 계정을 사용하여 Route 53 호스팅 영역과 Elastic Beanstalk 환경을 생성한 경우 Elastic Beanstalk 환경에 대한 CNAME 속성을 입력합니다.

   레코드 유형

   CNAME을 선택합니다.

   TTL(초)

   기본값 [300]을 수락합니다.
7. 레코드 생성을 선택합니다.

변경 사항은 일반적으로 60초 이내에 모든 Route 53 서버로 전파됩니다.

Elastic Beanstalk 환경으로 트래픽을 라우팅하는 Amazon Route 53 별칭 레코드를 생성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
3. Elastic Beanstalk 환경으로 트래픽을 라우팅하는 데 사용할 호스팅 영역의 이름을 선택합니다.
4. 레코드 세트 생성을 선택합니다.
5. 다음 값을 지정하세요.

   라우팅 정책

   해당 라우팅 정책을 선택합니다. 자세한 내용은 라우팅 정책 선택 단원을 참조하십시오.

   레코드 이름

   Elastic Beanstalk 환경으로 트래픽을 라우팅하는 데 사용할 도메인 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

   예를 들어, 호스팅 영역의 이름이 example.com이고 acme.example.com을 사용하여 트래픽을 사용 중인 환경으로 라우팅하려면 acme를 입력합니다.

   값/트래픽 라우팅 대상

   Elastic Beanstalk 환경에 대한 별칭(Alias to Elastic Beanstalk environment)을 선택한 다음 엔드포인트의 출처인 리전을 선택합니다. 트래픽을 라우팅할 환경의 도메인 이름을 선택합니다. 이것은 Elastic Beanstalk 환경의 도메인 이름 가져오기 주제의 절차를 수행할 때 가져온 값입니다.

   서로 다른 계정을 사용하여 Route 53 호스팅 영역과 Elastic Beanstalk 환경을 생성한 경우 Elastic Beanstalk 환경에 대한 CNAME 속성을 입력합니다.

   레코드 유형

   기본값 A - Ipv4 주소를 수락합니다.

   대상 상태 평가

   기본값인 예(Yes)를 수락합니다.
6. 레코드 생성을 선택합니다.

변경 사항은 일반적으로 60초 이내에 모든 Route 53 서버로 전파됩니다. 전파가 완료되면 이 절차에서 생성한 별칭 레코드의 이름을 사용하여 트래픽을 Elastic Beanstalk 환경으로 라우팅할 수 있습니다.

ELB 로드 밸런서로 트래픽 라우팅

여러 Amazon EC2 인스턴스에서 하나의 웹 사이트를 호스팅하는 경우 Elastic Load Balancing(ELB) 로드 밸런서를 사용하여 웹 사이트에 대한 트래픽을 인스턴스 간에 분산할 수 있습니다. 웹 사이트에 대한 트래픽이 시간에 따라 변화하므로 ELB 서비스가 로드 밸런서를 자동으로 확장합니다. 또한 로드 밸런서를 통해 등록된 인스턴스의 상태를 모니터링하고 상태가 양호한 인스턴스로만 도메인 트래픽을 라우팅할 수 있습니다.

도메인 트래픽을 ELB 로드 밸런서로 라우팅하려면 Amazon Route 53를 사용하여 로드 밸런서를 지정하는 별칭 레코드(alias record)를 생성합니다. 별칭 레코드는 DNS에 대한 Route 53 확장입니다. 이는 루트 도메인(예: example.com)과 하위 도메인(예: www.example.com)에 대해 모두 별칭 레코드를 만들 수 있다는 점을 제외하고, CNAME 레코드와 유사합니다. (CNAME 레코드는 하위 도메인에 대해서만 생성할 수 있습니다.)

> **Note**
>
> Route 53는 ELB 로드 밸런서 또는 기타 AWS 리소스에 대한 별칭 쿼리에 대해서는 요금을 부과하지 않습니다.

사전 조건

시작하기 전에 다음을 준비해야 합니다.

- ELB 로드 밸런서. ELB Classic, 애플리케이션 또는 Network Load Balancer를 사용할 수 있습니다. 로드 밸런서를 생성하는 방법에 대한 자세한 내용은 Elastic Load Balancing 사용 설명서의 Elastic Load Balancing 시작하기를 참조하세요.

  로드 밸런서 이름은 나중에 기억하기 쉬운 것으로 지정합니다. 로드 밸런서를 생성할 때 지정한 이름이 Route 53 콘솔에서 별칭 레코드를 생성할 때 선택할 이름입니다.
- 등록된 도메인 이름. Route 53를 도메인 등록 기관으로 사용하거나 다른 등록 기관을 사용할 수 있습니다.

- 도메인의 DNS 서비스가 될 Route 53입니다. Route 53를 사용하여 도메인 이름을 등록하면 Route 53가 해당 도메인의 DNS 서비스로 자동 구성됩니다.

  Route 53를 도메인의 DNS 서비스 공급자로 사용하는 방법에 대한 자세한 내용은 Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정 섹션을 참조하세요.

ELB 로드 밸런서로 트래픽을 라우팅하도록 Amazon Route 53 구성

ELB 로드 밸런서로 트래픽을 라우팅하도록 Amazon Route 53를 구성하려면 다음 절차를 수행합니다.

ELB 로드 밸런서로 트래픽을 라우팅하려면

1. 동일한 계정을 사용하여 Route 53 호스팅 영역 및 ELB 로드 밸런서를 생성한 경우 2단계로 이동합니다.

   다른 계정을 사용하여 호스팅 영역과 ELB 로드 밸런서를 생성한 경우 Elastic Load Balancing 로드 밸런서의 DNS 이름 가져오기 절차를 수행하여 로드 밸런서에 대한 DNS 이름을 가져옵니다.
2. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
3. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
4. 트래픽을 로드 밸런서로 라우팅하는 데 사용할 도메인 이름이 있는 호스팅 영역 이름을 선택합니다.
5. 레코드 세트 생성을 선택합니다.
6. 다음 값을 지정하세요.

   라우팅 정책

   해당 라우팅 정책을 선택합니다. 자세한 내용은 라우팅 정책 선택 단원을 참조하십시오.

   레코드 이름

   트래픽을 ELB 로드 밸런서로 라우팅하는 데 사용할 도메인 또는 하위 도메인 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

   예를 들어, 호스팅 영역의 이름이 example.com이고 acme.example.com을 사용하여 트래픽을 로드 밸런서로 라우팅하려면 acme를 입력합니다.

   별칭

   빠른 생성(Quick create)레코드 생성 방법을 사용하는 경우, 별칭(Alias)을 켭니다.

값/트래픽 라우팅 대상

애플리케이션 및 Classic Load Balancer 대한 별칭(Alias to Application and Classic Load Balancer) 또는 Network Load Balancer에 대한 별칭(Alias to Network Load Balancer)을 선택한 다음 엔드포인트의 출처인 리전을 선택합니다.

동일한 AWS 계정을 사용하여 호스팅 영역과 ELB 로드 밸런서를 생성한 경우 로드 밸런서에 할당한 이름을 선택합니다.

다른 계정을 사용하여 호스팅 영역과 ELB 로드 밸런서를 생성한 경우 이 절차의 1단계에서 얻은 값을 입력합니다.

> **Note**
>
> 콘솔은 동일한 AWS 계정에서만 애플리케이션의 DNS 이름과 Classic Load Balancer에 듀얼 스택을 우선합니다. 웹 브라우저와 같은 클라이언트가 도메인 이름(example.com) 또는 하위 도메인 이름(www.example.com)에 대한 IP 주소를 요청할 때 클라이언트는 IPv4 주소(A 레코드), IPv6 주소(AAAA 레코드), 또는 IPv4 및 IPv6 주소(별도 요청의 경우 IPv4 먼저) 둘 다를 요청할 수 있습니다. dualstack.을 지정하면 Route 53에서 클라이언트가 요청한 IP 주소 형식에 따라 로드 밸런서에 적절한 IP 주소로 응답할 수 있습니다. 다른 계정의 애플리케이션 및 Classic Load Balancer의 경우 앞에 듀얼 스택.을 추가해야 합니다.

레코드 유형

A - IPv4 주소(A – IPv4 address)를 선택합니다.

대상 상태 평가

Route 53가 리소스 상태에 따라 트래픽을 라우팅하도록 하려면 예(Yes)를 선택합니다. 리소스 상태 확인에 관한 자세한 내용은 Amazon Route 53 상태 확인 생성 단원을 참조하십시오.

7. 레코드 생성을 선택합니다.

변경 사항은 일반적으로 60초 이내에 모든 Route 53 서버로 전파됩니다. 전파가 완료되면 이 절차에서 생성한 별칭 레코드의 이름을 사용하여 트래픽을 로드 밸런서로 라우팅할 수 있게 됩니다.

Amazon S3 버킷에서 호스팅하는 웹 사이트로 트래픽 라우팅

Amazon Simple Storage Service(Amazon S3)는 안전하고 내구성과 확장성이 뛰어난 클라우드 스토리지를 제공합니다. 웹 페이지 및 클라이언트 측 스크립트를 포함할 수 있는 정적 웹 사이트를 호스팅하도록 S3 버킷을 구성할 수 있습니다. S3은 서버 측 스크립팅을 지원하지 않습니다.

도메인 트래픽을 S3 버킷으로 라우팅하려면 Amazon Route 53를 사용하여 버킷을 지정하는 별칭 레코드(alias record)를 생성합니다. 별칭 레코드는 DNS에 대한 Route 53 확장입니다. 이는 루트 도메인(예: example.com)과 하위 도메인(예: www.example.com)에 대해 모두 별칭 레코드를 만들 수 있다는 점을 제외하고, CNAME 레코드와 유사합니다. CNAME 레코드는 하위 도메인에 대해서만 생성할 수 있습니다.

> **Note**
>
> Route 53는 S3 버킷 또는 기타 AWS 리소스에 대한 별칭 쿼리에 대해 요금을 부과하지 않습니다.

사전 조건

시작하기 전에 다음을 준비해야 합니다. Amazon Route 53 또는 S3를 처음 사용할 경우 Amazon Route 53 시작하기 섹션을 참조하세요. 이 섹션에서는 도메인 이름을 등록하고 S3 버킷을 만들고 구성하는 모든 절차를 안내합니다.

- 정적 웹 사이트로 호스팅하도록 구성되어 있는 S3 버킷이 필요합니다.

  자세한 내용은 Amazon Simple Storage Service 사용 설명서의 웹 사이트 호스팅에 대한 버킷 구성을 참조하십시오.

  > **Important**
  >
  > 버킷은 도메인 또는 하위 도메인과 이름이 동일해야 합니다. 예를 들어, 하위 도메인인 acme.example.com을 사용하려면 버킷 이름이 acme.example.com이어야 합니다.

  도메인 및 하위 도메인(예: example.com 및 www.example.com)의 트래픽을 단일 버킷으로 라우팅할 수 있습니다. 도메인 및 각 하위 도메인에 대해 버킷을 생성하고 하나를 제외한 모든 버킷이 트래픽을 남은 버킷으로 리디렉션하도록 구성합니다. 자세한 내용은 Amazon Route 53 시작하기 단원을 참조하십시오.

> **Note**
>
> 웹 사이트 엔드포인트로 구성한 S3 버킷은 SSL/TLS를 지원하지 않으므로 CloudFront 배포로 트래픽을 라우팅하고 S3 버킷을 그 배포의 오리진으로 사용해야 합니다.
> CloudFront 배포를 생성하는 방법에 대한 지침은 도메인 이름을 사용하여 Amazon CloudFront 배포로 트래픽 라우팅뿐만 아니라 CloudFront 사용 설명서의 CloudFront 배포 생성 및 대체 도메인 이름과 HTTPS 구성 단원을 참조하세요.

- 등록된 도메인 이름. Route 53를 도메인 등록 기관으로 사용하거나 다른 등록 기관을 사용할 수 있습니다.
- 도메인의 DNS 서비스가 될 Route 53입니다. Route 53를 사용하여 도메인 이름을 등록하면 Route 53가 해당 도메인의 DNS 서비스로 자동 구성됩니다.

  Route 53를 도메인의 DNS 서비스 공급자로 사용하는 방법에 대한 자세한 내용은 Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정 섹션을 참조하세요.

트래픽을 S3 버킷으로 라우팅하도록 Amazon Route 53 구성

정적 웹 사이트를 호스팅하도록 구성되어 있는 S3 버킷으로 트래픽을 라우팅하도록 Amazon Route 53를 구성하려면 다음 절차를 수행합니다.

S3 버킷으로 트래픽을 라우팅하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
3. 트래픽을 S3 버킷으로 라우팅하는 데 사용할 도메인 이름이 있는 호스팅 영역 이름을 선택합니다.
4. 레코드 세트 생성을 선택합니다.
5. 다음 값을 지정하세요.

   라우팅 정책

   해당 라우팅 정책을 선택합니다. 자세한 내용은 라우팅 정책 선택 단원을 참조하십시오.

   레코드 이름

   트래픽을 S3 버킷으로 라우팅하는 데 사용할 도메인 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

예를 들어, 호스팅 영역의 이름이 example.com이고 acme.example.com을 사용하여 트래픽을 버킷으로 라우팅하려면 acme를 입력합니다.

별칭

빠른 생성(Quick create)레코드 생성 방법을 사용하는 경우, 별칭(Alias)을 켭니다.

값/트래픽 라우팅 대상

S3 웹 사이트 엔드포인트에 대한 별칭(Alias to S3 website endpoint)을 선택한 다음 엔드포인트의 출처인 리전을 선택합니다.

레코드 이름(Record name)에서 지정한 이름과 동일한 버킷을 선택합니다.

목록에는 다음 요구 사항을 충족하는 버킷만을 포함합니다.

- 버킷의 이름은 생성한 레코드의 이름과 동일합니다.
- 버킷이 웹 사이트 엔드포인트로 구성된 경우.
- 버킷이 현재 AWS 계정에 의해 생성되었습니다.

  다른 AWS 계정을 사용하여 버킷을 생성한 경우 S3 버킷을 생성한 리전의 이름을 입력합니다. 리전 이름에 대한 올바른 형식은 Amazon Web Services 일반 참조의 Amazon S3 웹 사이트 엔드포인트 테이블에서 웹 사이트 엔드포인트 열을 참조하세요.

레코드 유형

A - IPv4 주소(A – IPv4 address)를 선택합니다.

대상 상태 평가

기본값인 예(Yes)를 수락합니다.

6. 레코드 생성을 선택합니다.

변경 사항은 일반적으로 60초 이내에 모든 Route 53 서버로 전파됩니다. 전파가 완료되면 이 절차에서 생성한 별칭 레코드의 이름을 사용하여 트래픽을 S3 버킷으로 라우팅할 수 있게 됩니다.

도메인 이름을 사용하여 Amazon Virtual Private Cloud 인터페이스 엔드포인트로 트래픽 라우팅

AWS PrivateLink를 사용하여 Amazon Virtual Private Cloud(Amazon VPC) 인터페이스 엔드포인트를 사용하여 선택한 서비스에 액세스할 수 있습니다. 이러한 서비스에는 일부 AWS 서비스, 다른 AWS 고

객 및 파트너가 자체 VPCs에서 호스팅하는 서비스 및 지원되는 AWS Marketplace 파트너 서비스가 포함됩니다.

도메인 트래픽을 인터페이스 엔드포인트로 라우팅하려면 Amazon Route 53를 사용하여 별칭 레코드를 만드세요. 별칭 레코드는 DNS에 대한 Route 53 확장입니다. 이는 루트 도메인(예: example.com)과 하위 도메인(예: www.example.com)에 대해 모두 별칭 레코드를 만들 수 있다는 점을 제외하고, CNAME 레코드와 유사합니다. CNAME 레코드는 하위 도메인에 대해서만 생성할 수 있습니다.

> **Note**
>
> Route 53는 인터페이스 엔드포인트 또는 기타 AWS 리소스에 대한 별칭 쿼리에 대해 요금을 부과하지 않습니다.

주제

사전 조건

시작하기 전에 다음을 준비해야 합니다.

- Amazon VPC 인터페이스 엔드포인트 자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 VPC 엔드포인트(AWS PrivateLink)를 참조하세요.
- 등록된 도메인 이름. Amazon Route 53를 도메인 등록 기관으로 사용하거나 다른 등록 기관을 사용할 수 있습니다.
- 도메인의 DNS 서비스가 될 Route 53입니다. Route 53를 사용하여 도메인 이름을 등록하면 Route 53가 해당 도메인의 DNS 서비스로 자동 구성됩니다.

  Route 53를 도메인의 DNS 서비스 공급자로 사용하는 방법에 대한 자세한 내용은 Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정 섹션을 참조하세요.

Amazon Route 53를 구성하여 Amazon VPC 인터페이스 엔드포인트로 트래픽을 라우팅합니다.

Amazon VPC 인터페이스 엔드포인트로 트래픽을 라우팅하도록 Amazon Route 53를 구성하려면 다음 절차를 수행합니다.

트래픽을 Amazon VPC 인터페이스 엔드포인트로 라우팅하려면

1. 동일한 계정을 사용하여 Route 53 호스팅 영역과 Amazon VPC 엔드포인트를 생성한 경우, 2단계로 건너뜁니다.

   호스팅 영역과 인터페이스 엔드포인트를 서로 다른 계정을 사용하여 생성한 경우, 인터페이스 엔드포인트의 서비스 이름을 가져옵니다.

   a. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/vpc/ Amazon VPC 콘솔을 엽니다.
   b. 탐색 창에서 엔드포인트를 선택합니다.
   c. 오른쪽 창에서 인터넷 트래픽을 라우팅하려는 엔드포인트를 선택합니다.
   d. 하단 창에서 DNS 이름의 값(예: vpce-0fd00dd593example-dexample.cloudtrail.us-west-2.vpce.amazonaws.com)을 얻습니다.
2. https://console.aws.amazon.com/route53/에서 Route 53 콘솔을 엽니다.
3. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
4. 트래픽을 인터페이스 엔드포인트로 라우팅하는 데 사용할 도메인 이름이 있는 호스팅 영역 이름을 선택합니다.
5. 레코드 세트 생성을 선택합니다.
6. 다음 값을 지정하세요.

   라우팅 정책

   해당 라우팅 정책을 선택합니다. 자세한 내용은 라우팅 정책 선택 단원을 참조하십시오.

   레코드 이름

   트래픽을 Amazon VPC 인터페이스 엔드포인트로 라우팅하는 데 사용할 도메인 이름을 입력합니다.

   별칭

   빠른 생성(Quick create)레코드 생성 방법을 사용하는 경우, 별칭(Alias)을 켭니다.

   값/트래픽 라우팅 대상

   VPC 엔드포인트에 대한 별칭(Alias to VPC endpoint)을 선택한 다음 엔드포인트의 출처인 리전을 선택합니다.

엔드포인트 값을 지정하는 방법은 동일한 AWS 계정을 사용하여 호스팅 영역과 인터페이스 엔드포인트를 생성했는지 아니면 다른 계정을 사용하여 생성했는지에 따라 달라집니다.

- 동일한 계정(Same account) - 목록을 선택하고 Amazon VPC 엔드포인트(Amazon VPC endpoints) 범주를 찾습니다. 그런 다음 인터넷 트래픽을 라우팅할 인터페이스 엔드포인트의 DNS 이름을 선택합니다.
- 서로 다른 계정(Different accounts) - 이 절차의 1단계에서 가져온 값을 입력합니다.

레코드 유형

A - IPv4 주소(A – IPv4 address)를 선택합니다.

대상 상태 평가

기본값인 예(Yes)를 수락합니다.

7. 레코드 생성을 선택합니다.

변경 사항은 일반적으로 60초 이내에 모든 Route 53 서버로 전파됩니다. 전파가 완료되면 이 절차에서 생성한 별칭 레코드의 이름을 사용하여 트래픽을 인터페이스 엔드포인트로 라우팅할 수 있습니다.

Amazon WorkMail로 트래픽 라우팅

Route 53를 사용하여 트래픽을 Amazon WorkMail 이메일 도메인으로 라우팅할 수 있습니다. Route 53 호스팅 영역의 이름(예: example.com)은 Amazon WorkMail 도메인의 이름과 일치해야 합니다.

> **Note**
>
> 퍼블릭 호스팅 영역에 대해서만 Amazon WorkMail 도메인으로 트래픽을 라우팅할 수 있습니다.

Amazon WorkMail로 트래픽을 라우팅하려면 다음 네 가지 절차를 수행합니다.

Amazon Route 53를 DNS 서비스로 구성하고 Amazon WorkMail 조직 및 이메일 도메인을 추가하려면

1. 이메일 주소(예: john@example.com)에 사용할 도메인 이름을 등록하지 않았다면 지금 도메인을 등록하여 해당 도메인을 사용할 수 있도록 합니다. 자세한 내용은 새 도메인 등록 단원을 참조하십시오.

Amazon Route 53가 Amazon WorkMail에 추가한 이메일 도메인의 DNS 서비스가 아닌 경우 해당 도메인의 DNS 서비스를 Route 53으로 마이그레이션합니다. 자세한 내용은 Amazon Route 53를 기존 도메인에 대한 DNS 서비스로 설정 단원을 참조하십시오.

2. Amazon WorkMail 조직 및 이메일 도메인을 추가합니다. 자세한 내용은 Amazon WorkMail 관리자 안내서의 새 사용자를 위한 시작하기 섹션을 참조하세요.

Amazon WorkMail에 대한 Route 53 TXT 레코드를 생성하려면

1. Amazon WorkMail 콘솔의 탐색 창에서 도메인(Domains)을 선택합니다.
2. Amazon WorkMail로 트래픽을 라우팅하는 데 사용할 이메일 도메인 이름(예: example.com)을 선택합니다.
3. 다른 브라우저 탭을 연 다음, Route 53 콘솔을 엽니다.
4. Route 53 콘솔에서 다음을 수행합니다.
   a. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
   b. Amazon WorkMail 이메일 도메인에 사용할 호스팅 영역의 이름을 선택합니다.
5. Amazon WorkMail 콘솔의 1단계: 도메인 소유권 확인 섹션에서 Hostname 열로 이동한 다음, 이메일 도메인 이름 앞에 있는 값 부분을 복사합니다.

   예를 들어, Amazon WorkMail 이메일 도메인이 example.com이고 Hostname의 값이 _amazonses.example.com인 경우, _amazonses를 복사합니다.
6. Route 53 콘솔에서 다음을 수행합니다.
   a. 레코드 생성(Create record)을 선택한 다음 단순 라우팅(Simple routing)을 선택합니다.
   b. 레코드 이름(Record Name)에는 5단계에서 복사한 값을 붙여 넣습니다.
   c. 레코드 유형(Record type)에 대해 TXT – Text를 선택합니다.
7. Amazon WorkMail 콘솔에서 인용 부호를 포함하여 값(Value) 열의 값을 TXT 레코드에 복사합니다.
8. Route 53 콘솔에서 다음을 수행합니다.
   a. 값/트래픽 라우팅 대상(Value/Route traffic to)에서 IP 주소 또는 레코드 유형에 따라 다른 값(IP address or another value depending on the record type)을 선택하고 7단계에서 복사한 값을 붙여 넣습니다.

      다른 설정을 변경하지 마십시오.

b. 생성(Create)을 선택합니다.

Amazon WorkMail에 대한 Route 53 MX 레코드를 생성하려면

1. Amazon WorkMail 콘솔의 Step 2: Finalize domain setup(2단계: 도메인 설정 마무리) 섹션에서 Record type(레코드 유형)이 MX인 행으로 이동한 다음 Value(값) 열의 값을 복사합니다.
2. Route 53 콘솔에서 다음을 수행합니다.

   a. 레코드 세트 생성을 선택합니다.

   b. 값/트래픽 라우팅 대상(Value/Route traffic to)에서 IP 주소 또는 레코드 유형에 따라 다른 값(IP address or another value depending on the record type)을 선택하고 1단계에서 복사한 값을 붙여 넣습니다.

   c. 레코드 유형(Record type)에서 MX - Mail Exchange를 선택합니다.

      다른 설정을 변경하지 마십시오.

   d. 레코드 생성을 선택합니다.

Amazon WorkMail에 대한 Route 53 CNAME 레코드를 생성하려면

1. Amazon WorkMail 콘솔의 2단계: 도메인 설정 마무리 섹션에서 레코드 유형)Record type)이 CNAME인 첫 번째 행으로 이동합니다. [Hostname] 열에서 이메일 도메인 이름 앞에 있는 값 부분을 복사합니다.

   예를 들어, Amazon WorkMail 이메일 도메인이 example.com이고 Hostname의 값이 autodiscover.example.com인 경우, autodiscover를 복사합니다.
2. Route 53 콘솔에서 다음을 수행합니다.

   a. 레코드 세트 생성을 선택합니다.

   b. 레코드 이름(Record Name)에는 1단계에서 복사한 값을 붙여 넣습니다.

   c. 레코드 유형(Record type)에서 CNAME - Canonical Name을 선택합니다.
3. Amazon WorkMail 콘솔에서 레코드 유형(Record type)이 CNAME인 첫 번째 행에 있는 값(Value) 열의 값을 복사합니다.
4. Route 53 콘솔에서 다음을 수행합니다.

a. 값/트래픽 라우팅 대상(Value/Route traffic to)에서 IP 주소 또는 레코드 유형에 따라 다른 값(IP address or another value depending on the record type)을 선택하고 3단계에서 복사한 값을 붙여 넣습니다.

   다른 설정을 변경하지 마십시오.

b. 레코드 생성을 선택합니다.

5. Amazon WorkMail 콘솔에 나열된 나머지 CNAME 레코드에 대해 1~4단계를 반복합니다.

Amazon OpenSearch Service 도메인 엔드포인트로 트래픽 라우팅

Amazon OpenSearch Service는에서 OpenSearch 클러스터를 쉽게 배포, 운영 및 확장할 수 있는 관리형 서비스입니다 AWS 클라우드. OpenSearch Service 도메인은 OpenSearch Service 클러스터와 동의어입니다. 도메인은 지정된 설정, 인스턴스 유형, 인스턴스 수, 스토리지 리소스를 갖고 있는 클러스터입니다. 자세한 정보는 Amazon OpenSearch Service 개발자 안내서의 Amazon OpenSearch Service란 무엇인가요?를 참조하세요.

사전 조건

시작하기 전에 다음을 준비해야 합니다.

생성하려는 Route 53 레코드의 이름과 일치하는 example.com 같은 사용자 지정 도메인 이름이 있는 OpenSearch Service 도메인입니다.

자세한 정보는 다음의 주제를 참조하세요.

- Amazon OpenSearch Service 개발자 안내서 시작하기.
- Amazon OpenSearch Service 개발자 안내서에서 사용자 지정 엔드포인트 생성.

트래픽을 Amazon OpenSearch Service 도메인 엔드포인트로 라우팅하도록 Amazon Route 53 구성

Route 53을 사용하여 트래픽을 OpenSearch Service로 라우팅하려면 먼저 OpenSearch Service에서 제공하는 도메인 엔드포인트를 가져옵니다. 이 듀얼 스택 엔드포인트는 듀얼 스택 네트워크 모드가 있는 OpenSearch Service 도메인에서 사용자 지정 엔드포인트가 활성화된 경우에만 제공됩니다. 자세한 내용은 Amazon OpenSearch Service 개발자 안내서의 사용자 지정 엔드포인트 생성을 참조하세요.

트래픽을 OpenSearch Service 엔드포인트로 라우팅하려면

1. https://aws.amazon.com으로 이동하여 Sign In to the Console(콘솔에 로그인)을 선택합니다.
2. Analytics(분석)에서 Amazon OpenSearch Service를 선택합니다.
3. 관리형 클러스터에서 도메인을 선택합니다.
4. 도메인 페이지에서 트래픽을 라우팅할 도메인의 이름을 선택합니다.
5. 도메인 세부 정보 페이지에서 도메인 엔드포인트 v2(듀얼 스택)의 값을 복사합니다.
6. https://console.aws.amazon.com/route53/에서 Route 53 콘솔을 엽니다.
7. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
8. 트래픽을 OpenSearch Service 엔드포인트로 라우팅하는 데 사용할 도메인의 호스팅 영역의 연결된 이름을 선택합니다. 도메인 이름은 OpenSearch Service에 정의된 사용자 지정 엔드포인트와 일치해야 합니다.
9. 레코드 세트 생성을 선택합니다.

   마법사를 사용하여 레코드를 생성하거나 빠른 생성으로 전환(Switch to quick create)을 선택합니다.
10. 다음 값을 지정하세요.

    라우팅 정책

    해당 라우팅 정책을 선택합니다. 자세한 내용은 라우팅 정책 선택 단원을 참조하십시오.

    레코드 이름

    트래픽을 OpenSearch Service 도메인 엔드포인트로 라우팅하는 데 사용할 도메인 이름을 입력합니다. 기본값은 호스팅 영역 이름입니다.

    예를 들어, 호스팅 영역의 이름이 example.com이고 acme.example.com을 사용하여 트래픽을 배포로 라우팅하려면 acme를 입력합니다.

    별칭

    빠른 생성(Quick create)레코드 생성 방법을 사용하는 경우, 별칭(Alias)을 켭니다.

    값/트래픽 라우팅 대상

    OpenSearch Service 도메인 엔드포인트에 대한 별칭을 선택합니다. OpenSearch Service 도메인이 생성된 리전을 선택하고 1단계에서 얻은 값을 선택합니다.

레코드 유형

A – IPv4 주소 또는 AAAA – IPv6 주소를 선택합니다.

대상 상태 평가

기본값인 예(Yes)를 수락합니다.

11. 레코드 생성을 선택합니다.

트래픽을 다른 AWS 리소스로 라우팅

다음은 Route 53를 사용하여 트래픽을 해당 서비스로 라우팅하는 방법에 대한 다른 가이드의 주제 목록입니다.

- AWS Cloud Map 사용 설명서의 AWS Cloud Map사용.
- AWS App Runner 개발자 안내서의 사용자 지정 도메인을 관리합니다.
- AWS Transfer Family 사용 설명서의 Route 53를 DNS 공급자로 사용.
- Route 53를 사용하여 도메인을 Amazon Lightsail 인스턴스로 지정합니다.

Amazon Route 53 상태 확인 생성

Amazon Route 53 상태 확인은 웹 애플리케이션, 웹 서버, 기타 리소스의 상태와 성능을 모니터링합니다. 상태 확인을 각각 생성하여 다음 중 하나를 모니터링할 수 있습니다.

- 지정한 리소스(예: 웹 서버)의 상태
- 다른 상태 확인의 상태
- Amazon CloudWatch 경보 상태입니다.
- 또한 Amazon Application Recovery Controller(ARC)를 사용하면 DNS 장애 조치 레코드로 라우팅 제어 상태 확인을 설정하여 애플리케이션의 트래픽 장애 조치를 관리할 수 있습니다. 자세한 내용은 Amazon Application Recovery Controller(ARC) 개발자 안내서를 참조하세요.

상태 확인 유형에 대한 개요는 Amazon Route 53 상태 확인 유형 섹션을 참조하세요. 상태 확인 생성에 대한 정보는 다음(상태 확인의 생성 및 업데이트)을 참조하십시오.

상태 확인을 생성하면 상태 확인의 상태를 받고, 상태가 변경될 때 알림을 받으며, DNS 장애 조치를 구성할 수 있습니다.

상태 확인 상태 및 경보 받기

Route 53 콘솔에서 상태 확인의 현재 및 최근 상태를 볼 수 있습니다. 또한 AWS SDKs AWS Command Line Interface AWS Tools for Windows PowerShell, 또는 Route 53 API 중 하나를 통해 프로그래밍 방식으로 상태 확인을 수행할 수 있습니다.

상태 확인의 상태가 변경될 때 알림을 받고 싶을 경우, 각 상태 확인에 대해 Amazon CloudWatch 경보를 구성할 수 있습니다.

상태 확인의 상태를 보고 알림을 받는 것에 대한 정보는 다음(상태 확인의 상태 모니터링 및 알림 수신)을 참조하십시오.

DNS 장애 조치 구성

동일한 기능을 수행하는 리소스가 여러 개 있을 경우, Route 53가 비정상 리소스의 트래픽을 정상 리소스로 라우팅하도록 DNS 장애 조치를 구성할 수 있습니다. 예를 들어 웹 서버가 2개일 경우 그 중 하나의 상태가 좋지 않으면 Route 53가 트래픽을 다른 웹 서버로 라우팅할 수 있습니다. 자세한 내용은 DNS 장애 조치 구성 단원을 참조하십시오.

주제

Amazon Route 53 상태 확인 유형

다음과 같은 유형의 Amazon Route 53 상태 확인을 생성할 수 있습니다.

엔드포인트를 모니터링하는 상태 확인

IP 주소나 도메인 이름으로 지정한 엔드포인트를 모니터링하는 상태 확인을 구성할 수 있습니다. Route 53는 지정한 간격에 따라 규칙적으로 인터넷을 통해 애플리케이션, 서버 또는 다른 리소스로 자동화된 요청을 제출하여 연결 및 사용이 가능하고 정상적으로 작동되는지 확인합니다. 또한, 사용자가 특정 URL의 웹 페이지 요청 등과 같은 요청을 할 때 해당 요청과 비슷한 요청을 만들도록 상태 확인을 구성할 수도 있습니다.

다른 상태 확인을 모니터링하는 상태 확인(계산된 상태 확인)

Route 53에서 다른 상태 확인의 상태를 정상으로 여기는지 아니면 비정상으로 여기는지를 모니터링하는 상태 확인을 생성할 수 있습니다. 이 기능은 예를 들어, 웹 서버 등과 같이 동일한 기능을 수행하는 리소스가 여러 개일 때 상태가 좋은 리소스의 최소 개수를 어느 수준 이상으로 유지하려 할 경우 유용합니다. 그러한 상태 확인의 알림을 구성하지 않고도 각 리소스의 상태 확인을 생성할 수 있습니다. 그런 다음, 다른 상태 확인의 상태를 모니터링하여 사용 가능한 웹 리소스 개수가 지정한 임계값 미만으로 떨어질 경우에만 알림을 보내는 상태 확인을 생성할 수 있습니다.

CloudWatch 경보를 모니터링하는 상태 확인

CloudWatch 지표(Amazon DynamoDB 데이터베이스에 대해 병목 현상이 발생한 읽기 이벤트 수, 정상으로 간주되는 Elastic Load Balancing 호스트 수 등)의 상태를 모니터링하는 CloudWatch 경보를 생성할 수 있습니다. 경보를 생성하면 해당 경보에 대해 CloudWatch에서 모니터링하는 데이터 스트림과 동일한 데이터 스트림을 모니터링하는 상태 확인을 생성할 수 있습니다.

복원성과 가용성을 높이기 위해 Route 53는 CloudWatch 경보가 `ALARM` 상태가 될 때까지 기다리지 않습니다. 상태 확인의 상태는 데이터 스트림에 따라 그리고 CloudWatch 경보의 기준에 따라 정상에서 비정상으로 변경됩니다.

Route 53는 다음과 같은 CloudWatch 경보를 지원합니다.

- 표준 분해능 지표. 고분해능 지표는 지원되지 않습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 고해상도 지표를 참조하세요.
- 통계: Average, Minimum, Maximum, Sum, SampleCount. 확장된 통계는 지원되지 않습니다.
- Route 53는 “N 중 M” 경보를 지원하지 않습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 경보 평가를 참조하세요.
- 상태 확인은 상태 확인과 동일한 AWS 계정에 있는 CloudWatch 경보만 모니터링할 수 있습니다.
- Route 53는 지표 수식을 사용하여 여러 CloudWatch 지표를 쿼리하는 경보를 지원하지 않습니다.

Amazon Application Recovery Controller(ARC) 라우팅 컨트롤러

ARC의 상태 확인은 간단한 켜기/끄기 스위치인 라우팅 컨트롤과 연결됩니다. 장애 조치 DNS 레코드를 사용하여 각 라우팅 컨트롤 상태 확인을 구성합니다. 그런 다음 ARC에서 라우팅 제어를 업데이트하여 트래픽을 다시 라우팅하고 가용 영역 또는 AWS리전 간에 애플리케이션을 장애 조치할 수 있습니다. 자세한 내용은 ARC 개발자 안내서의 ARC에서 라우팅 제어를 참조하세요.

Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법

Amazon Route 53에서 상태 확인이 정상인지 여부를 결정하는 데 사용하는 방법은 상태 확인 유형에 따라 다릅니다.

주제

- Route 53에서 엔드포인트를 모니터링하는 상태 확인의 상태를 판단하는 방법
- Route 53에서 기타 상태 확인을 모니터링하는 상태 확인의 상태를 판단하는 방법
- Route 53에서 CloudWatch 경보를 모니터링하는 상태 확인의 상태를 판단하는 방법

Route 53에서 엔드포인트를 모니터링하는 상태 확인의 상태를 판단하는 방법

Route 53는 전 세계 곳곳에 상태 확인 프로그램을 두고 있습니다. 엔드포인트를 모니터링하는 상태 확인을 생성하면 상태 확인 프로그램에서는 엔드포인트가 정상인지 확인하기 위해 지정하는 엔드포인트로 요청을 보내기 시작합니다. Route 53가 사용하도록 할 위치를 선택할 수 있고, 확인 사이의 간격을 10초마다 또는 30초마다로 지정할 수 있습니다. 다른 데이터 센터에 있는 Route 53 상태 확인 프로그램은 상호 연계되지 않으므로 선택한 간격에 상관 없이 초당 여러 번의 요청이 표시되는 경우도 있고 몇 초 동안 상태 확인이 없는 경우도 있습니다.

각각의 상태 확인 프로그램은 다음 두 가지 값을 기준으로 엔드포인트의 상태를 평가합니다.

- 응답 시간. 여러 가지 이유로 리소스의 응답 속도가 느리거나 상태 확인 요청에 응답하지 못할 수 있습니다. 예를 들어 리소스가 유지 관리를 위해 종료되거나, DDoS(Distributed Denial of Service) 공격을 받고 있거나, 네트워크가 다운되었을 수 있습니다.
- 엔드포인트가 사용자가 지정한 다수의 연속적인 상태 확인(장애 임계값)에 응답하는지 여부

Route 53는 상태 확인 프로그램에서 데이터를 집계하여 엔드포인트가 정상인지 확인합니다.

- 상태 확인 프로그램의 18% 이상이 엔드포인트가 정상이라고 보고하는 경우 Route 53는 엔드포인트가 정상이라고 간주합니다.
- 상태 확인 프로그램의 18% 미만이 엔드포인트가 정상이라고 보고하는 경우 Route 53는 엔드포인트가 비정상이라고 간주합니다.

여러 리전에 있는 상태 확인 프로그램이 엔드포인트가 정상이라고 간주하도록 보장하기 위해 18%라는 값을 선택했습니다. 이에 따라 네트워크 상태로 인해 엔드포인트가 일부 상태 확인 중인 위치에서 격리되었다는 이유만으로 엔드포인트가 비정상인 것으로 간주되는 상황이 방지됩니다. 이 값은 향후 릴리스에서는 달라질 수 있습니다.

개별 상태 확인 프로그램이 엔드포인트가 정상인지 확인하는 데 사용하는 응답 시간은 상태 확인의 유형에 따라 다릅니다.

- HTTP 및 HTTPS 상태 확인(HTTP and HTTPS health checks) - Route 53는 반드시 4초 안에 엔드포인트와의 TCP 연결을 설정해야 합니다. 뿐만 아니라 엔드포인트는 연결 후 2초 내에 2xx 또는 3xx의 HTTP 상태 코드와 반응해야 합니다.

  > **Note**
  >
  > HTTPS 상태 확인은 SSL/TLS 인증서를 검증하지 않으므로 인증서가 유효하지 않거나 만료된 경우에도 검사가 실패하지 않습니다.

- TCP 상태 확인(TCP health checks) - Route 53는 반드시 10초 안에 엔드포인트와의 TCP 연결을 설정해야 합니다.
- 문자열 매치로 HTTP 및 HTTPS 상태 확인(HTTP and HTTPS health checks with string matching) - HTTP 및 HTTPS 상태 확인과 마찬가지로 Route 53는 4초 내에 엔드포인트와의 TCP 연결을 설정해야 하고, 엔드포인트는 연결 후 2초 내에 2xx 또는 3xx의 HTTP 상태 코드와 반응해야 합니다.

Route 53 상태 확인 프로그램은 HTTP 상태 코드를 수신한 후 2초 내에 엔드포인트로부터 오는 응답의 본문을 수신해야 합니다. Route 53는 지정한 문자열을 찾기 위해 응답의 본문을 검색합니다. 문자열은 응답 본문의 최초 5,120바이트 내에서 모두 나타나야 합니다. 그렇지 않으면 엔드포인트는 상태 확인에 실패합니다. Route 53 콘솔을 사용한다면, 문자열 검색(Search String) 필드에서 문자열을 지정합니다. Route 53 API를 사용한다면, 상태 확인을 생성할 때 `SearchString` 요소에서 문자열을 지정합니다.

엔드포인트를 모니터링하는 상태 확인(TCP 상태 확인 제외)의 경우, 엔드포인트로부터의 응답에 헤더가 포함되어 있으면 헤더가 RFC7230, Hypertext Transfer Protocol(HTTP/1.1): Message Syntax and Routing의 섹션 3.2, "Header Fields"에 정의된 형식을 따라야 합니다.

Route 53에서는 실제 상태가 정상인지 비정상인지를 결정할 수 있는 충분한 데이터가 생길 때까지 새로운 상태 확인을 정상으로 간주합니다. 상태 확인 상태를 반전하는 옵션을 선택한 경우 Route 53에서 충분한 데이터가 생길 때까지 새로운 상태 확인을 비정상(unhealthy)으로 간주합니다.

Route 53에서 기타 상태 확인을 모니터링하는 상태 확인의 상태를 판단하는 방법

상태 확인은 다른 상태 확인의 상태를 모니터링할 수 있습니다. 이러한 유형의 상태 확인을 계산된 상태 확인이라 합니다. 모니터링을 수행하는 상태 확인을 상위 상태 확인이라 하며, 모니터링 대상인 상태 확인을 하위 상태 확인이라 합니다. 하나의 상위 상태 확인은 최대 255개의 하위 상태 확인을 모니터링할 수 있습니다. 모니터링 작동 방식은 다음과 같습니다.

- Route 53가 정상으로 간주되는 하위 상태 확인의 수를 합산합니다.
- Route 53는 정상으로 간주되는 상위 상태 확인의 상태에 대해 정상이어야 하는 하위 상태 확인의 수와 위에서 합산한 수를 비교합니다.

자세한 설명은 상태 확인 생성 또는 업데이트 시 지정하는 값에서 다른 상태 확인 모니터링(계산된 상태 확인) 섹션을 참조하세요.

Route 53에서는 실제 상태가 정상인지 비정상인지를 결정할 수 있는 충분한 데이터가 생길 때까지 새로운 상태 확인을 정상으로 간주합니다. 상태 확인 상태를 반전하는 옵션을 선택한 경우 Route 53에서 충분한 데이터가 생길 때까지 새로운 상태 확인을 비정상(unhealthy)으로 간주합니다. 상태 확인을 반전하면 Route 53는 정상 엔드포인트를 비정상으로 취급하고 그 반대의 경우도 마찬가지입니다.

Route 53에서 CloudWatch 경보를 모니터링하는 상태 확인의 상태를 판단하는 방법

CloudWatch 경보를 기반으로 상태 확인을 생성하면 Route 53는 경보 상태를 모니터링하는 대신 해당 경보의 데이터 스트림을 모니터링합니다. 데이터 스트림이 가리키는 경보 상태가 확인이면 상태 확인은 정상으로 간주합니다. 데이터 스트림이 가리키는 경보 상태가 경보면 상태 확인은 이상 있음으로 간주합니다. 데이터 스트림이 경보 상태를 판단하기에 충분한 정보를 제공하지 않을 경우, 상태 확인의 상태는 상태 확인의 상태의 설정, 즉 정상, 이상 있음, 마지막으로 알려진 상태 중 하나에 따라 결정됩니다. (Route 53 API에서 이 설정은 `InsufficientDataHealthStatus`입니다.)

Route 53는 교차 계정 CloudWatch 경보를 지원하지 않습니다.

> **Note**
>
> Route 53 상태 확인은 CloudWatch 경보 상태 대신 CloudWatch 데이터 스트림을 모니터링하므로 CloudWatch SetAlarmState API 작업을 사용하여 상태 확인의 상태를 강제로 변경할 수 없습니다.

Route 53에서는 실제 상태가 정상인지 비정상인지를 결정할 수 있는 충분한 데이터가 생길 때까지 새로운 상태 확인을 정상으로 간주합니다. 상태 확인 상태를 반전하는 옵션을 선택한 경우 Route 53에서 충분한 데이터가 생길 때까지 새로운 상태 확인을 비정상(unhealthy)으로 간주합니다. 상태 확인을 반전하면 Route 53는 정상 엔드포인트를 비정상으로 취급하고 그 반대의 경우도 마찬가지입니다.

상태 확인의 생성, 업데이트 및 삭제

> **Important**
>
> 레코드와 연결된 상태 확인을 업데이트 또는 삭제하는 경우 작업을 수행하기 전에 먼저 DNS 장애 조치 구성 시 상태 확인 업데이트 또는 삭제의 작업을 검토합니다.

이 섹션에서는 Route 53 상태 확인 관리와 관련된 다음 주제를 다룹니다.

1. 상태 확인의 생성 및 업데이트:
   - Route 53 콘솔을 사용하여 상태 확인을 생성하고 업데이트하는 방법을 알아봅니다.
   - 엔드포인트 모니터링, 프로토콜, IP 주소, 도메인 이름, 고급 구성 옵션 등 상태 확인을 생성하거나 업데이트할 때 지정해야 하는 값을 이해합니다.

2. 상태 확인을 생성할 때 표시되는 값:
   - 전체 URL 또는 IP 주소 및 포트와 같이 상태 확인을 생성할 때 Route 53 콘솔이 입력에 따라 표시하는 값을 알아봅니다.
3. CloudWatch 경보 변경에 대한 상태 확인 업데이트:
   - 연결된 CloudWatch 경보의 설정을 변경할 때 상태 확인을 업데이트하는 방법을 알아봅니다.
4. 상태 확인 삭제:
   - 절차에 따라 Route 53 콘솔을 사용하여 상태 확인을 삭제합니다.
5. DNS 장애 조치 구성 시 상태 확인 업데이트 또는 삭제:
   - DNS 레코드와 연결된 상태 확인을 업데이트하거나 삭제할 때 수행해야 하는 권장 작업을 파악하여 라우팅 및 장애 조치 구성이 적절한지 확인합니다.
6. 라우터 및 방화벽 규칙 구성:
   - Route 53 상태 확인 프로그램의 인바운드 트래픽을 허용하도록 라우터 및 방화벽 규칙을 구성하여 성공적인 상태 확인을 보장하는 방법을 이해합니다.

이 섹션에 제공된 정보를 따르면 Route 53 상태 확인을 효과적으로 생성, 업데이트 및 삭제하고, 구성을 관리하고, DNS 장애 조치 및 라우팅 정책과 적절하게 통합되게 할 수 있습니다.

주제

상태 확인의 생성 및 업데이트

다음 절차에서는 Route 53 콘솔을 이용해 상태 확인을 생성하고 업데이트하는 방법을 설명합니다.

> **Note**
>
> Route 53용 상태 확인 콘솔을 업데이트하고 있습니다. 전환 기간 동안에는 기존 콘솔을 계속 사용할 수 있습니다.

사용 중인 콘솔의 탭을 선택합니다.

- 새로운 콘솔
- 이전 콘솔

New console

상태 확인을 생성 또는 업데이트하려면

1. 이미 레코드와 연결된 상태 확인을 업데이트하는 경우 DNS 장애 조치 구성 시 상태 확인 업데이트 또는 삭제에서 권장하는 작업을 수행합니다.
2. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
3. 탐색 창에서 상태 확인(Health Checks)을 선택합니다.
4. 기존의 상태 확인을 업데이트하려면 상태 확인에 연결된 ID를 선택한 다음 편집을 선택합니다.

   상태 확인을 생성하려면 상태 확인 생성을 선택합니다.
5. 관련 값들을 입력합니다. 상태 확인을 생성한 후에는 일부 값들을 변경할 수 없다는 점에 유의하십시오. 자세한 내용은 상태 확인 생성 또는 업데이트 시 지정하는 값 단원을 참조하십시오.
6. 상태 확인 생성을 선택합니다.

   > **Note**
   >
   > Route 53에서는 실제 상태가 정상인지 비정상인지를 결정할 수 있는 충분한 데이터가 생길 때까지 새로운 상태 확인을 정상으로 간주합니다.
7. 상태 확인을 하나 이상의 Route 53 레코드와 연결합니다. 레코드 생성 및 업데이트에 대한 자세한 내용은 레코드 작업을 참조하십시오.

Old console

상태 확인을 생성 또는 업데이트하려면

1. 이미 레코드와 연결된 상태 확인을 업데이트하는 경우 DNS 장애 조치 구성 시 상태 확인 업데이트 또는 삭제에서 권장하는 작업을 수행합니다.
2. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
3. 탐색 창에서 상태 확인(Health Checks)을 선택합니다.
4. 기존의 상태 확인을 업데이트하려면, 상태 확인을 선택한 다음, [Edit Health Check]를 선택합니다.

   상태 확인을 생성하고 싶다면, [Create Health Check]를 선택합니다. 라벨 위에 마우스 포인터를 대면 도움말이 표시되어 설정에 관한 자세한 내용을 볼 수 있습니다.
5. 관련 값들을 입력합니다. 상태 확인을 생성한 후에는 일부 값들을 변경할 수 없다는 점에 유의하십시오. 자세한 내용은 상태 확인 생성 또는 업데이트 시 지정하는 값 단원을 참조하십시오.
6. [Create Health Check]를 선택합니다.

   > **Note**
   >
   > Route 53에서는 실제 상태가 정상인지 비정상인지를 결정할 수 있는 충분한 데이터가 생길 때까지 새로운 상태 확인을 정상으로 간주합니다. 상태 확인 상태를 반전하는 옵션을 선택한 경우 Route 53에서 충분한 데이터가 생길 때까지 새로운 상태 확인을 비정상(unhealthy)으로 간주합니다.
7. 상태 확인을 하나 이상의 Route 53 레코드와 연결합니다. 레코드 생성 및 업데이트에 대한 자세한 내용은 레코드 작업을 참조하십시오.

상태 확인 생성 또는 업데이트 시 지정하는 값

상태 확인을 생성 또는 업데이트할 때 적용 가능한 값을 지정합니다. 상태 확인을 생성한 후에는 일부 값들을 변경할 수 없다는 점에 유의하십시오.

주제

- 엔드포인트 모니터링
- 다른 상태 확인 모니터링(계산된 상태 확인)

- CloudWatch 경보 모니터링
- 고급 구성("Monitor an endpoint" 전용)
- 상태 확인 실패 시 알림 메시지를 받음

명칭

선택 사항이지만 권장되는 것: 상태 확인에 할당하고 싶은 이름. 이름(Name)에 대한 값을 지정하면, Route 53가 상태 확인에 태그를 추가하고 태그 키에 이름(Name)의 값을 할당하며 지정한 값을 태그 값에 할당합니다. 이름(Name) 태그의 값은 Route 53 콘솔의 상태 확인 목록에 표시되는데, 이는 상태 확인을 서로 쉽게 구별할 수 있게 해줍니다.

태그 지정 및 상태 확인에 대한 자세한 내용은 다음(상태 확인에 대한 이름 및 태그 지정)을 참조하십시오.

모니터링할 항목

이 상태 확인을 통해 엔드포인트 또는 다른 상태 확인의 상태를 모니터링할지 여부:

- 엔드포인트(Endpoint) - Route 53는 사용자가 지정하는 엔드포인트의 상태를 모니터링합니다. 도메인 이름 또는 IP 주소와 포트를 제공하여 엔드포인트를 지정할 수 있습니다.

  > **Note**
  >
  > AWS 엔드포인트가 아닌를 지정하면 추가 요금이 적용됩니다. AWS 엔드포인트의 정의를 비롯한 자세한 내용은 Route 53 요금(Route 53 Pricing) 페이지에서 "상태 확인" 섹션을 참조하세요.

- 다른 상태 확인(계산된 상태 확인)의 상태(Status of other health checks (calculated health check)) - Route 53는 이 상태 확인이 사용자가 지정하는 다른 상태 확인의 상태를 기준으로 정상인지 판단합니다. 또한, 정상으로 간주되는 이 상태 확인에 대해 상태 확인 중 얼마나 많이 정상이어야 하는지도 지정합니다.
- CloudWatch 경보 데이터 스트림의 상태(State of CloudWatch alarm data stream) - Route 53가 CloudWatch 경보의 데이터 스트림을 모니터링하여 이 상태 확인이 정상인지를 판단합니다.

엔드포인트 모니터링

> **Note**
>
> Route 53용 상태 확인 콘솔을 업데이트하고 있습니다. 전환 기간 동안에는 기존 콘솔을 계속 사용할 수 있습니다.

사용 중인 콘솔의 탭을 선택합니다.

- 새로운 콘솔
- 이전 콘솔

New console

이 상태 확인을 통해 엔드포인트를 모니터링하려면 다음 값을 지정하십시오:

- 엔드포인트 지정 기준
- IP 주소
- 도메인 이름

엔드포인트 지정

IP 주소나 도메인 이름을 사용하여 엔드포인트를 지정할지 여부.

상태 확인을 생성한 후에는 [Specify endpoint by]의 값을 변경할 수 없습니다.

IP 주소(IP address)("IP 주소로 엔드포인트 지정(Specify endpoint by IP address)" 전용)

드롭다운에서 프로토콜을 선택하고 IP 주소, 포트, 경로를 텍스트 상자에 입력합니다.

- 프로토콜은 다음 중 하나일 수 있습니다.

  HTTP - Route 53가 TCP 연결을 설정하려고 시도합니다. 성공할 경우 Route 53는 HTTP 요청을 제출하고 2xx 또는 3xx의 HTTP 상태 코드를 기다립니다.
- HTTPS - Route 53가 TCP 연결을 설정하려고 시도합니다. 성공할 경우 Route 53는 HTTPS 요청을 제출하고 2xx 또는 3xx의 HTTP 상태 코드를 기다립니다.

> **Important**
>
> HTTPS를 선택한다면 엔드포인트가 TLS v1.0, v1.1 또는 v1.2를 지원해야 합니다.

프로토콜 값으로 HTTPS를 선택할 경우 추가 요금이 적용됩니다. 자세한 내용은 Route 53 요금을 참조하세요.

- TCP - Route 53가 TCP 연결을 설정하려고 시도합니다.

자세한 내용은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 단원을 참조하십시오.

상태 확인을 생성한 후에는 프로토콜의 값을 변경할 수 없습니다.

IP 주소에서 IP 주소로 엔드포인트 지정을 선택한 경우 Route 53에서 상태 확인을 수행할 엔드포인트의 IPv4 또는 IPv6 주소를 입력합니다.

Route 53는 IP 주소가 로컬, 프라이빗, 라우팅 불가, 또는 멀티캐스트 범위에 있는 엔드포인트의 상태는 확인할 수 없습니다. 상태 확인을 생성할 수 없는 IP 주소에 대한 자세한 내용은 다음 문서를 참조하십시오.

- RFC 5735, Special Use IPv4 Addresses(RFC 5735, 특수 용도 IPv4 주소)
- RFC 6598, IANA-Reserved IPv4 Prefix for Shared Address Space(RFC 6598, IANA에서 공유 주소 공간으로 예약된 IPv4 접두사).
- RFC 5156, Special-Use IPv6 Addresses(RFC 5156, 특수 용도 IPv6 주소)

엔드포인트가 Amazon EC2 인스턴스일 경우, 탄력적 IP 주소를 생성하여 EC2 인스턴스와 연결하고 탄력적 IP 주소를 지정하는 것이 좋습니다. 이렇게 하면 인스턴스의 IP 주소가 변경되지 않습니다. 자세한 내용은 Amazon EC2 사용 설명서의 탄력적 IP 주소(EIP)를 참조하세요.

Amazon EC2 인스턴스를 삭제하는 경우 EIP에 연결된 상태 확인도 삭제해야 합니다. 자세한 내용은 Amazon Route 53 상태 확인의 모범 사례 단원을 참조하십시오.

> **Note**
>
> AWS 엔드포인트가 아닌를 지정하면 추가 요금이 적용됩니다. AWS 엔드포인트의 정의를 비롯한 자세한 내용은 Route 53 요금(Route 53 Pricing) 페이지에서 "상태 확인" 섹션을 참조하세요.

포트의 경우 Route 53에서 상태 확인을 수행할 엔드포인트의 포트를 입력합니다.

경로(HTTP 및 HTTPS 프로토콜만 해당)의 경우 상태 확인을 수행할 때 Route 53에서 요청할 경로를 입력합니다. 이 경로는 엔드포인트가 정상일 때, 엔드포인트가 2xx나 3xx의 HTTP 상태 코드를 반환하는 모든 값이 될 수 있습니다. 예를 들면 /docs/route53-health-check.html 파일이 여기에 해당됩니다. /welcome.html?language=jp&login=y와 같은 쿼리 문자열 파라미터를 포함할 수도 있습니다. 앞에 슬래시(/) 문자가 없으면 Route 53가 자동으로 하나 추가합니다.

도메인 이름(Domain name)("도메인 이름으로 엔드포인트 지정(Specify endpoint by domain name)" 전용, 모든 프로토콜)

도메인 이름으로 엔드포인트 지정(Specify endpoint by domain name)을 선택한 경우 Route 53가 상태 확인을 수행하게 하려는 엔드포인트의 도메인 이름(example.com) 또는 하위 도메인 이름(backend.example.com) 입니다.

도메인 이름으로 엔드포인트를 지정하도록 선택하는 경우, Route 53는 도메인 이름(Domain name)에 지정한 도메인 이름을 확인하기 위해 요청 간격(Request interval)에 지정한 간격으로 DNS 쿼리를 전송합니다. 그런 다음 Route 53는 DNS가 반환하는 IP 주소를 사용하여 엔드포인트의 상태를 확인합니다.

> **Note**
>
> 도메인 이름으로 엔드포인트를 지정하는 경우에는 Route 53가 IPv4만 사용하여 상태 확인을 엔드포인트에 전송합니다. [Domain name]에 지정하는 도메인 이름에 대해 A 유형의 레코드가 없는 경우에는 "DNS resolution failed" 오류와 함께 상태 확인이 중단됩니다.

장애 조치, 지리 위치, 지리적 근접성, 지연 시간, 다중 값, 가중치 레코드의 상태를 확인하려는 경우, 도메인 이름에 따라 엔드포인트를 지정하도록 선택하면 각 엔드포인트에 대해 별도의 상태 확인을 생성하는 것이 좋습니다. 예를 들어, www.example.com의 콘텐츠를 제공하는 각 HTTP 서버마다 상태 확인을 생성합니다. [Domain name]의 값은 레코드의 이름(www.example.com)이 아니라 서버의 도메인 이름(예: us-east-2-www.example.com)을 지정합니다.

> **Important**
>
> 이 구성에서 [Domain name]의 값이 레코드의 이름과 일치하는 상태 확인을 생성한 후 상태 확인을 이러한 레코드와 연결하는 경우 상태 확인 결과를 예측할 수 없습니다.

또한, 프로토콜(Protocol) 값이 HTTP 또는 HTTPS인 경우, 이 목록의 앞부분에서 호스트 이름(Host name)에 설명된 대로 Route 53는 `Host` 헤더의 도메인 이름(Domain name) 값을 전달합니다. 프로토콜(Protocol)의 값이 TCP라면, Route 53는 `Host` 헤더를 전달하지 않습니다.

> **Note**
>
> AWS 엔드포인트가 아닌를 지정하면 추가 요금이 적용됩니다. AWS 엔드포인트의 정의를 비롯한 자세한 내용은 Route 53 요금(Route 53 Pricing) 페이지에서 "상태 확인" 섹션을 참조하세요.

Old console

이 상태 확인을 통해 엔드포인트를 모니터링하려면 다음 값을 지정하십시오:

- 엔드포인트 지정
- 프로토콜
- IP 주소
- 호스트 이름
- Port
- 도메인 이름
- 경로

엔드포인트 지정

IP 주소나 도메인 이름을 사용하여 엔드포인트를 지정할지 여부.

상태 확인을 생성한 후에는 [Specify endpoint by]의 값을 변경할 수 없습니다.

프로토콜

엔드포인트 상태 확인을 위해 Route 53에서 사용하길 바라는 방법:

- HTTP - Route 53가 TCP 연결을 설정하려고 시도합니다. 성공할 경우 Route 53는 HTTP 요청을 제출하고 2xx 또는 3xx의 HTTP 상태 코드를 기다립니다.
- HTTPS - Route 53가 TCP 연결을 설정하려고 시도합니다. 성공할 경우 Route 53는 HTTPS 요청을 제출하고 2xx 또는 3xx의 HTTP 상태 코드를 기다립니다.

> **Important**
>
> HTTPS를 선택한다면 엔드포인트가 TLS v1.0, v1.1 또는 v1.2를 지원해야 합니다.

프로토콜 값으로 HTTPS를 선택할 경우 추가 요금이 적용됩니다. 자세한 내용은 Route 53 요금을 참조하세요.

- TCP - Route 53가 TCP 연결을 설정하려고 시도합니다.

자세한 내용은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 단원을 참조하십시오.

상태 확인을 생성한 후에는 프로토콜의 값을 변경할 수 없습니다.

IP 주소(IP address)("IP 주소로 엔드포인트 지정(Specify endpoint by IP address)" 전용)

IP 주소로 엔드포인트 지정(Specify endpoint by IP address)을 선택한 경우 Route 53가 상태 확인을 수행하게 하려는 엔드포인트의 IPv4 또는 IPv6 주소입니다.

Route 53는 IP 주소가 로컬, 프라이빗, 라우팅 불가, 또는 멀티캐스트 범위에 있는 엔드포인트의 상태는 확인할 수 없습니다. 상태 확인을 생성할 수 없는 IP 주소에 대한 자세한 내용은 다음 문서를 참조하십시오.

- RFC 5735, Special Use IPv4 Addresses(RFC 5735, 특수 용도 IPv4 주소)
- RFC 6598, IANA-Reserved IPv4 Prefix for Shared Address Space(RFC 6598, IANA에서 공유 주소 공간으로 예약된 IPv4 접두사).
- RFC 5156, Special-Use IPv6 Addresses(RFC 5156, 특수 용도 IPv6 주소)

엔드포인트가 Amazon EC2 인스턴스일 경우, 탄력적 IP 주소를 생성하여 EC2 인스턴스와 연결하고 탄력적 IP 주소를 지정하는 것이 좋습니다. 이렇게 하면 인스턴스의 IP 주소가 변경되지 않습니다. 자세한 내용은 Amazon EC2 사용 설명서의 탄력적 IP 주소(EIP)를 참조하세요.

Amazon EC2 인스턴스를 삭제하는 경우 EIP에 연결된 상태 확인도 삭제해야 합니다. 자세한 내용은 Amazon Route 53 상태 확인의 모범 사례 단원을 참조하십시오.

> **Note**
>
> AWS 엔드포인트가 아닌를 지정하면 추가 요금이 적용됩니다. AWS 엔드포인트의 정의를 비롯한 자세한 내용은 Route 53 요금 페이지에서 "상태 확인" 섹션을 참조하세요.

호스트 이름(Host name)("IP 주소로 엔드포인트 지정(Specify endpoint by IP address)" 전용, HTTP 및 HTTPS 프로토콜 전용)

HTTP 및 HTTPS 상태 확인의 `Host` 헤더에서 Route 53가 전달하길 원하는 값입니다. 이 값은 일반적으로 Route 53가 상태 확인을 수행하기를 원하는 웹 사이트의 전체 주소 도메인 이름입니다. 다음은 Route 53가 엔드포인트의 상태를 확인할 때 어떻게 `Host` 헤더를 생성하는지를 보여줍니다.

- 포트(Port)에 **`80`** 값을 지정하고, 프로토콜(Protocol)에 HTTP를 지정하면, Route 53가 호스트 이름(Host name) 값을 포함하는 `Host` 헤더를 엔드포인트에 전달합니다.
- 포트(Port)에 **`443`** 값을 지정하고, 프로토콜(Protocol)에 HTTPS를 지정하면, Route 53가 호스트 이름(Host name) 값을 포함하는 `Host` 헤더를 엔드포인트에 전달합니다.
- 포트(Port)에 다른 값을 지정하고, 프로토콜(Protocol)에 HTTP 또는 HTTPS를 지정하면, Route 53가 *`Host name`*:*`Port`*를 포함하는 `Host` 헤더를 엔드포인트에 전달합니다.

IP 주소로 엔드포인트를 지정하도록 선택하고 호스트 이름 값을 지정하지 않은 경우, Route 53는 이전 사례의 각각에서 `Host` 헤더의 IP 주소 값을 대체합니다.

포트

Route 53에서 상태 확인을 수행할 엔드포인트의 포트입니다.

도메인 이름(Domain name)("도메인 이름으로 엔드포인트 지정(Specify endpoint by domain name)" 전용, 모든 프로토콜)

도메인 이름으로 엔드포인트 지정(Specify endpoint by domain name)을 선택한 경우 Route 53가 상태 확인을 수행하게 하려는 엔드포인트의 도메인 이름(example.com) 또는 하위 도메인 이름(backend.example.com) 입니다.

도메인 이름으로 엔드포인트를 지정하도록 선택하는 경우, Route 53는 도메인 이름(Domain name)에 지정한 도메인 이름을 확인하기 위해 요청 간격(Request interval)에 지정한 간격으로 DNS 쿼리를 전송합니다. 그런 다음 Route 53는 DNS가 반환하는 IP 주소를 사용하여 엔드포인트의 상태를 확인합니다.

> **Note**
>
> 도메인 이름으로 엔드포인트를 지정하는 경우에는 Route 53가 IPv4만 사용하여 상태 확인을 엔드포인트에 전송합니다. [Domain name]에 지정하는 도메인 이름에 대해 A 유형의 레코드가 없는 경우에는 "DNS resolution failed" 오류와 함께 상태 확인이 중단됩니다.

장애 조치, 지리 위치, 지리적 근접성, 지연 시간, 다중 값, 가중치 레코드의 상태를 확인하려는 경우, 도메인 이름에 따라 엔드포인트를 지정하도록 선택하면 각 엔드포인트에 대해 별도의 상태 확인을 생성하는 것이 좋습니다. 예를 들어, www.example.com의 콘텐츠를 제공하는 각 HTTP 서버마다 상태 확인을 생성합니다. [Domain name]의 값은 레코드의 이름(www.example.com)이 아니라 서버의 도메인 이름(예: us-east-2-www.example.com)을 지정합니다.

> **Important**
>
> 이 구성에서 [Domain name]의 값이 레코드의 이름과 일치하는 상태 확인을 생성한 후 상태 확인을 이러한 레코드와 연결하는 경우 상태 확인 결과를 예측할 수 없습니다.

또한, 프로토콜(Protocol) 값이 HTTP 또는 HTTPS인 경우, 이 목록의 앞부분에서 호스트 이름(Host name)에 설명된 대로 Route 53는 `Host` 헤더의 도메인 이름(Domain name) 값을 전달합니다. 프로토콜(Protocol)의 값이 TCP라면, Route 53는 `Host` 헤더를 전달하지 않습니다.

> **Note**
>
> AWS 엔드포인트가 아닌를 지정하면 추가 요금이 적용됩니다. AWS 엔드포인트의 정의를 비롯한 자세한 내용은 Route 53 요금 페이지에서 "상태 확인" 섹션을 참조하세요.

경로(HTTP 및 HTTPS 프로토콜 전용)

상태 확인을 수행할 때 Route 53에서 요청할 경로입니다. 이 경로는 엔드포인트가 정상일 때 2xx 또는 3xx의 HTTP 상태 코드를 반환하는 값이면 무엇이든 가능한데, 예를 들면 `/docs/route53-health-check.html` 파일이 있습니다. 쿼리 문자열 파라미터를 포함해도 됩니다(예: `/welcome.html?language=jp&login=y`). 앞에 슬래시(/) 문자가 없으면 Route 53가 자동으로 하나 추가합니다.

다른 상태 확인 모니터링(계산된 상태 확인)

> **Note**
>
> Route 53용 상태 확인 콘솔을 업데이트하고 있습니다. 전환 기간 동안에는 기존 콘솔을 계속 사용할 수 있습니다.

사용 중인 콘솔의 탭을 선택합니다.

- 새로운 콘솔
- 이전 콘솔

New console

이 상태 확인을 통해 다른 상태 확인의 상태를 모니터링하려면 다음 값을 지정하십시오:

- 모니터링할 상태 확인
- 정상 보고 시기

모니터링할 상태 확인

이 상태 확인의 상태를 결정하기 위해 Route 53에서 모니터링하도록 하려는 상태 확인입니다.

[Health checks to monitor]에 최대 256개의 상태 확인을 추가할 수 있습니다. 목록에서 상태 확인을 제거하려면 해당 상태 확인에 대한 강조 표시의 오른쪽에 있는 [x]를 선택합니다.

> **Note**
>
> 다른 계산된 상태 확인의 상태를 모니터링하기 위한 계산된 상태 확인을 구성할 수는 없습니다.

계산된 상태 확인이 모니터링 중인 상태 확인을 비활성화할 경우, Route 53는 계산된 상태 확인이 정상인지 여부를 계산하기 때문에 비활성화된 상태 확인이 정상인 것으로 간주합니다. 비활성화된 상태 확인을 비정상인 것으로 간주해야 할 경우에는 Invert health check status(상태 확인 상태 변환) 확인란을 선택합니다.

정상 보고 시기

Route 53가 상태 확인이 정상인지 확인하기 위해 수행하도록 하려는 계산:

- 선택된 상태 확인 y 중 최소 x개가 정상인 경우 정상 보고(Report healthy when at least x of y selected health checks are healthy) - Route 53는 모니터링할 상태 확인(Health checks to monitor)에 추가한 지정된 수의 상태 확인이 정상일 때 이 상태 확인이 정상인 것으로 간주합니다. 다음 사항에 유의하세요.
  - 모니터링할 상태 확인(Health checks to monitor)에서 상태 확인의 수보다 큰 수를 지정할 경우, Route 53는 항상 이 상태 확인을 비정상으로 간주합니다.

- 0을 지정하면 Route 53는 항상 이 상태 확인을 정상으로 간주합니다.
- 모든 상태 확인이 정상인 경우 정상 보고(AND)(Report healthy when all health checks are healthy(AND)) - Route 53는 모니터링할 상태 확인(Health checks to monitor)에 추가한 모든 상태 확인이 정상일 때만 이 상태 확인이 정상인 것으로 간주합니다.
- 하나 이상의 상태 확인이 정상인 경우 정상 보고(OR)(Report healthy when one or more health checks are healthy(OR)) - Route 53는 모니터링할 상태 확인(Health checks to monitor)에 추가한 상태 확인 중 하나라도 정상일 때 이 상태 확인이 정상인 것으로 간주합니다.

Old console

이 상태 확인을 통해 다른 상태 확인의 상태를 모니터링하려면 다음 값을 지정하십시오:

- 모니터링할 상태 확인
- 정상 보고 시기
- 상태 확인 상태 반전
- 비활성

모니터링할 상태 확인

이 상태 확인의 상태를 결정하기 위해 Route 53에서 모니터링하도록 하려는 상태 확인입니다.

[Health checks to monitor]에 최대 256개의 상태 확인을 추가할 수 있습니다. 목록에서 상태 확인을 제거하려면 해당 상태 확인에 대한 강조 표시의 오른쪽에 있는 [x]를 선택합니다.

> **Note**
>
> 다른 계산된 상태 확인의 상태를 모니터링하기 위한 계산된 상태 확인을 구성할 수는 없습니다.

계산된 상태 확인이 모니터링 중인 상태 확인을 비활성화할 경우, Route 53는 계산된 상태 확인이 정상인지 여부를 계산하기 때문에 비활성화된 상태 확인이 정상인 것으로 간주합니다. 비활성화된 상태 확인을 비정상인 것으로 간주해야 할 경우에는 Invert health check status(상태 확인 상태 변환) 확인란을 선택합니다.

정상 보고 시기

Route 53가 상태 확인이 정상인지 확인하기 위해 수행하도록 하려는 계산:

- 선택된 상태 확인 y 중 최소 x개가 정상인 경우 정상 보고(Report healthy when at least x of y selected health checks are healthy) - Route 53는 모니터링할 상태 확인(Health checks to monitor)에 추가한 지정된 수의 상태 확인이 정상일 때 이 상태 확인이 정상인 것으로 간주합니다. 다음 사항에 유의하세요.
  - 모니터링할 상태 확인(Health checks to monitor)에서 상태 확인의 수보다 큰 수를 지정할 경우, Route 53는 항상 이 상태 확인을 비정상으로 간주합니다.
  - 0을 지정하면 Route 53는 항상 이 상태 확인을 정상으로 간주합니다.
- 모든 상태 확인이 정상인 경우 정상 보고(AND)(Report healthy when all health checks are healthy(AND)) - Route 53는 모니터링할 상태 확인(Health checks to monitor)에 추가한 모든 상태 확인이 정상일 때만 이 상태 확인이 정상인 것으로 간주합니다.
- 하나 이상의 상태 확인이 정상인 경우 정상 보고(OR)(Report healthy when one or more health checks are healthy(OR)) - Route 53는 모니터링할 상태 확인(Health checks to monitor)에 추가한 상태 확인 중 하나라도 정상일 때 이 상태 확인이 정상인 것으로 간주합니다.

상태 확인 상태 반전(이전 콘솔만 해당)

새 콘솔에서 상태 확인을 반전하려면 상태 확인 반전 섹션을 참조하세요.

Route 53가 상태 확인의 상태를 반전하도록 할지 선택합니다. 이 옵션을 선택하면 Route 53가 상태가 정상일 때는 상태 확인이 비정상인 것으로 간주하고, 그 반대도 마찬가지입니다.

비활성화됨(이전 콘솔만 해당)

새 콘솔에서 상태 확인을 비활성화하려면 상태 확인 비활성화 또는 활성화 섹션을 참조하세요.

Route 53의 상태 확인 실행을 정지시킵니다. 상태 확인을 비활성화하면 Route 53가 참조된 상태 확인 상태의 집계를 중지합니다.

상태 확인을 비활성화한 후에는 Route 53는 상태 확인 상태가 항상 정상인 것으로 간주합니다. DNS 장애 조치를 구성한 경우에는 Route 53가 해당 리소스로 트래픽을 계속 라우팅합니다. 트래픽이 리소스로 라우팅되는 것을 중지해야 할 경우에는 상태 확인을 반전합니다.

> **Note**
>
> 상태 확인에 대한 요금은 상태 확인이 비활성화되어 있을 때도 적용됩니다.

CloudWatch 경보 모니터링

> **Note**
>
> Route 53용 상태 확인 콘솔을 업데이트하고 있습니다. 전환 기간 동안에는 기존 콘솔을 계속 사용할 수 있습니다.

사용 중인 콘솔의 탭을 선택합니다.

- 새로운 콘솔
- 이전 콘솔

New console

이 상태 확인을 통해 CloudWatch 경보의 경보 상태를 모니터링하려면 다음 값을 지정하세요.

- CloudWatch 경보
- 상태 확인 상태

CloudWatch 경보

Route 53에서 이 상태 확인이 정상인지 확인하기 위해 사용하려는 CloudWatch 경보를 선택합니다. CloudWatch 경보는 상태 확인 AWS 계정 과 동일해야 합니다.

> **Note**
>
> Route 53는 다음과 같은 CloudWatch 경보를 지원합니다.
>
> - 표준 분해능 지표. 고분해능 지표는 지원되지 않습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 고해상도 지표를 참조하세요.
> - 통계: `Average`, `Minimum`, `Maximum`, `Sum` 및 `SampleCount`. 확장된 통계는 지원되지 않습니다.
> - Route 53는 “N 중 M” 경보를 지원하지 않습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 경보 평가를 참조하세요.
>
> Route 53는 지표 수식을 사용하여 여러 CloudWatch 지표를 쿼리하는 경보를 지원하지 않습니다.

경보를 생성하려는 경우 다음 단계를 수행하십시오.

1. 생성을 선택합니다. 새 브라우저 탭에 CloudWatch 콘솔이 나타납니다.
2. 관련 값들을 입력합니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 CloudWatch 경보 편집 또는 삭제를 참조하세요.
3. Route 53 콘솔이 나타나는 브라우저 탭으로 돌아갑니다.
4. [CloudWatch alarm] 목록 옆의 새로 고침 버튼을 선택합니다.
5. 목록에서 새 경보를 선택합니다.

> **Important**
>
> 상태 확인을 생성한 후 CloudWatch 경보의 설정을 변경할 경우 상태 확인을 업데이트해야 합니다. 자세한 내용은 CloudWatch 경보 설정 변경 시 상태 확인 업데이트(CloudWatch 경보만 모니터링하는 상태 확인) 단원을 참조하십시오.

상태 확인 상태

CloudWatch에 데이터가 부족하여 CloudWatch 경보(CloudWatch alarm)에서 선택한 경보의 상태를 확인할 데이터가 충분하지 않은 경우 상태 확인의 상태(정상, 비정상, 또는 마지막으로 알려진 상태)를 선택합니다. 마지막으로 알려진 상태를 사용하도록 선택하면 Route 53에서는 마지막으로 경보 상태를 확인할 만큼 CloudWatch에 충분한 데이터가 있었던 때의 상태 확인의 상태를 사용합니다. 마지막으로 알려진 상태가 없는 새로운 상태 확인의 경우 상태 확인의 기본 상태는 정상입니다.

상태 확인 상태(Health check status)는 CloudWatch 지표에 대한 데이터 스트림을 잠시 사용할 수 없는 경우 임시 상태를 제공합니다. (Route 53는 해당 경보의 상태가 아니라 CloudWatch 지표에 대한 데이터 스트림을 모니터링합니다.) 측정치를 자주 또는 장기간(몇 시간 이상) 사용하지 않을 예정인 경우, 마지막으로 알려진 상태를 사용하지 않는 것이 좋습니다.

Old console

이 상태 확인을 통해 CloudWatch 경보의 경보 상태를 모니터링하려면 다음 값을 지정하세요.

- CloudWatch 경보
- 상태 확인 상태

- 상태 확인 상태 반전
- 비활성

CloudWatch 경보

Route 53에서 이 상태 확인이 정상인지 확인하기 위해 사용하려는 CloudWatch 경보를 선택합니다. CloudWatch 경보는 상태 확인 AWS 계정 과 동일해야 합니다.

> **Note**
>
> Route 53는 다음과 같은 CloudWatch 경보를 지원합니다.
>
> - 표준 분해능 지표. 고분해능 지표는 지원되지 않습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 고해상도 지표를 참조하세요.
> - 통계: `Average`, `Minimum`, `Maximum`, `Sum` 및 `SampleCount`. 확장된 통계는 지원되지 않습니다.
> - Route 53는 “N 중 M” 경보를 지원하지 않습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 경보 평가를 참조하세요.
>
> Route 53는 지표 수식을 사용하여 여러 CloudWatch 지표를 쿼리하는 경보를 지원하지 않습니다.

경보를 생성하려는 경우 다음 단계를 수행하십시오.

1. 생성을 선택합니다. 새 브라우저 탭에 CloudWatch 콘솔이 나타납니다.
2. 관련 값들을 입력합니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 CloudWatch 경보 편집 또는 삭제를 참조하세요.
3. Route 53 콘솔이 나타나는 브라우저 탭으로 돌아갑니다.
4. [CloudWatch alarm] 목록 옆의 새로 고침 버튼을 선택합니다.
5. 목록에서 새 경보를 선택합니다.

> **Important**
>
> 상태 확인을 생성한 후 CloudWatch 경보의 설정을 변경할 경우 상태 확인을 업데이트해야 합니다. 자세한 내용은 CloudWatch 경보 설정 변경 시 상태 확인 업데이트 (CloudWatch 경보만 모니터링하는 상태 확인) 단원을 참조하십시오.

상태 확인 상태

CloudWatch에 데이터가 부족하여 CloudWatch 경보(CloudWatch alarm)에서 선택한 경보의 상태를 확인할 데이터가 충분하지 않은 경우 상태 확인의 상태(정상, 비정상, 또는 마지막으로 알려진 상태)를 선택합니다. 마지막으로 알려진 상태를 사용하도록 선택하면 Route 53에서는 마지막으로 경보 상태를 확인할 만큼 CloudWatch에 충분한 데이터가 있었던 때의 상태 확인의 상태를 사용합니다. 마지막으로 알려진 상태가 없는 새로운 상태 확인의 경우 상태 확인의 기본 상태는 정상입니다.

상태 확인 상태(Health check status)는 CloudWatch 지표에 대한 데이터 스트림을 잠시 사용할 수 없는 경우 임시 상태를 제공합니다. (Route 53는 해당 경보의 상태가 아니라 CloudWatch 지표에 대한 데이터 스트림을 모니터링합니다.) 측정치를 자주 또는 장기간(몇 시간 이상) 사용하지 않을 예정인 경우, 마지막으로 알려진 상태를 사용하지 않는 것이 좋습니다.

상태 확인 상태 반전(이전 콘솔만 해당)

새 콘솔에서 상태 확인을 반전하려면 상태 확인 반전 섹션을 참조하세요.

Route 53가 상태 확인의 상태를 반전하도록 할지 선택합니다. 이 옵션을 선택하면 Route 53가 상태가 정상일 때는 상태 확인이 비정상인 것으로 간주하고, 그 반대도 마찬가지입니다.

비활성화됨(이전 콘솔만 해당)

새 콘솔에서 상태 확인을 비활성화하려면 상태 확인 비활성화 또는 활성화 섹션을 참조하세요.

Route 53의 상태 확인 실행을 정지시킵니다. 상태 확인을 비활성화하면 Route 53는 해당 CloudWatch 지표의 모니터링을 중지합니다.

상태 확인을 비활성화한 후에는 Route 53는 상태 확인 상태가 항상 정상인 것으로 간주합니다. DNS 장애 조치를 구성한 경우에는 Route 53가 해당 리소스로 트래픽을 계속 라우팅합니다. 트래픽이 리소스로 라우팅되는 것을 중지해야 할 경우에는 상태 확인을 반전합니다.

> **Note**
>
> 상태 확인에 대한 요금은 상태 확인이 비활성화되어 있을 때도 적용됩니다.

고급 구성("Monitor an endpoint" 전용)

> **Note**
>
> Route 53용 상태 확인 콘솔을 업데이트하고 있습니다. 전환 기간 동안에는 기존 콘솔을 계속 사용할 수 있습니다.

- 새로운 콘솔
- 이전 콘솔

New console

- 요청 간격
- 실패 임계값
- 문자열 일치
- 검색 문자열
- 지연 시간 그래프
- SNI 활성화
- 호스트 이름

요청 간격

각 Route 53 상태 확인 프로그램이 엔드포인트로부터 응답을 받는 시점과 그 다음 상태 확인 요청을 전송하는 시점 사이에 경과된 초 단위 시간. 30초 간격을 선택한 경우 전 세계 데이터 센터에 있는 각 Route 53 상태 확인 프로그램에서 30초 간격으로 엔드포인트에 상태 확인 요청을 보냅니다. 평균적으로 엔드포인트에서는 약 2초 간격으로 상태 확인 요청을 수신합니다. 간격을 10초로 선택하면, 엔드포인트는 1초당 1회 이상 요청을 받게 됩니다.

다른 데이터 센터에 있는 Route 53 상태 확인 프로그램은 상호 연계되지 않으므로 선택한 간격에 상관 없이 초당 여러 번의 요청이 표시되는 경우도 있고 몇 초 동안 상태 확인이 없는 경우도 있습니다.

상태 확인을 생성한 후에는 [Request interval]의 값을 변경할 수 없습니다.

> **Note**
>
> 요청 간격(Request interval)의 값으로 빠른 간격(10초)을 선택한 경우 추가 요금이 적용됩니다. 자세한 내용은 Route 53 요금을 참조하세요.

실패 임계값

이 현재 엔드포인트의 상태를 비정상에서 정상 또는 그 반대로 변경하도록 하기 위해서 엔드포인트가 Route 53를 위해 전송 또는 실패해야 하는 연속적인 상태 확인 횟수입니다. 자세한 내용은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 단원을 참조하십시오.

문자열 일치(String matching)(HTTP 및 HTTPS 전용)

Route 53가 HTTP 또는 HTTPS 요청을 엔드포인트로 제출하고 지정된 문자열에 대한 응답의 본문을 검색함으로써 엔드포인트의 상태를 판단하기를 원하는가 여부. 응답의 본문이 문자열 검색(Search string)에서 지정한 값을 포함하고 있다면, Route 53는 엔드포인트가 정상이라고 판단합니다. 그렇지 않다면, 또는 엔드포인트가 응답하지 않는다면, Route 53는 엔드포인트가 비정상이라고 여깁니다. 문자열 검색은 응답 본문의 최초 5,120바이트 내에서 모두 나타나야 합니다.

상태 확인을 생성한 후에는 [String matching]의 값을 변경할 수 없습니다.

> **Note**
>
> 문자열 일치(String matching) 값으로 예(Yes)를 선택하는 경우 추가 요금이 적용됩니다. 자세한 내용은 Route 53 요금을 참조하세요.

상태 확인 프로그램이 압축된 응답을 처리하는 방법

엔드포인트가 압축된 응답을 반환하는 웹 서버인 경우 Route 53 상태 확인 프로그램은 웹 서버가 상태 확인 프로그램이 지원하는 압축 알고리즘을 사용하여 응답을 압축한 경우에만 지정된 문자열 검색을 확인하기 전에 응답을 압축 해제합니다. 상태 확인 프로그램은 다음과 같은 압축 알고리즘을 지원합니다.

- Gzip
- Deflate

응답이 다른 알고리즘을 사용하여 압축된 경우 상태 확인 프로그램은 문자열을 검색하기 전에 응답을 압축 해제할 수 없습니다. 이 경우 검색은 거의 항상 실패하며 Route 53는 엔드포인트를 비정상으로 간주합니다.

문자열 검색(Search string)("문자열 일치(String matching)"가 활성화된 경우만)

Route 53가 엔드포인트로부터 오는 응답의 본문에서 검색하길 원하는 문자열입니다. 최대 길이는 255자입니다.

Route 53는 응답의 본문에서 문자열 검색(Search string)을 검색하는 경우를 고려합니다.

지연 시간 그래프

Route 53에서 여러 AWS 리전의 상태 확인기와 엔드포인트 간의 지연 시간을 측정할지 여부를 선택합니다. 이 옵션을 선택하면 CloudWatch 지연 시간 그래프가 Route 53 콘솔의 상태 확인(Health checks) 페이지에 지연 시간(Latency) 탭에 나타납니다. Route 53 상태 확인 프로그램이 엔드포인트에 연결할 수 없으면 Route 53가 그 엔드포인트에 대한 지연 시간 그래프를 표시할 수 없습니다.

상태 확인을 생성한 후에는 [Latency measurements]의 값을 변경할 수 없습니다.

> **Note**
>
> 상태 확인 프로그램과 엔드포인트 간 지연을 측정하도록 Route 53를 구성할 경우 추가 요금이 적용됩니다. 자세한 내용은 Route 53 요금을 참조하세요.

SNI 활성화(HTTPS 전용)

Route 53에서 TLS 협상 중에 `client_hello` 메시지의 엔드포인트로 호스트 이름을 보내도록 할지 여부를 지정합니다. 그러면 엔드포인트에서 해당하는 SSL/TLS 인증서를 사용하여 HTTPS 요청에 응답할 수 있습니다.

일부 엔드포인트의 경우, HTTPS 요청에는 client_hello 메시지에 호스트 이름이 포함되어야 합니다. SNI를 활성화하지 않으면 상태 확인 상태가 실패로 표시될 수 있습니다. 오류 메시지는 서버가 SNI 정보가 포함되지 않은 요청에 응답하도록 구성된 방식에 따라 달라집니다. 상태 확인은 다른 이유로 실패 상태가 될 수도 있습니다. SNI를 사용하는데도 여전히 오류가 발생하는 경우, 엔드포인트의 SSL/TLS 구성을 확인하고 인증서가 유효한지 확인합니다.

다음과 같은 요구 사항을 확인합니다.

- 엔드포인트가 SNI를 지원해야 합니다.

- 엔드포인트의 SSL/TLS 인증서에는 `Common Name` 필드의 도메인 이름과 `Subject Alternative Names` 필드의 그 밖의 항목이 포함됩니다. 인증서의 도메인 이름 중 하나는 호스트 이름(Host name)에 지정하는 값과 일치해야 합니다.

상태 확인 리전

Route 53에서 권장 리전의 상태 확인 프로그램을 사용하여 엔드포인트의 상태를 확인할지 또는 지정한 리전의 상태 확인 프로그램을 사용하여 엔드포인트의 상태를 확인할지를 선택합니다.

상태 확인을 업데이트하여 상태 확인을 수행한 리전을 제거하면 Route 53는 해당 리전에서 최대 1시간 동안 검사를 계속 수행합니다. 이렇게 하면 일부 상태 확인 프로그램이 항상 엔드포인트를 확인하게 됩니다(예를 들어, 세 개의 리전을 네 개의 다른 리전으로 바꾼 경우).

사용자 지정을 선택하는 경우 리전에 대한 x를 선택하여 리전을 제거합니다. 목록 하단의 공백을 클릭하여 리전을 목록에 다시 추가합니다. 최소 3개의 리전을 지정해야 합니다.

호스트 이름(Host name)("IP 주소로 엔드포인트 지정(Specify endpoint by IP address)" 전용, HTTP 및 HTTPS 프로토콜 전용)

HTTP 및 HTTPS 상태 확인의 `Host` 헤더에서 Route 53가 전달하길 원하는 값입니다. 이 값은 일반적으로 Route 53가 상태 확인을 수행하기를 원하는 웹 사이트의 전체 주소 도메인 이름입니다. 다음은 Route 53가 엔드포인트의 상태를 확인할 때 어떻게 `Host` 헤더를 생성하는지를 보여줍니다.

- 포트(Port)에 **`80`** 값을 지정하고, 프로토콜(Protocol)에 HTTP를 지정하면, Route 53가 호스트 이름(Host name) 값을 포함하는 `Host` 헤더를 엔드포인트에 전달합니다.
- 포트에 **`443`** 값을 지정하고, 프로토콜에 HTdTPS를 지정하면, Route 53가 호스트 이름 값을 포함하는 `Host` 헤더를 엔드포인트에 전달합니다.
- 포트(Port)에 다른 값을 지정하고, 프로토콜(Protocol)에 HTTP 또는 HTTPS를 지정하면, Route 53가 *`Host name`*:*`Port`*를 포함하는 `Host` 헤더를 엔드포인트에 전달합니다.

IP 주소로 엔드포인트를 지정하도록 선택하고 호스트 이름 값을 지정하지 않은 경우, Route 53는 이전 사례의 각각에서 `Host` 헤더의 IP 주소 값을 대체합니다.

Old console

엔드포인트를 모니터링하기 위해 이 옵션을 선택할 경우 다음 설정을 지정할 수도 있습니다:

- 요청 간격
- 실패 임계값
- 문자열 일치

- 검색 문자열
- 지연 시간 그래프
- SNI 활성화
- 상태 확인 프로그램 리전
- 상태 확인 상태 반전
- 비활성

요청 간격

각 Route 53 상태 확인 프로그램이 엔드포인트로부터 응답을 받는 시점과 그 다음 상태 확인 요청을 전송하는 시점 사이에 경과된 초 단위 시간. 30초 간격을 선택한 경우 전 세계 데이터 센터에 있는 각 Route 53 상태 확인 프로그램에서 30초 간격으로 엔드포인트에 상태 확인 요청을 보냅니다. 평균적으로 엔드포인트에서는 약 2초 간격으로 상태 확인 요청을 수신합니다. 간격을 10초로 선택하면, 엔드포인트는 1초당 1회 이상 요청을 받게 됩니다.

다른 데이터 센터에 있는 Route 53 상태 확인 프로그램은 상호 연계되지 않으므로 선택한 간격에 상관 없이 초당 여러 번의 요청이 표시되는 경우도 있고 몇 초 동안 상태 확인이 없는 경우도 있습니다.

상태 확인을 생성한 후에는 [Request interval]의 값을 변경할 수 없습니다.

> **Note**
>
> 요청 간격(Request interval)의 값으로 빠른 간격(10초)을 선택한 경우 추가 요금이 적용됩니다. 자세한 내용은 Route 53 요금을 참조하세요.

실패 임계값

이 현재 엔드포인트의 상태를 비정상에서 정상 또는 그 반대로 변경하도록 하기 위해서 엔드포인트가 Route 53를 위해 전송 또는 실패해야 하는 연속적인 상태 확인 횟수입니다. 자세한 내용은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 단원을 참조하십시오.

문자열 일치(String matching)(HTTP 및 HTTPS 전용)

Route 53가 HTTP 또는 HTTPS 요청을 엔드포인트로 제출하고 지정된 문자열에 대한 응답의 본문을 검색함으로써 엔드포인트의 상태를 판단하기를 원하는가 여부. 응답의 본문이 문자열 검색(Search string)에서 지정한 값을 포함하고 있다면, Route 53는 엔드포인트가 정상이라고 판

단합니다. 그렇지 않다면, 또는 엔드포인트가 응답하지 않는다면, Route 53는 엔드포인트가 비정상이라고 여깁니다. 문자열 검색은 응답 본문의 최초 5,120바이트 내에서 모두 나타나야 합니다.

상태 확인을 생성한 후에는 [String matching]의 값을 변경할 수 없습니다.

> **Note**
>
> 문자열 일치(String matching) 값으로 예(Yes)를 선택하는 경우 추가 요금이 적용됩니다. 자세한 내용은 Route 53 요금을 참조하세요.

상태 확인 프로그램이 압축된 응답을 처리하는 방법

엔드포인트가 압축된 응답을 반환하는 웹 서버인 경우 Route 53 상태 확인 프로그램은 웹 서버가 상태 확인 프로그램이 지원하는 압축 알고리즘을 사용하여 응답을 압축한 경우에만 지정된 문자열 검색을 확인하기 전에 응답을 압축 해제합니다. 상태 확인 프로그램은 다음과 같은 압축 알고리즘을 지원합니다.

- Gzip
- Deflate

응답이 다른 알고리즘을 사용하여 압축된 경우 상태 확인 프로그램은 문자열을 검색하기 전에 응답을 압축 해제할 수 없습니다. 이 경우 검색은 거의 항상 실패하며 Route 53는 엔드포인트를 비정상으로 간주합니다.

문자열 검색(Search string)("문자열 일치(String matching)"가 활성화된 경우만)

Route 53가 엔드포인트로부터 오는 응답의 본문에서 검색하길 원하는 문자열입니다. 최대 길이는 255자입니다.

Route 53는 응답의 본문에서 문자열 검색(Search string)을 검색하는 경우를 고려합니다.

지연 시간 그래프

Route 53에서 여러 AWS 리전의 상태 확인기와 엔드포인트 간의 지연 시간을 측정할지 여부를 선택합니다. 이 옵션을 선택하면 CloudWatch 지연 시간 그래프가 Route 53 콘솔의 상태 확인(Health checks) 페이지에 지연 시간(Latency) 탭에 나타납니다. Route 53 상태 확인 프로그램이 엔드포인트에 연결할 수 없으면 Route 53가 그 엔드포인트에 대한 지연 시간 그래프를 표시할 수 없습니다.

상태 확인을 생성한 후에는 [Latency measurements]의 값을 변경할 수 없습니다.

> **Note**
>
> 상태 확인 프로그램과 엔드포인트 간 지연을 측정하도록 Route 53를 구성할 경우 추가 요금이 적용됩니다. 자세한 내용은 Route 53 요금을 참조하세요.

SNI 활성화(HTTPS 전용)

Route 53에서 TLS 협상 중에 `client_hello` 메시지의 엔드포인트로 호스트 이름을 보내도록 할지 여부를 지정합니다. 그러면 엔드포인트에서 해당하는 SSL/TLS 인증서를 사용하여 HTTPS 요청에 응답할 수 있습니다.

일부 엔드포인트의 경우, HTTPS 요청에는 `client_hello` 메시지에 호스트 이름이 포함되어야 합니다. SNI를 활성화하지 않으면 상태 확인 상태가 실패로 표시될 수 있습니다. 오류 메시지는 서버가 SNI 정보가 포함되지 않은 요청에 응답하도록 구성된 방식에 따라 달라집니다. 상태 확인은 다른 이유로 실패 상태가 될 수도 있습니다. SNI를 사용하는데도 여전히 오류가 발생하는 경우, 엔드포인트의 SSL/TLS 구성을 확인하고 인증서가 유효한지 확인합니다.

다음과 같은 요구 사항을 확인합니다.

- 엔드포인트가 SNI를 지원해야 합니다.
- 엔드포인트의 SSL/TLS 인증서에는 `Common Name` 필드의 도메인 이름과 `Subject Alternative Names` 필드의 그 밖의 항목이 포함됩니다. 인증서의 도메인 이름 중 하나는 호스트 이름(Host name)에 지정하는 값과 일치해야 합니다.

상태 확인 리전

Route 53에서 권장 리전의 상태 확인 프로그램을 사용하여 엔드포인트의 상태를 확인할지 또는 지정한 리전의 상태 확인 프로그램을 사용하여 엔드포인트의 상태를 확인할지를 선택합니다.

상태 확인을 업데이트하여 상태 확인을 수행한 리전을 제거하면 Route 53는 해당 리전에서 최대 1시간 동안 검사를 계속 수행합니다. 이렇게 하면 일부 상태 확인 프로그램이 항상 엔드포인트를 확인하게 됩니다(예를 들어, 세 개의 리전을 네 개의 다른 리전으로 바꾼 경우).

사용자 지정을 선택하는 경우 리전에 대한 x를 선택하여 리전을 제거합니다. 목록 하단의 공백을 클릭하여 리전을 목록에 다시 추가합니다. 최소 3개의 리전을 지정해야 합니다.

상태 확인 상태 반전(이전 콘솔만 해당)

새 콘솔에서 상태 확인을 반전하려면 상태 확인 반전 섹션을 참조하세요.

Route 53가 상태 확인의 상태를 반전하도록 할지 선택합니다. 이 옵션을 선택하면 Route 53가 상태가 정상일 때는 상태 확인이 비정상인 것으로 간주하고, 그 반대도 마찬가지입니다. 예를 들

어, 일치하는 문자열을 구성하고 엔드포인트가 특정 값을 반환하는 경우 Route 53가 상태 확인을 비정상으로 간주하고자 할 수 있습니다.

비활성화됨(이전 콘솔만 해당)

새 콘솔에서 상태 확인을 비활성화하려면 상태 확인 비활성화 또는 활성화 섹션을 참조하세요.

Route 53의 상태 확인 실행을 정지시킵니다. 상태 확인을 비활성화하면 Route 53는 TCP와 엔드포인트의 연결 시도를 중지합니다.

상태 확인을 비활성화한 후에는 Route 53는 상태 확인 상태가 항상 정상인 것으로 간주합니다. DNS 장애 조치를 구성한 경우에는 Route 53가 해당 리소스로 트래픽을 계속 라우팅합니다. 트래픽이 리소스로 라우팅되는 것을 중지해야 할 경우에는 상태 확인을 반전합니다.

> **Note**
>
> 상태 확인에 대한 요금은 상태 확인이 비활성화되어 있을 때도 적용됩니다.

상태 확인 실패 시 알림 메시지를 받음

다음 옵션을 사용하여 상태 확인 실패 시 이메일 알림을 구성합니다:

- Create alarm
- Send notification to
- Topic name
- Recipient email addresses

알람 생성(상태 확인 생성 시에만 해당)

기본 CloudWatch 경보를 생성하길 원하는지 여부를 지정합니다. 예(Yes)를 선택하면, 이 엔드포인트의 상태가 비정상으로 변경되고 Route 53가 1분 동안 엔드포인트가 비정상이라고 여길 때 CloudWatch가 Amazon SNS 알림을 보냅니다.

> **Note**
>
> 상태가 다시 정상으로 돌아갈 경우 CloudWatch에서 Amazon SNS 알림을 한 번 더 보내도록 하려면 상태 확인을 생성한 후 다른 경보를 생성하면 됩니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 Amazon CloudWatch 경보 생성을 참조하세요.

기존 상태 확인에 대한 경보를 생성하길 원하거나 Route 53가 1분(기본값) 이상 또는 미만 동안 엔드포인트가 비정상이라고 여길 때 알림을 받기를 원한다면, 아니요(No)를 선택하고 상태 확인을 생성한 후 경보를 추가합니다. 자세한 내용은 CloudWatch를 이용한 상태 확인 모니터링 단원을 참조하십시오.

알림 보내기(경보 생성 시에만 해당)

CloudWatch가 기존 Amazon SNS 주제 또는 새로운 주제에 알림을 전송하기를 원하는지 여부를 다음과 같이 지정합니다.

- 기존 SNS 주제(Existing SNS topic) - 목록에서 주제의 이름을 선택합니다. 주제는 미국 동부(버지니아 북부) 리전에 있어야 합니다.
- 새 SNS 주제(New SNS topic) - 주제 이름(Topic name)에서 이름을 입력하고, 수신자(Recipients)에서 알림 수신자의 이메일 주소를 입력합니다. 여러 개의 주소는 쉼표(,), 세미콜론(;), 공백으로 구분합니다.

  Route 53는 미국 동부(버지니아 북부) 리전에서 주제를 생성합니다.

제목 이름(새로운 SNS 주제를 생성할 때만 해당)

[New SNS Topic]을 지정했다면, 새 주제의 이름을 입력합니다.

수신자 이메일 주소(새로운 SNS 주제를 생성할 때만 해당)

[New SNS topic]을 지정한 경우 알림 수신자의 이메일 주소를 입력합니다. 여러 개의 이름은 쉼표(,), 세미콜론(;), 공백으로 구분합니다.

상태 확인 생성 시 Amazon Route 53가 표시하는 값

[Create Health Check] 페이지는 입력한 값을 근거로 다음의 값들을 표시합니다.

URL

Route 53가 상태 확인을 수행할 때 요청을 보낼 전체 URL(HTTP 또는 HTTPS 상태 확인의 경우) 또는 IP 주소 및 포트(TCP 상태 확인용).

상태 확인 유형

이 상태 확인을 위해 지정한 설정에 기반을 둔 [Basic] 또는 [Basic + additional options]. 추가 옵션의 요금에 대한 자세한 내용은 Route 53 요금을 참조하세요.

CloudWatch 경보 설정 변경 시 상태 확인 업데이트(CloudWatch 경보만 모니터링하는 상태 확인)

CloudWatch 경보의 데이터 스트림을 모니터링하는 Route 53 상태 확인을 생성한 후 CloudWatch 경보의 설정을 업데이트할 경우, Route 53는 상태 확인의 경보 설정을 자동으로 업데이트하지 않습니다. 새로운 경보 설정을 사용하여 상태 확인을 시작하려면 상태 확인을 업데이트해야 합니다.

> **Note**
>
> 상태 확인을 프로그래밍 방식으로 업데이트하려면 `UpdateHealthCheck` API를 사용하십시오. `AlarmIdentifier` 및 `Region`의 현재 값을 지정하면 Route 53가 CloudWatch의 최신 설정을 받습니다. 자세한 내용은 Amazon Route 53 API 참조의 UpdateHealthCheck를 참조하세요.

> **Note**
>
> Route 53용 상태 확인 콘솔을 업데이트하고 있습니다. 전환 기간 동안에는 기존 콘솔을 계속 사용할 수 있습니다.

사용 중인 콘솔의 탭을 선택합니다.

- 새로운 콘솔
- 이전 콘솔

New console

상태 확인을 새로운 CloudWatch 경보 설정으로 업데이트하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 상태 확인을 선택합니다.
3. 업데이트하려는 상태 확인의 연결된 ID를 선택합니다.
4. 편집을 선택합니다.

상태 확인의 CloudWatch 경보가 변경되었다는 메시지가 표시됩니다. [Details] 필드에 새로운 경보 설정이 표시됩니다.

5. 저장(Save)을 선택합니다.

Old console

상태 확인을 새로운 CloudWatch 경보 설정으로 업데이트하려면(콘솔)

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 상태 확인(Health Checks)을 선택합니다.
3. 업데이트하려는 상태 확인의 확인란을 선택합니다.
4. [Edit health check]를 선택합니다.

   상태 확인의 CloudWatch 경보가 변경되었다는 메시지가 표시됩니다. [Details] 필드에 새로운 경보 설정이 표시됩니다.
5. 저장(Save)을 선택합니다.

상태 확인 비활성화 또는 활성화

상태 확인을 비활성화하면 Route 53가 상태 확인을 수행하지 못하게 됩니다. 상태 확인을 비활성화하면 Route 53가 참조된 상태 확인 상태의 집계를 중지합니다. 상태 확인을 비활성화한 후에는 Route 53는 상태 확인 상태가 항상 정상인 것으로 간주합니다. DNS 장애 조치를 구성한 경우에는 Route 53가 해당 리소스로 트래픽을 계속 라우팅합니다.

> **Note**
>
> Route 53용 상태 확인 콘솔을 업데이트하고 있습니다. 전환 기간 동안에는 기존 콘솔을 계속 사용할 수 있습니다.

상태 확인을 생성하거나 편집할 때 이전 콘솔에서 상태 확인을 비활성화하거나 활성화할 수 있습니다. 자세한 내용은 상태 확인 생성 또는 업데이트 시 지정하는 값 단원을 참조하십시오.

새 콘솔에서 상태 확인을 비활성화하려면 다음 절차를 수행합니다.

상태 확인을 비활성화하거나 활성화하려면(새 콘솔만 해당)

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 상태 확인을 선택합니다.
3. 작업 열에서 점 3개를 선택한 다음 비활성화 또는 활성화를 선택합니다.

   또는 비활성화하거나 활성화하려는 상태 확인의 연결된 ID를 선택합니다.
4. 구성 테이블에서 상태 필드는 상태 확인의 활성화 여부를 지정합니다.
5. 상태 확인을 비활성화하거나 활성화하려면 비활성화 또는 활성화를 선택합니다

상태 확인 반전

상태 확인을 반전하면 Route 53가 상태가 정상일 때는 상태 확인이 비정상인 것으로 간주하고, 그 반대도 마찬가지입니다.

> **Note**
>
> Route 53용 상태 확인 콘솔을 업데이트하고 있습니다. 전환 기간 동안에는 기존 콘솔을 계속 사용할 수 있습니다.

상태 확인을 생성하거나 편집할 때 이전 콘솔에서 상태 확인을 반전할 수 있습니다. 자세한 내용은 상태 확인 생성 또는 업데이트 시 지정하는 값 단원을 참조하십시오.

새 콘솔에서 상태 확인을 반전하려면 다음 절차를 수행합니다.

상태 확인을 반전하려면(새 콘솔만 해당)

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 상태 확인을 선택합니다.
3. 작업 열에서 점 3개를 선택한 다음 반전을 선택합니다.

   또는 반전하려는 상태 확인의 연결된 ID를 선택합니다.
4. 구성 테이블에서 반전된 파일은 상태 확인이 반전되는지(예) 또는 아닌지(아니요)를 지정합니다.
5. 상태 확인을 반전하려면 반전을 선택합니다.

반전된 상태를 실행 취소하려는 경우 반전된 필드가 예 인 경우 반전을 다시 선택합니다.

상태 확인 삭제

상태 확인을 비활성화하려면 다음 절차를 수행합니다.

> **Note**
>
> 를 사용하고 AWS Cloud Map 인스턴스를 등록할 때 Route 53 상태 확인을 생성 AWS Cloud Map 하도록를 구성한 경우 Route 53 콘솔을 사용하여 상태 확인을 삭제할 수 없습니다. 인스턴스 등록을 취소하면 상태 확인이 자동으로 삭제됩니다. Route 53 콘솔에서 상태 확인이 사라질 때까지 몇 시간이 더 걸릴 수 있습니다.

> **Note**
>
> Route 53용 상태 확인 콘솔을 업데이트하고 있습니다. 전환 기간 동안에는 기존 콘솔을 계속 사용할 수 있습니다.

사용 중인 콘솔의 탭을 선택합니다.

- 새로운 콘솔
- 이전 콘솔

New console

상태 확인을 삭제하려면

1. 레코드와 연결된 상태 확인을 삭제하는 경우 DNS 장애 조치 구성 시 상태 확인 업데이트 또는 삭제에서 권장하는 작업을 수행합니다.
2. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
3. 탐색 창에서 상태 확인을 선택합니다.
4. 삭제하려는 상태 확인의 연결된 ID를 선택합니다.
5. Delete(삭제)를 선택합니다.

6. 텍스트 상자에 **confirm**을 입력한 다음, 삭제를 선택합니다.

Old console

상태 확인을 삭제하려면(콘솔)

1. 레코드와 연결된 상태 확인을 삭제하는 경우 DNS 장애 조치 구성 시 상태 확인 업데이트 또는 삭제에서 권장하는 작업을 수행합니다.
2. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
3. 탐색 창에서 상태 확인(Health Checks)을 선택합니다.
4. 오른쪽 창에서 삭제할 상태 확인을 선택합니다.
5. [Delete Health Check]를 선택합니다.
6. 확인하려면 [Yes, Delete]를 선택합니다.

DNS 장애 조치 구성 시 상태 확인 업데이트 또는 삭제

레코드와 연결된 상태 확인을 업데이트 또는 삭제하거나 상태 확인을 연결한 레코드를 변경할 때는 변경 사항이 DNS 쿼리의 라우팅 및 DNS 장애 조치 구성에 어떤 영향을 미치는지 반드시 고려해야 합니다.

> **Important**
>
> Route 53는 상태 확인이 하나 이상의 레코드와 연결된 경우에도 상태 확인 삭제를 방지하지 않습니다. 상태 확인을 삭제하고 연결된 레코드를 업데이트하지 않는 경우 상태 확인의 향후 상태가 예측될 수 없으며 변경될 수 있습니다. 이는 DNS 장애 조치 구성에 대한 DNS 쿼리 라우팅에 영향을 미칩니다.

레코드와 이미 연결된 상태 확인을 업데이트 또는 삭제하려면 다음 작업을 수행하는 것이 좋습니다.

1. 상태 확인과 연결된 레코드를 찾습니다. 상태 확인과 연결된 레코드를 찾으려면 다음 중 하나를 반드시 수행해야 합니다.
   - Route 53 콘솔을 사용하여 각 호스팅 영역에서 레코드를 검토합니다. 자세한 내용은 레코드 나열 단원을 참조하십시오.

- 각 호스팅 영역에서 `ListResourceRecordSets` API 작업을 실행하여 그 반응을 살핍니다. 자세한 내용은 Amazon Route 53 API 참조에서 ListResourceRecordSets를 참조하세요.

2. 상태 확인 업데이트 또는 삭제, 또는 레코드 업데이트로 인한 동작의 변화를 평가합니다. 평가를 기반으로 변경할 사항을 결정합니다.

   자세한 내용은 상태 확인을 생략하면 어떻게 됩니까? 섹션을 참조하세요.

3. 해당하는 상태 확인 및 레코드를 변경합니다. 자세한 정보는 다음의 주제를 참조하세요.

   - 상태 확인의 생성 및 업데이트
   - 레코드 편집

4. 사용하지 않는 상태 확인이 있다면, 삭제합니다. 자세한 내용은 상태 확인 삭제 단원을 참조하십시오.

Amazon Route 53 상태 확인을 위한 라우터 및 방화벽 규칙 구성

Route 53는 엔드포인트의 상태를 점검할 때, 상태 확인 생성 시에 지정한 IP 주소 및 포트에 HTTP, HTTPS, 또는 TCP 요청을 전송합니다. 상태 확인이 성공하려면 라우터 및 방화벽 규칙은 Route 53 상태 확인 프로그램이 사용하는 IP 주소에서 오는 인바운드 트래픽을 반드시 허용해야 합니다.

Route 53 상태 확인기의 현재 IP 주소 목록, Route 53 이름 서버 및 기타 AWS 서비스는 섹션을 참조하세요Amazon Route 53 서버의 IP 주소 범위.

Amazon EC2에서 보안 그룹은 방화벽과 같은 역할을 합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EC2 보안 그룹을 참조하세요. Route 53 상태 확인을 허용하도록 보안 그룹을 구성하려면 각 IP 주소 범위의 인바운드 트래픽을 허용하거나 AWS관리형 접두사 목록을 사용할 수 있습니다. Amazon EC2

AWS관리형 접두사 목록을 사용하려면 보안 그룹을 수정하여의 인바운드 트래픽을 허용합니다. `com.amazonaws.<region>.route53-healthchecks`여기서 `<region>` 는 Amazon EC2 인스턴스 또는 리소스 AWS 리전 의 입니다. Route 53 상태 확인을 사용하여 IPv6 엔드포인트를 확인하는 경우 `com.amazonaws.<region>.ipv6.route53-healthchecks`로부터의 인바운드 트래픽도 허용해야 합니다.

AWS관리형 접두사 목록에 대한 자세한 내용은 Amazon VPC 사용 설명서의 AWS관리형 접두사 목록 작업을 참조하세요.

> **Important**
>
> 허용된 IP 주소 목록에 IP 주소를 추가할 때 상태 확인을 생성할 때 지정한 각 AWS 리전의 CIDR 범위와 글로벌 CIDR 범위에 있는 모든 IP 주소를 추가합니다. 상태 확인 요청은 한 리전의 한 IP 주소에서만 제공됩니다. 그러나 해당 IP 주소는 언제든지 해당 리전의 다른 IP 주소로 변경될 수 있습니다.
> 현재 및 이전 상태 확인 프로그램 IP 주소를 모두 포함하려면 모든 /26 및 /18 IP 주소 범위를 허용 목록에 추가합니다. 자세한 내용은 AWS 일반 참조의 AWS IP 주소 범위를 참조하세요.
> 인바운드 보안 그룹에 AWS관리형 접두사 목록을 추가하면 필요한 모든 범위가 자동으로 추가됩니다.

DNS 장애 조치 구성

동일한 기능을 수행하는 2개 이상의 리소스(예: 1개 이상의 HTTP 서버 또는 메일 서버)가 있는 경우, Amazon Route 53를 구성하여 리소스들의 상태를 확인하고 정상적인 리소스만을 사용하여 DNS 쿼리에 응답하도록 할 수 있습니다. 예를 들어, 전 세계에 3개의 데이터 센터에서 각각 2개의 서버, 즉 6개의 서버 상에서 example.com라는 웹 사이트가 호스팅된다고 가정합니다. 이러한 서버들의 상태를 확인하고 현재 정상적인 서버만을 사용하여 example.com에 대한 DNS 쿼리에 응답하도록 Route 53를 구성할 수 있습니다.

Route 53는 단순 구성 및 복잡 구성 모두에서 리소스의 상태를 확인할 수 있습니다.

- 단순 구성에서 이름과 유형이 모두 동일한 레코드의 그룹(예: 유형이 A인 example.com에 대한 가중치 기반 레코드의 그룹)을 생성합니다. 그런 다음 Route 53를 구성해 해당 리소스의 상태를 확인합니다. Route 53는 리소스의 상태를 기반으로 DNS 쿼리에 응답합니다. 자세한 내용은 단순 Amazon Route 53 구성에서 상태 확인 작동 방식 섹션을 참조하세요.
- 더욱 복잡한 구성에서는 여러 기준을 기반으로 트래픽을 라우팅하는 레코드 트리를 생성합니다. 예를 들어, 사용자에 대한 지연 시간이 가장 중요한 기준인 경우 지연 시간 별칭 레코드를 사용하여 최적의 지연 시간을 제공하는 리전으로 트래픽을 라우팅할 수 있습니다. 지연 시간 별칭 레코드에서 각 리전의 가중치 기반 레코드를 별칭 대상으로 보유할 수 있습니다. 가중치 기반 레코드는 인스턴스 유형을 기반으로 트래픽을 EC2 인스턴스로 라우팅할 수 있습니다. 단순 구성에서와 마찬가지로 Route 53가 리소스 상태를 기반으로 트래픽을 라우팅하도록 구성할 수 있습니다. 자세한 내용은 상태 확인이 복잡한 Amazon Route 53 구성에서 작동하는 방식 섹션을 참조하세요.

주제

- DNS 장애 조치 구성을 위한 작업 목록

- 단순 Amazon Route 53 구성에서 상태 확인 작동 방식
- 상태 확인이 복잡한 Amazon Route 53 구성에서 작동하는 방식
- 상태 확인 구성 시 Amazon Route 53의 레코드 선택 방식
- 액티브-액티브 및 액티브-패시브 장애 조치
- 프라이빗 호스팅 영역에서 장애 조치 구성
- Amazon Route 53가 장애 조치 문제를 방지하는 방법

DNS 장애 조치 구성을 위한 작업 목록

Route 53를 사용하여 DNS 장애 조치를 구성하려면 다음 작업을 수행하세요.

1. 구성에 대한 완전한 트리 다이어그램을 그리고 각 노드마다 어떤 유형의 레코드(가중치 기반 별칭, 장애 조치, 지연 시간 등)를 생성하는지 나타냅니다. 트리 상단에 사용자가 웹 사이트 또는 웹 애플리케이션에 액세스하는 데 사용하는 도메인 이름(예: example.com)에 대한 레코드를 놓습니다.

   트리 다이어그램에 표시되는 레코드의 종류는 구성의 복잡성에 따라 다릅니다.

   - 단순 구성에서 다이어그램에 어떠한 별칭 레코드도 포함하지 않거나 별칭 레코드가 다른 Route 53 레코드 대신 ELB 로드 밸런서와 같은 리소스에 직접 트래픽을 라우팅합니다. 자세한 내용은 단순 Amazon Route 53 구성에서 상태 확인 작동 방식 섹션을 참조하세요.
   - 복잡한 구성에서는 상태 확인이 복잡한 Amazon Route 53 구성에서 작동하는 방식 주제의 예제처럼 다중 트리에서 별칭 레코드(가중치 기반 별칭, 장애 조치 별칭 등)와 비 별칭 레코드의 조합이 다이어그램에 포함됩니다.

   > **Note**
   >
   > 복잡한 라우팅 구성에 대한 레코드를 빠르고 쉽게 생성한 후 상태 확인에 연결하려면 트래픽 흐름 시각적 편집기를 사용하고 구성을 트래픽 정책으로 저장할 수 있습니다. 그런 다음 동일한 호스팅 영역이나 여러 호스팅 영역의 하나 이상의 도메인 이름(예: example.com) 또는 하위 도메인 이름(예: www.example.com)과 해당 트래픽 정책을 연결할 수 있습니다. 새 구성이 예상대로 수행되지 않을 경우 업데이트를 롤백할 수도 있습니다. 자세한 내용은 트래픽 흐름을 사용하여 DNS 트래픽 라우팅 섹션을 참조하세요.

   자세한 내용은 다음 설명서를 참조하세요.

   - 라우팅 정책 선택

- 별칭 또는 비 별칭 레코드 선택

2. 데이터 센터에서 실행 중인 Amazon EC2 서버 및 이메일 서버와 같은 별칭 레코드를 생성할 수 없는 리소스의 상태 확인을 생성합니다. 이러한 상태 확인을 비 별칭 레코드와 연결합니다.

   자세한 내용은 상태 확인의 생성, 업데이트 및 삭제 섹션을 참조하세요.

3. 필요한 경우 상태 확인에서 지정한 엔드포인트에 대해 Route 53가 규칙적으로 요청을 전송할 수 있도록 하기 위해서는 라우터 및 방화벽 규칙을 구성합니다. 자세한 내용은 Amazon Route 53 상태 확인을 위한 라우터 및 방화벽 규칙 구성 섹션을 참조하세요.

4. 다이어그램에서 비 별칭 레코드 전체를 생성하고 2단계에서 생성한 상태 확인을 해당 레코드와 연결합니다.

   별칭 레코드가 없는 단순 구성에서 DNS 장애 조치를 구성하는 경우 남은 작업을 건너뜁니다.

5. 트래픽을 ELB 로드 밸런서 및 CloudFront 배포와 같은 AWS 리소스로 라우팅하는 별칭 레코드를 생성합니다. 리소스가 비정상일 때 Route 53가 트리의 다른 가지를 시도하도록 하려면 별칭 레코드 각각에 대해 대상 상태 평가(Evaluate Target Health) 값을 예(Yes)로 설정합니다. (일부 AWS 리소스에서는 대상 상태 평가가 지원되지 않습니다.)

6. 1단계에서 생성한 트리 다이어그램의 하단에서 4단계와 5단계에서 생성한 레코드로 트래픽을 라우팅하는 별칭 레코드를 생성합니다. 비 별칭 레코드 전체가 트리의 가지에서 비정상인 경우 Route 53가 트리의 다른 가지를 시도하도록 하려면 별칭 레코드 각각에 대해 대상 상태 평가(Evaluate Target Health)의 값을 예(Yes)로 설정합니다.

   다른 레코드를 생성하기 전까지 다른 레코드로 트래픽을 라우팅하는 별칭 레코드를 생성할 수 없다는 것에 유의하십시오.

단순 Amazon Route 53 구성에서 상태 확인 작동 방식

동일한 기능을 수행하는 둘 이상의 리소스(예: example.com에 대한 둘 이상의 웹 서버)가 있으면 다음 상태 확인 기능을 사용하여 트래픽을 정상적인 리소스에만 라우팅할 수 있습니다.

EC2 인스턴스 및 기타 리소스(비 별칭 레코드)의 상태 확인

EC2 인스턴스와 같이 별칭 레코드를 생성할 수 없는 리소스로 트래픽을 라우팅하는 경우 각 리소스에 대해 레코드 및 상태 확인을 생성합니다. 그런 다음 각 상태 확인을 해당 레코드와 연결합니다. 상태 확인은 해당 리소스의 상태를 주기적으로 확인하고, Route 53는 상태 확인 보고에 따라 정상인 리소스에만 트래픽을 라우팅합니다.

AWS 리소스의 상태 평가(별칭 레코드)

별칭 레코드를 사용하여 트래픽을 ELB 로드 밸런서와 같은 선택한 AWS 리소스로 라우팅하는 경우 리소스의 상태를 평가하고 트래픽을 정상인 리소스로만 라우팅하도록 Route 53을 구성할 수 있습니다. 별칭 레코드를 구성하여 리소스의 상태를 확인하는 경우 리소스에 대한 상태 확인을 생성할 필요가 없습니다.

단순 구성에서 Route 53가 리소스의 상태를 확인하도록 구성하는 방법에 대한 개요입니다.

1. Route 53가 모니터링할 리소스를 식별합니다. 예컨대 example.com 대한 요청에 응답하는 HTTP 서버 전체를 모니터링하기 원할 수도 있습니다.
2. 고유 데이터 센터의 EC2 인스턴스 또는 서버와 같은 레코드의 별칭을 생성할 수 없는 리소스의 상태 확인을 생성합니다. 리소스에 상태 확인 요청을 전송하는 방법을 지정합니다. 즉, 사용할 프로토콜(HTTP, HTTPS, 또는 TCP), 사용할 IP 주소 및 포트, 그리고 HTTP/HTTPS 상태 확인을 위한 도메인 이름 및 경로를 알려줍니다.

   > **Note**
   >
   > ELB 로드 밸런서와 같이 별칭 레코드를 생성할 수 있는 리소스를 사용하는 경우 이러한 리소스에 대한 상태 확인을 생성하지 않습니다.

   기본 구성은 각 리소스마다 하나의 상태 확인을 생성하고 리소스마다 상태 확인 엔드포인트를 위한 동일한 IP 주소를 사용하는 것입니다. 상태 확인은 지정된 IP 주소로 요청을 전송합니다.

   > **Note**
   >
   > Route 53는 IP 주소가 로컬, 프라이빗, 라우팅 불가, 또는 멀티캐스트 범위에 있는 리소스의 상태는 확인할 수 없습니다. 상태 확인을 생성할 수 없는 IP 주소에 대한 자세한 내용은 RFC 5735, Special Use IPv4 Addresses와 RFC 6598, IANA-Reserved IPv4 Prefix for Shared Address Space를 참조하십시오.

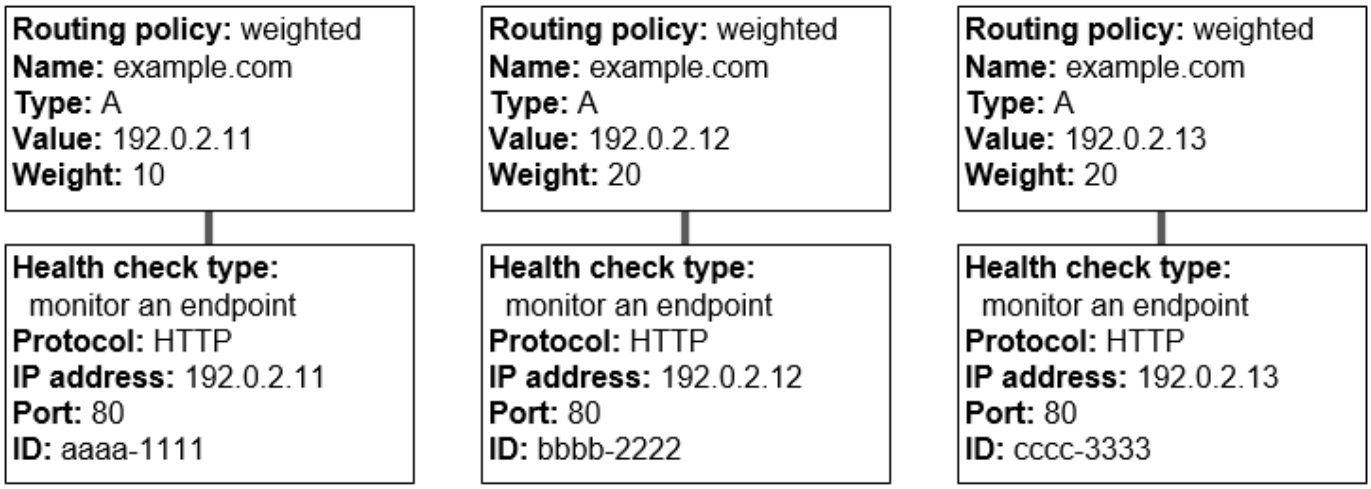
   상태 확인 생성에 대한 자세한 내용은 상태 확인의 생성, 업데이트 및 삭제 단원을 참조하십시오.
3. 상태 확인에서 지정한 엔드포인트에 대해 Route 53가 규칙적으로 요청을 전송할 수 있도록 하기 위해서는 라우터 및 방화벽 규칙을 구성할 필요가 있을 수 있습니다. 자세한 내용은 Amazon Route 53 상태 확인을 위한 라우터 및 방화벽 규칙 구성 섹션을 참조하세요.

4. 리소스(예: 가중치 기반 레코드 그룹)에 대한 레코드 그룹을 생성합니다. 별칭 및 비 별칭 레코드를 조합할 수 있습니다. 하지만 모두 동일한 [Name], [Type] 및 [Routing Policy] 값을 보유해야 합니다.

   Route 53가 리소스의 상태를 확인하도록 구성하는 방법은 별칭 레코드 또는 비 별칭 레코드 생성 여부에 따라 다릅니다.

   - 별칭 레코드(Alias records) - 대상 상태 평가(Evaluate Target Health)를 예(Yes)로 지정합니다.
   - 비 별칭 레코드(Non-alias records) - 2단계에서 생성한 상태 확인을 해당 레코드와 연결합니다.

   완료되면 구성은 다음 다이어그램과 비슷해지며, 비 별칭 레코드만을 포함합니다.



   Route 53 콘솔을 사용하여 레코드를 생성하는 방법에 대한 자세한 내용은 Amazon Route 53 콘솔을 사용하여 레코드 생성 섹션을 참조하세요.

5. 상태 확인을 생성한 경우 Route 53는 각 상태 확인 시 엔드포인트로 요청을 주기적으로 전송하지만, DNS 쿼리를 수신할 때는 상태 확인을 수행하지 않습니다. Route 53는 응답을 근거로 엔드포인트가 정상인지 판단하고 그 정보를 이용하여 어떻게 쿼리에 응답할 것인지 결정합니다. 자세한 내용은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 섹션을 참조하세요.

   Route 53는 example.com의 A 레코드에서 지정된 IP 주소와 같이 레코드에 지정된 리소스의 상태를 확인하지 않습니다. 상태 확인을 레코드와 연결하면 Route 53는 상태 확인에서 지정한 엔드포인트의 상태를 확인하기 시작합니다. 또한 Route 53가 다른 상태 확인의 상태 또는 CloudWatch 경보의 데이터 스트림을 모니터링하도록 구성할 수도 있습니다. 자세한 내용은 Amazon Route 53 상태 확인 유형 섹션을 참조하세요.

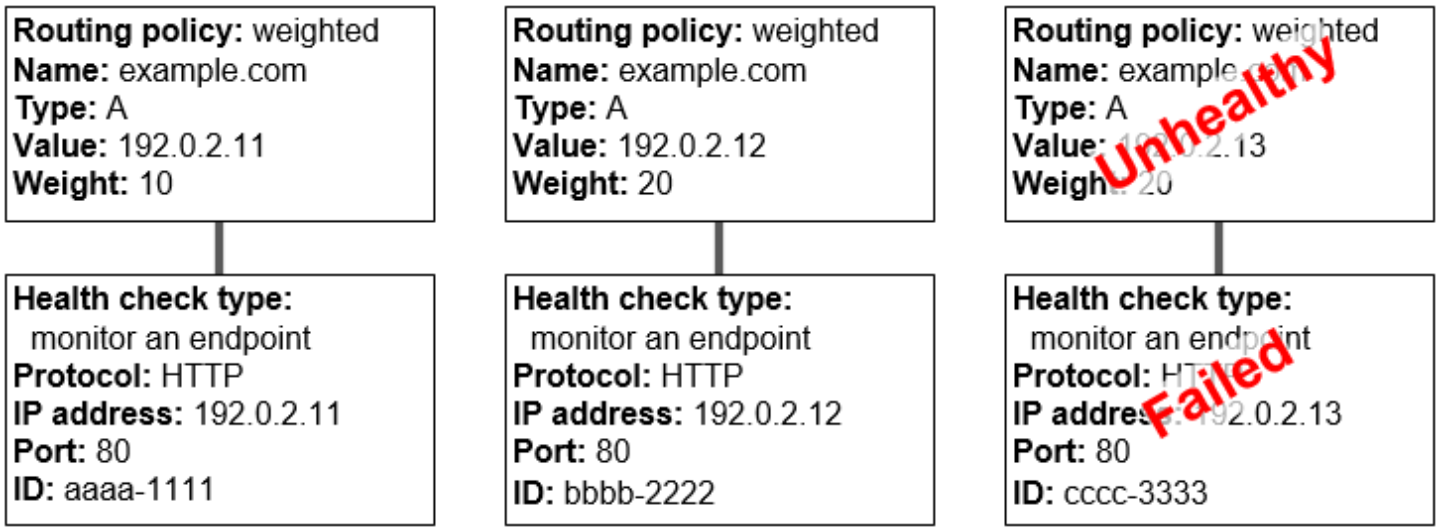
Route 53가 example.com에 대한 쿼리를 수신할 때 다음 현상이 발생합니다.

1. Route 53는 라우팅 정책을 기반으로 레코드를 선택합니다. 이 경우에는 가중치를 기반으로 레코드를 선택합니다.
2. 선택한 레코드에 대한 상태 확인의 상태를 확인하여 해당 레코드의 현재 상태를 판단합니다.
3. 선택한 레코드가 비정상인 경우 Route 53는 다른 레코드를 선택합니다. 이 경우 비정상적인 레코드는 고려 대상이 아닙니다.

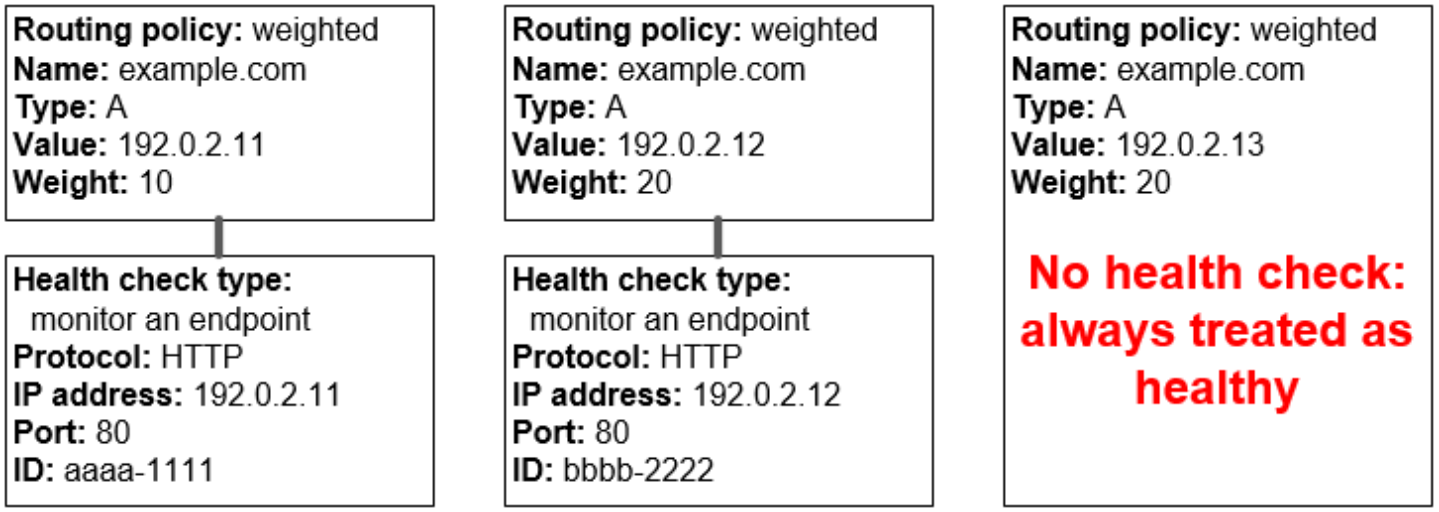
   자세한 내용은 상태 확인 구성 시 Amazon Route 53의 레코드 선택 방식 섹션을 참조하세요.
4. Route 53가 정상인 레코드를 찾으면 A 레코드의 IP 주소와 같이 해당되는 값으로 쿼리에 응답합니다.

다음 예제에서는 세 번째 레코드가 비정상적인 가중치 기반 레코드의 그룹을 보여 줍니다. 처음에 Route 53는 3개의 레코드 전체의 가중치를 기반으로 레코드를 선택합니다. 처음에 비정상적인 레코드를 선택하는 일이 발생하면 Route 53는 다른 레코드를 선택하지만 이번에는 세 번째 레코드의 가중치를 계산에서 제외합니다.

- Route 53가 처음에 3개의 레코드 전체 중에서 선택할 때는 10/(10 + 20 + 20)이라는 시간의 약 20% 동안만 최초 레코드를 사용하여 요청에 응답합니다.
- 이 세 번째 레코드가 비정상이라고 판단할 때는 10/(10 + 20)이라는 시간의 약 33% 동안만 최초 레코드를 사용하여 요청에 응답합니다.



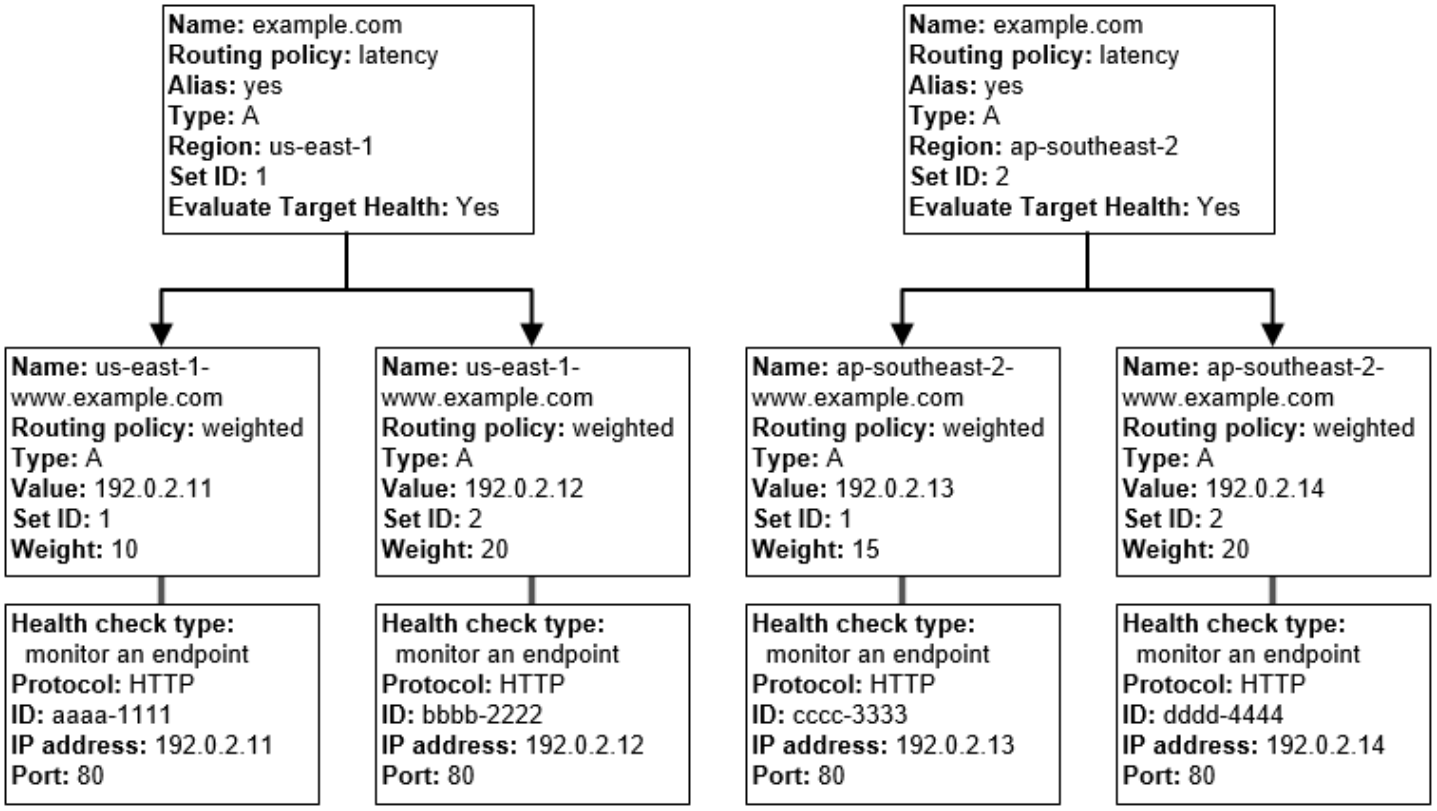
레코드 그룹에서 1개 이상의 레코드에 대한 상태 확인을 생략한 경우 Route 53가 해당 리소스의 상태를 확인할 방법이 없습니다. Route 53에서는 해당 레코드를 정상으로 취급합니다



상태 확인이 복잡한 Amazon Route 53 구성에서 작동하는 방식

복잡한 구성에서 리소스의 상태를 확인하는 것은 단순한 구성에 이루어지는 방식과 상당 부분 같습니다. 그러나 복잡한 구성에서는 별칭 레코드(가중치 기반 별칭, 장애 조치 별칭 등)와 비 별칭 레코드의 조합을 사용하여 Route 53가 요청에 응답하는 방식을 더 잘 제어할 수 있게 해주는 판단 트리를 구축합니다.

예를 들어 지연 시간 별칭 레코드를 사용하여 사용자에게 가까운 리전을 선택하고 각 리전 내의 둘 이상의 리소스에 대한 가중치 기반 레코드를 사용하여 단일 엔드포인트 또는 가용 영역의 실패를 방지할 수 있습니다. 다음 다이어그램은 이 구성을 보여줍니다.



Amazon EC2 및 Route 53가 구성되는 방법은 다음과 같습니다. 트리의 하단에서 시작합니다. 레코드를 생성하는 순서이기 때문입니다.

- us-east-1 및 ap-southeast-2의 두 리전 각각에서 2개의 EC2 인스턴스를 갖습니다. Route 53가 정상 여부를 기반으로 EC2 인스턴스로 트래픽을 라우팅하고자 하는 경우 각 인스턴스에 대해 상태 확인을 생성합니다. 각 상태 확인을 구성하여 상태 확인 요청을 해당 인스턴스의 탄력적 IP 주소에 있는 해당 인스턴스로 전송합니다.

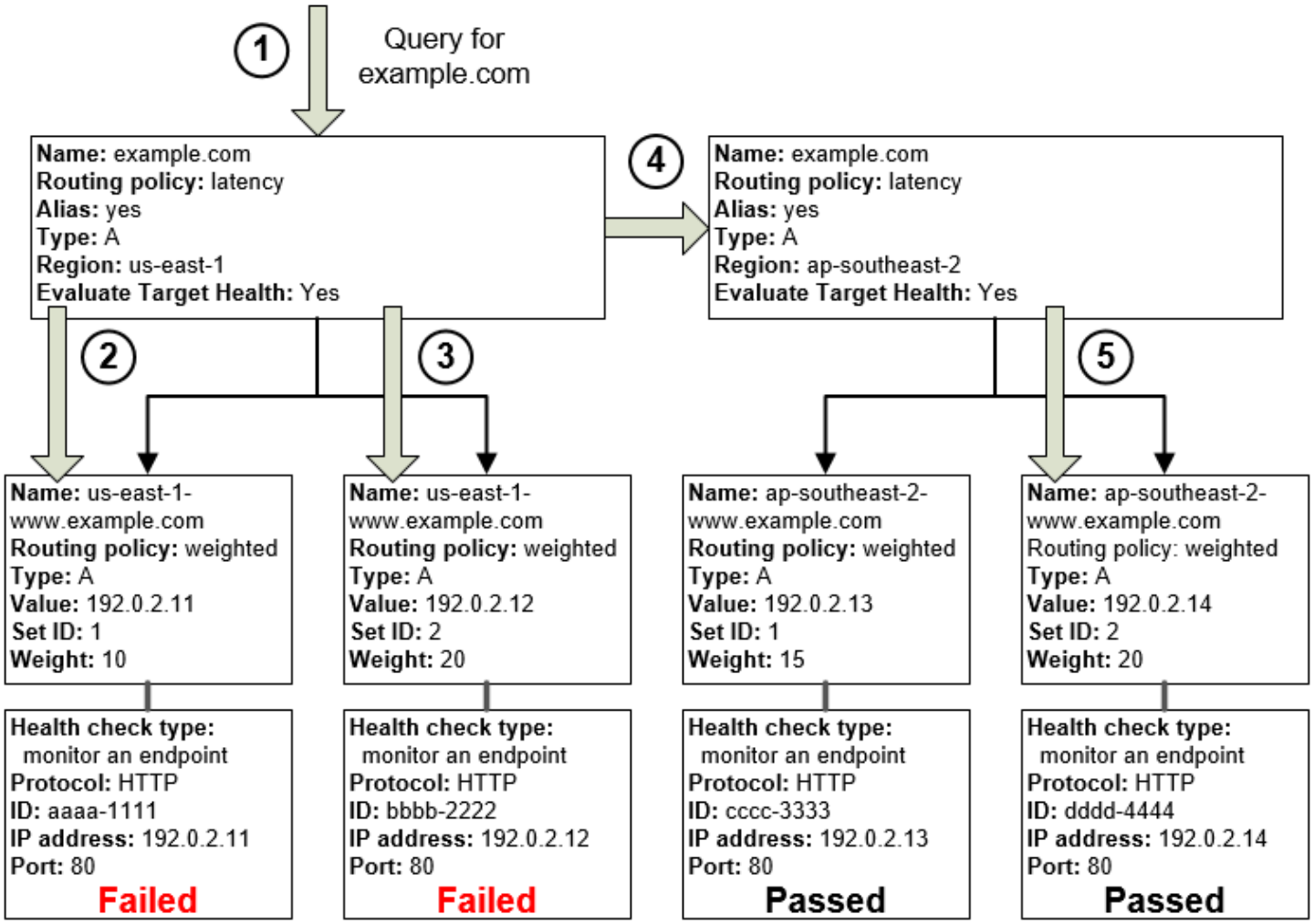
  Route 53는 전역 서비스이므로 상태 확인을 생성하고자 하는 리전을 지정하지 않습니다.
- 인스턴스 유형을 기반으로 각 리전에 있는 2개의 인스턴스로 트래픽을 라우팅하고자 하는 경우 각 인스턴스에 대한 가중치 기반 레코드를 생성하고 각 레코드에 가중치를 부여합니다. (이후 가중치를 변경하여 인스턴스로의 트래픽 라우팅을 늘리거나 줄일 수 있습니다.) 또한 해당 상태 확인을 각 인스턴스와 연결합니다.

  레코드를 생성할 때 us-east-1-www.example.com 및 ap-southeast-2-www.example.com과 같은 이름을 사용합니다. 레코드에 사용자가 웹 사이트 또는 웹 애플리케이션에 액세스하는 데 사용하는 이름(예: example.com)을 지정하려면 트리 상단으로 이동할 때까지 기다립니다.
- 사용자에 대해 가장 낮은 지연 시간을 제공하는 리전으로 트래픽을 라우팅하고자 하는 경우 트리 상단에서 레코드에 대한 지연 시간 라우팅 정책을 선택합니다.

직접 각 리전의 리소스가 아니라 각 리전의 레코드로 트래픽을 라우팅하고자 합니다(이미 가중치 기반 레코드가 이를 수행하고 있음). 그 결과 지연 시간 별칭 레코드를 생성합니다.

별칭 레코드를 생성할 때 사용자가 웹 사이트 또는 웹 애플리케이션에 액세스하는 데 사용하는 이름(예: example.com)을 지정합니다. 별칭 레코드는 example.com에 대한 트래픽을 us-east-1-www.example.com 및 ap-southeast-2-www.example.com 레코드로 라우팅합니다.

지연 시간 별칭 레코드 모두에 대해 [Evaluate Target Health]의 값을 [Yes]로 설정합니다. 이렇게 하면 Route 53는 트래픽 라우팅을 시도하기 전에 리전에 정상 리소스가 있는지 여부를 확인합니다. 정상 리소스가 없는 경우 Route 53는 다른 리전의 정상 리소스를 선택합니다.



앞의 다이어그램에서는 이벤트들의 순서를 다음과 같이 보여줍니다.

1. Route 53는 example.com에 대한 쿼리를 수신합니다. Route 53는 요청을 보내는 사용자의 지연 시간을 기반으로 us-east-1 리전에 대한 지연 시간 별칭 레코드를 선택합니다.
2. Route 53는 가중치를 기반으로 가중치 기반 레코드를 선택합니다. 대상 상태 평가(Evaluate Target Health)는 지연 시간 별칭 레코드에 대해 예(Yes)이므로 Route 53는 선택한 가중치 기반 레코드의 상태를 확인합니다.
3. 상태 확인이 실패했으므로 Route 53는 가중치를 기반으로 다른 가중치 기반 레코드를 선택하여 그 상태를 확인합니다. 해당 레코드 역시 비정상입니다.
4. Route 53는 트리의 가지를 포기하고 차선의 지연 시간을 지닌 지연 시간 별칭 레코드를 찾아 ap-southeast-2에 대한 레코드를 선택합니다.
5. Route 53는 다시 가중치를 기반으로 레코드를 선택한 다음 선택한 리소스의 상태를 확인합니다. 리소스가 정상이므로 Route 53는 쿼리에 응답해 해당하는 값을 반환합니다.

주제

상태 확인을 별칭 레코드와 연결하면 어떻게 됩니까?

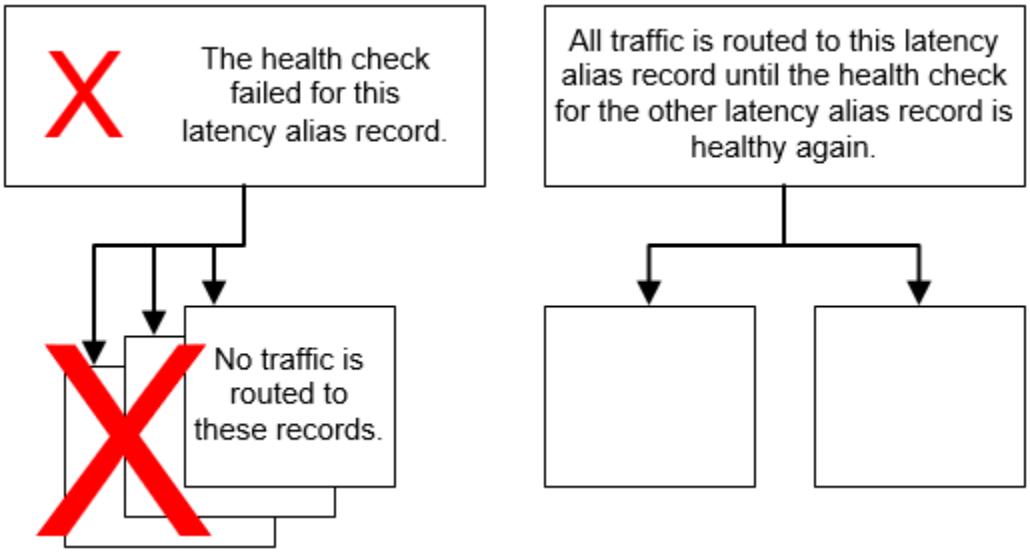
[Evaluate Target Health]의 값을 [Yes]로 설정하는 작업 대신 또는 이 작업 외에 상태 확인을 별칭 레코드와 연결할 수 있습니다. 그러나 Route 53가 기본 리소스(별칭 레코드가 참조하는 HTTP 서버, 데이터베이스 서버, 및 기타 리소스)의 상태에 따라 쿼리에 반응한다면 대개의 경우 더 유용합니다. 예를 들어, 다음과 같은 구성을 가정해 봅시다.

- 별칭 대상이 가중치 기반 레코드의 그룹인 지연 시간 별칭 레코드에 상태 확인을 할당합니다.
- 지연 시간 별칭 레코드에 대해 [Evaluate Target Health]의 값을 [Yes]로 설정합니다.

이 구성에서는 Route 53가 가중치 기반 레코드에 해당하는 값을 반환하기 전에 다음 두 가지가 모두 참이어야 합니다.

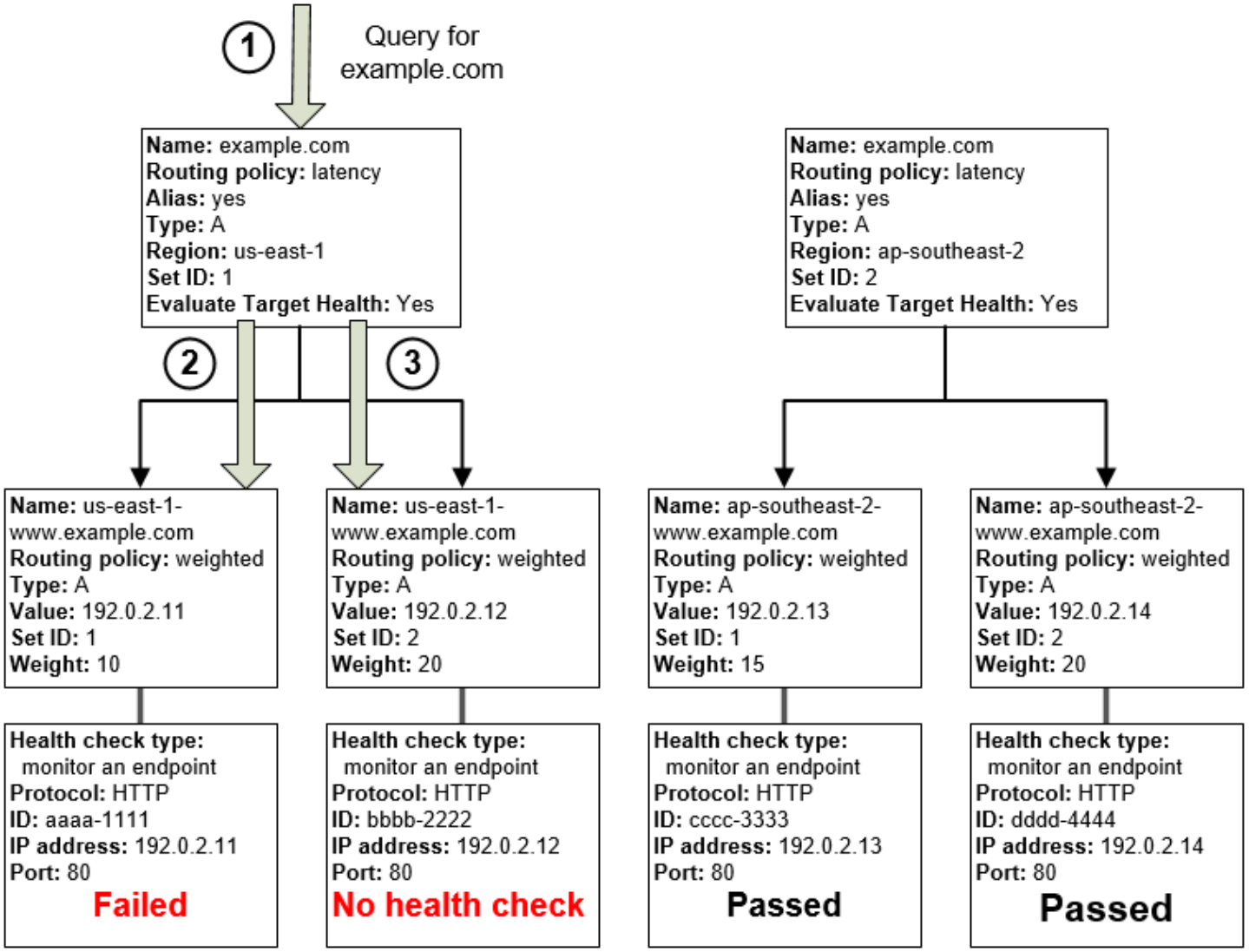
- 지연 시간 별칭 레코드와 연결된 상태 확인이 통과되어야 합니다.
- 통과하는 상태 확인과 연결되어 있거나 상태 확인과 연결되어 있지 않기 때문에 한 개 이상의 가중치 기반 레코드가 정상 상태로 간주되어야 합니다. 후자의 경우 Route 53는 항상 가중치 기반 레코드를 정상 상태로 간주합니다.

다음 그림에서 왼쪽 상단에 있는 지연 시간 별칭 레코드에 대한 상태 확인이 실패했습니다. 그 결과 Route 53는 가중치 기반 레코드가 모두 정상인 경우에도 지연 시간 별칭 레코드가 참조하는 가중치 기반 레코드를 사용하여 쿼리에 응답하는 것을 중단합니다. Route 53는 지연 시간 별칭 레코드에 대한 상태 확인이 다시 정상인 경우에만 이러한 가중치 기반 레코드를 다시 고려하기 시작합니다. (예외 사항은 상태 확인 구성 시 Amazon Route 53의 레코드 선택 방식 단원을 참조하십시오.)



상태 확인을 생략하면 어떻게 됩니까?

복잡한 구성에서는 상태 확인을 비 별칭 레코드 전체에 연결하는 것이 중요합니다. 다음 예제에서 us-east-1 리전에서 가중치 기반 레코드 중 하나에 대한 상태 확인이 누락되었습니다.



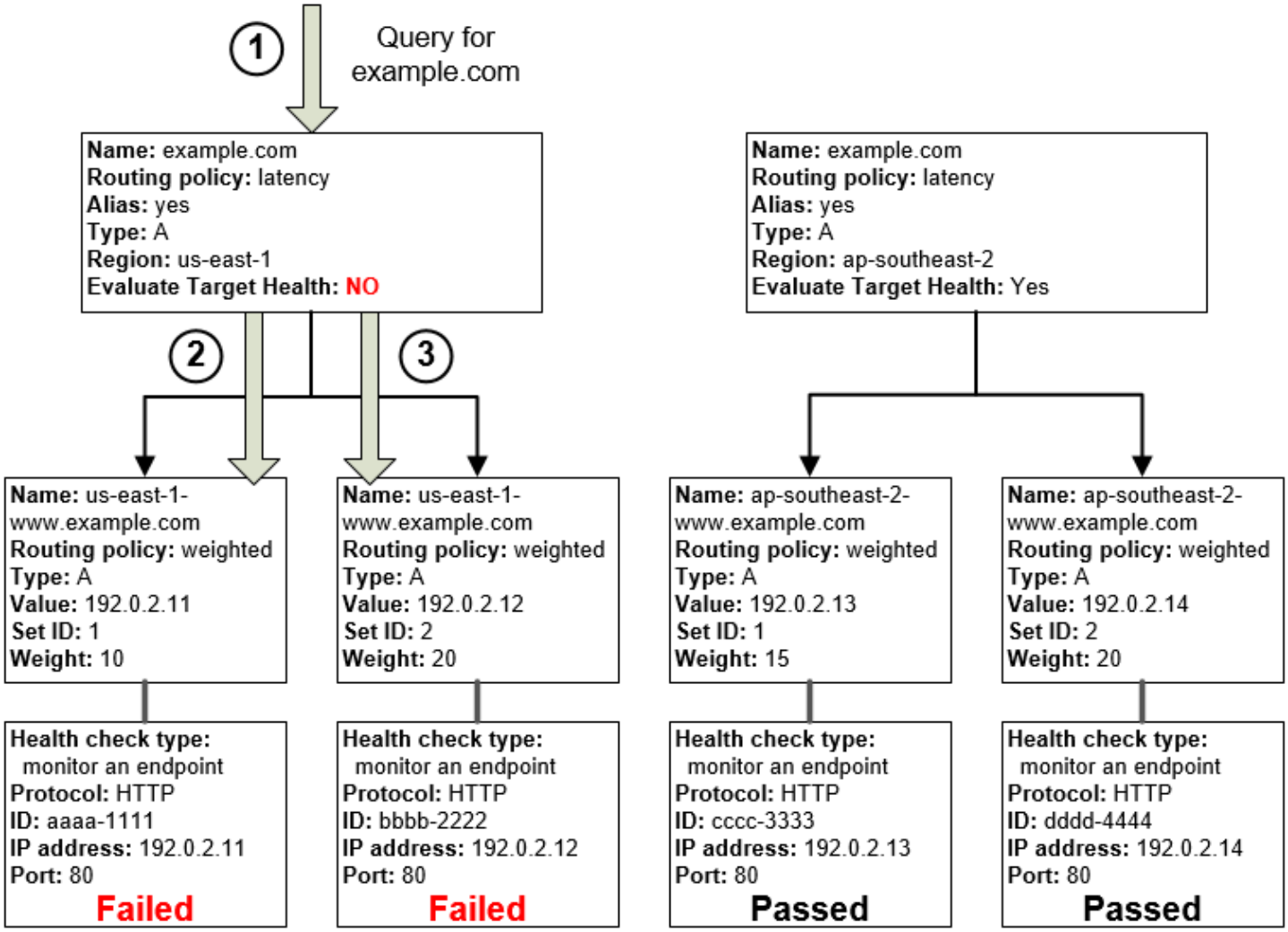
이 구성에서 비 별칭 레코드에 대한 상태 확인을 생략할 때 발생하는 일은 다음과 같습니다.

1. Route 53는 example.com에 대한 쿼리를 수신합니다. Route 53는 요청을 보내는 사용자의 지연 시간을 기반으로 us-east-1 리전에 대한 지연 시간 별칭 레코드를 선택합니다.
2. Route 53는 지연 시간 별칭 레코드에 대한 별칭 대상을 찾아서 해당 상태 확인의 상태를 확인합니다. 한 개의 가중치 기반 레코드에 대한 상태 확인이 실패했으므로 레코드는 고려 대상에서 생략됩니다.
3. us-east-1 리전에 대한 별칭 대상에서 기타 가중치 기반 레코드에는 상태 확인이 없습니다. 해당 리소스는 정상이거나 비정상이겠지만, 상태 확인이 없으면 Route 53는 알 방법이 없습니다. 리소스가 정상으로 가정하여 Route 53는 쿼리에 응답해 해당하는 값을 반환합니다.

[Evaluate Target Health]를 [No]로 설정하면 어떻게 됩니까?

일반적으로 트리의 모든 별칭 레코드에 대해 [Evaluate Target Health]를 [Yes]로 설정해야 합니다. 대상 상태 평가(Evaluate Target Health)를 아니요(No)로 설정한 경우 레코드에 대한 상태 확인이 실패하는 경우에도 Route 53는 계속해서 별칭 레코드가 참조하는 레코드로 트래픽을 라우팅합니다.

다음 예제에서는 가중치 기반 레코드 전체가 상태 확인과 연결되었지만 us-east-1 리전의 지연 시간 별칭 레코드에 대해 [Evaluate Target Health]가 [No]로 설정되어 있습니다.



이 구성에서 별칭 레코드에 대해 [Evaluate Target Health]를 [No]로 설정할 때 발생하는 일은 다음과 같습니다.

1. Route 53는 example.com에 대한 쿼리를 수신합니다. Route 53는 요청을 보내는 사용자의 지연 시간을 기반으로 us-east-1 리전에 대한 지연 시간 별칭 레코드를 선택합니다.
2. Route 53는 지연 시간 별칭 레코드에 대한 별칭 대상이 무엇인지 판단하여 해당 상태 확인을 확인합니다. 둘 다 실패합니다.

3. us-east-1 리전의 지연 시간 별칭 레코드에 대해 대상 상태 평가(Evaluate Target Health)의 값이 아니요(No)로 설정되어 있으므로 Route 53는 가지를 포기하고 ap-southeast-2 리전의 정상적인 레코드를 찾는 대신 이 가지에서 하나의 레코드를 선택해야 합니다.

상태 확인 구성 시 Amazon Route 53의 레코드 선택 방식

동일한 이름, 동일한 유형(예: A 또는 AAAA) 및 동일한 라우팅 정책(예: 가중치 또는 장애 조치)을 보유한 레코드 그룹의 모든 레코드에 대한 상태 확인을 구성한 경우 Route 53는 정상 레코드를 선택하고 해당 레코드로부터 해당되는 값을 반환함으로써 DNS 쿼리에 응답합니다.

예를 들어, 3개의 가중치 A 레코드를 생성하고 세 레코드 모두에 상태 확인을 할당한다고 가정합니다. 한 레코드의 상태 확인이 비정상인 경우 Route 53는 다른 2개 레코드의 IP 주소를 통해 DNS 쿼리에 응답합니다.

다음은 Route 53가 정상적인 레코드를 선택하는 방식입니다.

1. Route 53는 처음에 라우팅 정책과 각 레코드에 대해 지정한 값을 기반으로 레코드를 선택합니다. 예를 들어, 가중치 레코드의 경우 Route 53는 각 레코드에 대해 지정한 가중치를 기반으로 레코드를 선택합니다.
2. Route 53가 레코드가 정상이라 확인한 경우:
   - 상태 확인이 연결된 비 별칭 레코드 - 상태 확인과 비 별칭 레코드를 연결한 경우 Route 53는 상태 확인의 현재 상태를 확인합니다.

     Route 53는 상태 확인에 지정된 엔드포인트의 상태를 주기적으로 점검하는데, DNS 쿼리가 도착할 때는 상태 확인을 수행하지 않습니다.

     상태 확인과 별칭 레코드를 연결할 수 있지만 상태 확인과 비 별칭 레코드만을 연결하는 것이 좋습니다. 자세한 내용은 상태 확인을 별칭 레코드와 연결하면 어떻게 됩니까? 섹션을 참조하세요.
   - 대상 상태 평가가 예로 설정된 별칭 레코드 - Route 53는 ELB 로드 밸런서 또는 동일한 호스팅 영역의 또 다른 레코드와 같이 별칭 레코드가 참조하는 리소스의 상태를 확인합니다.
3. 레코드가 정상인 경우 Route 53는 IP 주소와 같이 해당되는 값으로 쿼리에 응답합니다.

   레코드가 비정상인 경우 Route 53는 동일한 기준을 사용하여 또 다른 레코드를 선택하고 정상 레코드를 찾을 때까지 프로세스를 반복합니다.

Route 53는 레코드 선택 시 다음 기준을 사용합니다.

항상 정상인 상태 확인이 없는 레코드

동일한 이름과 유형을 보유한 레코드 그룹의 레코드에 연결된 상태 확인이 없는 경우 Route 53는 항상 이를 정상으로 여기고 쿼리에 대한 가능한 응답에 항상 이를 포함시킵니다.

정상인 레코드가 없는 경우 모두 레코드가 정상임

레코드 그룹의 레코드가 정상이 아닌 경우 Route 53는 DNS 쿼리에 대한 응답으로 무언가를 반환해야 하지만 한 레코드에 견주어 다른 레코드를 선택할 근거가 없습니다. 이런 상황에서 Route 53는 그룹의 레코드 전체를 정상으로 간주하고 라우팅 정책과 각 레코드에 지정한 값을 기반으로 하나의 레코드를 선택합니다.

가중치가 0인 가중치 기반 레코드

가중치 기반 레코드의 그룹에서 레코드 전체에 상태 확인을 추가하지만 어떤 레코드에는 0이 아닌 가중치를 부여하고 또 다른 레코드에는 0인 가중치를 부여하는 경우 상태 확인은 모든 레코드의 가중치가 0일 때와 동일하게 작업합니다. 단, 다음 경우는 예외입니다.

- Route 53는 처음에 0이 아닌 가중치 기반 레코드만을 고려합니다(해당되는 경우).
- 0보다 큰 가중치를 지닌 레코드 전체가 비정상인 경우 Route 53는 0인 가중치 기반 레코드를 고려합니다.

Route 53은 상황에 따라 가중치가 0인 레코드를 고려하므로 가중치가 0인 대상에도 DNS 쿼리에 대한 실행 가능한 응답이 있는지 확인하는 것이 중요합니다.

가중치 기반 레코드에 대한 자세한 내용은 상태 확인 및 가중치 기반 라우팅을 참조하십시오.

별칭 레코드

각 별칭 레코드에 대해 [Evaluate Target Health]를 [Yes]로 설정함으로써 별칭 레코드에 대한 상태 확인을 구성할 수도 있습니다. 이로 인해 Route 53는 ELB 로드 밸런서 또는 동일한 호스팅 영역의 또 다른 레코드와 같이 레코드가 트래픽을 라우팅하는 리소스의 상태를 확인합니다.

예를 들어, 별칭 레코드에 대한 별칭 대상이 0이 아닌 가중치를 모두 지닌 가중치 기반 레코드의 그룹인 경우를 가정해 봅시다.

- 하나 이상의 가중치 기반 레코드가 정상인 경우 Route 53는 별칭 레코드를 정상 상태로 간주합니다.
- 가중치 기반 레코드가 정상이 아닌 경우 Route 53는 별칭 레코드를 비정상 상태로 간주합니다.
- Route 53는 하나 이상의 가중치 기반 레코드가 다시 정상이 될 때까지 트리의 가지에 있는 레코드에 대한 판단을 중지합니다.

자세한 내용은 상태 확인이 복잡한 Amazon Route 53 구성에서 작동하는 방식 섹션을 참조하세요.

장애 조치 레코드

장애 조치 레코드는 일반적으로 다른 라우팅 유형과 동일한 방식으로 작동합니다. 상태 확인을 생성하고 이를 비 별칭 레코드와 연결한 다음 별칭 레코드에 대해 [Evaluate Target Health]를 [Yes]로 설정합니다. 다음 사항에 유의하세요.

- 기본 및 보조 레코드는 모두 비 별칭 레코드 또는 별칭 레코드일 수 있습니다.
- 기본 및 보조 장애 조치 레코드와 상태 확인을 연결하는 경우 Route 53가 요청에 응답하는 방식은 다음과 같습니다.
  - Route 53가 기본 레코드를 정상 상태로 간주하는 경우(상태 확인 엔드포인트가 정상인 경우) Route 53는 DNS 쿼리에 대한 응답으로 기본 레코드만 반환합니다.
  - Route 53가 기본 레코드를 비정상 상태로 간주하고 보조 레코드를 정상 상태로 간주하는 경우 Route 53는 그 대신에 보조 레코드를 반환합니다.
  - Route 53가 기본 및 보조 레코드를 모두 비정상 상태로 간주하는 경우 Route 53는 기본 레코드를 반환합니다.
- 보조 레코드를 구성할 때 상태 확인 추가는 선택 사항입니다. 보조 레코드에 대한 상태 확인을 생략하고 기본 레코드에 대한 상태 확인 엔드포인트가 비정상인 경우 Route 53는 항상 보조 레코드를 사용하여 DNS 쿼리에 응답합니다. 이는 보조 레코드가 비정상인 경우라 할지라도 그대로 적용됩니다.

자세한 정보는 다음의 주제를 참조하세요.

- 하나의 기본 및 보조 리소스를 사용한 액티브-패시브 장애 조치 구성
- 여러 개의 기본 및 보조 리소스를 사용한 액티브-패시브 장애 조치 구성

액티브-액티브 및 액티브-패시브 장애 조치

Route 53 상태 확인을 사용하여 액티브-액티브 및 액티브-패시브 장애 조치 구성을 구성할 수 있습니다. 장애 조치를 제외한 모든 라우팅 정책(또는 라우팅 정책의 조합)을 사용하여 액티브-액티브 장애 조치를 구성하고, 장애 조치 라우팅 정책을 사용하여 액티브-패시브 장애 조치를 구성합니다.

주제

- 액티브-액티브 장애 조치
- 액티브-패시브 장애 조치

액티브-액티브 장애 조치

모든 리소스를 대부분의 시간 동안 사용 가능하도록 하려면 이 장애 조치 구성을 사용하십시오. 리소스를 사용할 수 없는 경우 Route 53가 비정상 상태임을 판별하여 쿼리에 응답할 때 해당 리소스를 포함하지 않습니다.

액티브-액티브 장애 조치에서 동일한 이름, 동일한 유형(예: A 또는 AAAA) 및 동일한 라우팅 정책(예: 가중치 또는 지연 시간)을 보유한 모든 레코드는 Route 53가 이를 비정상으로 간주하지 않는 이상 활성 상태입니다. Route 53는 정상 레코드를 사용하여 DNS 쿼리에 응답할 수 있습니다.

액티브-패시브 장애 조치

기본 리소스 또는 리소스 그룹이 대부분의 시간 동안 사용 가능하도록 하고 보조 리소스 또는 리소스 그룹은 기본 리소스가 사용 불가능할 경우를 대비해 대기 중에 있도록 하고 싶다면 이 장애 조치 구성을 사용하십시오. 쿼리에 응답할 때 Route 53는 정상적인 기본 리소스만을 포함합니다. 모든 기본 리소스가 비정상인 경우 Route 53는 DNS 쿼리에 응답할 때 정상적인 보조 리소스만을 포함시키기 시작합니다.

주제

- 하나의 기본 및 보조 리소스를 사용한 액티브-패시브 장애 조치 구성
- 여러 개의 기본 및 보조 리소스를 사용한 액티브-패시브 장애 조치 구성
- 가중치 레코드를 사용하여 액티브-패시브 장애 조치 구성

하나의 기본 및 보조 리소스를 사용한 액티브-패시브 장애 조치 구성

하나의 기본 레코드 및 보조 레코드를 사용하여 액티브-패시브 장애 조치를 생성하려면 레코드를 생성하고 라우팅 정책을 장애 조치로 지정합니다. 기본 리소스가 정상일 때 Route 53는 기본 레코드를 사용하여 DNS 쿼리에 응답합니다. 기본 리소스가 비정상일 때 Route 53는 보조 레코드를 사용하여 DNS 쿼리에 응답합니다.

여러 개의 기본 및 보조 리소스를 사용한 액티브-패시브 장애 조치 구성

여러 개의 리소스를 기본 레코드, 보조 레코드 또는 둘 모두에 연결할 수 있습니다. 이 구성에서 Route 53는 연결된 리소스 중 최소 하나가 정상인 한 기본 장애 조치 레코드를 정상으로 간주합니다. 자세한 내용은 상태 확인 구성 시 Amazon Route 53의 레코드 선택 방식 섹션을 참조하세요.

기본 또는 보조 레코드에 대해 여러 리소스를 사용하여 액티브-패시브 장애 조치를 구성하려면 다음 작업을 수행합니다.

1. 데이터 센터의 EC2 인스턴스 또는 웹 서버와 같이 트래픽을 라우팅하고자 하는 각 리소스에 대한 상태 확인을 생성합니다.

   > **Note**
   >
   > 별칭 레코드를 생성할 수 있는 AWS 리소스로 트래픽을 라우팅하는 경우 해당 리소스에 대한 상태 확인을 생성하지 마십시오. 별칭 레코드를 생성할 때 대신 [Evaluate Target Health]의 값을 [Yes]로 설정합니다.

   자세한 내용은 상태 확인의 생성 및 업데이트 섹션을 참조하세요.

2. 기본 리소스에 대한 레코드를 생성하고 다음 값을 지정합니다.

   - 각 레코드에 동일한 이름, 유형 및 라우팅 정책을 제공합니다. 예를 들어, 이름이 모두 failover-primary.example.com인 3개의 가중치 A 레코드를 생성할 수 있습니다.
   - 별칭 레코드를 생성할 수 있는 AWS 리소스를 사용하는 경우 대상 상태 평가에 예를 지정합니다.

     별칭 레코드를 생성할 수 없는 리소스를 사용하는 경우 1단계의 해당 상태 확인을 각 레코드와 연결합니다.

   자세한 내용은 Amazon Route 53 콘솔을 사용하여 레코드 생성 섹션을 참조하세요.

3. 보조 리소스에 대한 레코드를 생성하고 해당되는 경우 다음 값을 지정합니다.

   - 각 레코드에 동일한 이름, 유형 및 라우팅 정책을 제공합니다. 예를 들어, 이름이 모두 failover-secondary.example.com인 3개의 가중치 A 레코드를 생성할 수 있습니다.
   - 별칭 레코드를 생성할 수 있는 AWS 리소스를 사용하는 경우 대상 상태 평가에 예를 지정합니다.

     별칭 레코드를 생성할 수 없는 리소스를 사용하는 경우 1단계의 해당 상태 확인을 각 레코드와 연결합니다.

   > **Note**
   >
   > 일부 고객은 웹 서버를 기본 리소스로 사용하고 웹 사이트 엔드포인트로 구성된 Amazon S3 버킷을 보조 리소스로 사용합니다. S3 버킷에는 단순한 "temporarily unavailable" 메시지가 포함됩니다. 해당 구성을 사용하는 경우 이 단계를 건너뛰고 4단계의 보조 리소스에 대한 장애 조치 별칭 레코드를 생성합니다.

4. 2개의 장애 조치 별칭 레코드(하나는 기본, 다른 하나는 보조)를 생성하고 다음 값을 지정합니다.

기본 레코드

- 이름(Name) - Route 53가 트래픽을 라우팅하고자 하는 도메인 이름(example.com) 또는 하위 도메인 이름(www.example.com)을 지정합니다.
- 별칭(Alias) - 예(Yes)로 지정합니다.
- 별칭 대상(Alias Target) - 2단계에서 생성한 레코드의 이름을 지정합니다.
- 라우팅 정책(Routing Policy) - 장애 조치(Failover)를 지정합니다.
- 장애 조치 레코드 유형(Failover Record Type) - 기본(Primary)을 지정합니다.
- 대상 상태 평가(Evaluate Target Health) - 예(Yes)를 지정합니다.
- 상태 확인과 연결(Associate with Health Check) - 아니요(No)를 지정합니다.

보조 레코드

- 이름(Name) - 기본 레코드에 대해 지정한 것과 동일한 이름을 지정합니다.
- 별칭(Alias) - 예(Yes)로 지정합니다.
- 별칭 대상(Alias Target) - 3단계에서 보조 리소스에 대한 레코드를 생성한 경우 해당 레코드의 이름을 지정합니다. 보조 리소스에 대해 Amazon S3 버킷을 사용하는 경우 웹 사이트 엔드포인트의 DNS 이름을 지정합니다.
- 라우팅 정책(Routing Policy) - 장애 조치(Failover)를 지정합니다.
- 장애 조치 레코드 유형(Failover Record Type) - 보조(Secondary)를 지정합니다.
- 대상 상태 평가(Evaluate Target Health) - 예(Yes)를 지정합니다.
- 상태 확인과 연결(Associate with Health Check) - 아니요(No)를 지정합니다.

가중치 레코드를 사용하여 액티브-패시브 장애 조치 구성

경고를 포함하여 액티브-패시브 장애 조치에 대한 가중치 기반 레코드를 사용할 수도 있습니다. 일부 레코드에 대해 0이 아닌 가중치를 지정하고, 나머지 레코드에 대해 0의 가중치를 지정한 경우 Route 53는 0이 아닌 가중치를 가진 정상 레코드만을 사용하여 DNS 쿼리에 응답합니다. 0보다 큰 가중치를 지닌 레코드 전체가 비정상인 경우 Route 53는 가중치가 0인 레코드를 사용하여 쿼리에 응답합니다.

> **Note**
>
> Route 53가 가중치가 0인 레코드를 사용하여 DNS 쿼리에 응답하기 전에 가중치가 0이 아닌 모든 레코드가 비정상이어야 합니다. 다른 리소스를 사용할 수 없을 때 웹 서버와 같은 마지막

정상 리소스가 모든 트래픽을 처리할 수 없는 경우 이로 인해 웹 애플리케이션 또는 웹 사이트가 불안정하게 될 수 있습니다.

프라이빗 호스팅 영역에서 장애 조치 구성

프라이빗 호스팅 영역에서 장애 조치 레코드를 생성하는 경우 다음에 유의하십시오.

- Route 53 상태 확인은 VPC 외부에 있습니다. IP 주소별로 VPC 내에 있는 엔드포인트의 상태를 확인하려면 VPC의 인스턴스에 퍼블릭 IP 주소를 할당해야 합니다.
- CloudWatch 지표를 생성하고 경보를 지표와 연결한 다음 경보의 데이터 스트림을 기반으로 하는 상태 확인을 생성할 수 있습니다. 예를 들어, EC2 `StatusCheckFailed` 지표의 상태를 확인하는 CloudWatch 지표를 생성하고 경보를 지표에 추가한 다음 경보의 데이터 스트림을 기반으로 하는 상태 확인을 생성하여 프라이빗 IP 주소만 가지는 Virtual Private Cloud(VPC) 내의 인스턴스를 확인할 수 있습니다. CloudWatch 콘솔을 사용한 CloudWatch 지표 및 경보 생성에 대한 정보는 Amazon CloudWatch 사용 설명서를 참조하십시오.

자세한 내용은 프라이빗 호스팅 영역 사용 및 CloudWatch를 이용한 상태 확인 모니터링 단원을 참조하세요.

Amazon Route 53가 장애 조치 문제를 방지하는 방법

Route 53가 실행하는 장애 조치 알고리즘은 트래픽을 정상적인 엔드포인트로 라우팅할 뿐만 아니라 상태 확인 및 애플리케이션의 구성 오류, 엔드포인트 오버로드, 분할 오류 등으로 인해 재난 시나리오가 악화되는 것을 방지하기 위해 설계되었습니다.

주제

- Amazon Route 53가 Cascading 오류를 방지하는 방법
- Amazon Route 53가 인터넷 분할을 다루는 방식

Amazon Route 53가 Cascading 오류를 방지하는 방법

Cascading 오류에 대한 1차 방어로, 각 요청 라우팅 알고리즘(가중치, 장애 조치 등)에는 최후의 수단 모드가 있습니다. 이 특수 모드에서 모든 레코드가 비정상 상태로 간주되는 경우 Route 53 알고리즘은 다시 모든 레코드를 정상 상태로 간주하기 시작합니다.

예를 들어 몇 개의 호스트 상에서 애플리케이션의 모든 인스턴스가 상태 확인 요청을 거부하면, Route 53 DNS 서버는 DNS 응답을 반환하지 않거나 NXDOMAIN(존재하지 않는 도메인) 응답을 반환하기보다는 어떻게든 하나의 응답을 선택하여 반환합니다. 애플리케이션은 사용자에게 응답할 수 있지만 여전히 상태 확인에 실패하므로, 이것은 구성 오류를 어느 정도 방지해 줍니다.

마찬가지로 애플리케이션이 오버로드되고 3개 중 1개의 엔드포인트가 상태 확인에 실패하여 Route 53 DNS 응답에서 제외되는 경우에 Route 53는 2개의 남은 엔드포인트 사이에 응답을 분산합니다. 남은 엔드포인트가 추가 로드를 다루지 못하여 실패하게 되면, Route 53는 요청을 다시 3개의 엔드포인트 전체로 분산하기 시작합니다.

Amazon Route 53가 인터넷 분할을 다루는 방식

비록 흔하지는 않지만 때때로 심각한 인터넷 분할이 발생하는데, 이는 더 큰 지리 지역이 다른 지리 지역과 인터넷상에서 통신할 수 없는 상태를 뜻합니다. 이러한 분할 동안 Route 53 위치는 엔드포인트의 상태에 대해 서로 다른 결론에 도달하여 CloudWatch에 보고되는 상태와 다를 수 있습니다. 각 AWS 리전의 Route 53 상태 확인기는 상태 확인 상태를 모든 Route 53 위치로 지속적으로 전송합니다. 인터넷 분할이 일어나는 동안에 각 Route 53 위치는 보통 가장 가까운 리전에서 이러한 상태의 일부에만 액세스할 수 있습니다.

예를 들어 남아메리카를 오가는 연결에 영향을 미치는 인터넷 분할 동안 Route 53 남아메리카(상파울루) 위치의 Route 53 DNS 서버들은 남아메리카(상파울루) AWS 리전의 상태 확인 엔드포인트에는 접속이 양호할 수 있지만, 그 밖의 리전에 있는 엔드포인트에 대해서는 접속이 불량일 수 있습니다. 이와 동시에 미국 동부(오하이오)의 Route 53는 남아메리카(상파울루) 리전의 상태 확인 엔드포인트에 대해 접속이 불량하여 해당 레코드가 비정상이라는 결론을 내릴 수도 있습니다.

이와 같은 분할은 엔드포인트들의 국지적 가시성을 근거로 Route 53 위치가 엔드포인트들의 상태에 대해 서로 다른 결론을 내리는 상황을 야기할 수 있습니다. 이것이 바로 연결할 수 있는 상태 확인 프로그램 중 일부만이 엔드포인트를 정상이라고 여기면 각 Route 53 위치가 엔드포인트를 정상이라고 여기는 이유입니다.

상태 확인에 대한 이름 및 태그 지정

Amazon Route 53 상태 확인에 태그를 추가할 수 있는데, 이를 통해 상태 확인 ID보다 더 이해하기 쉬운 이름을 상태 확인에 부여할 수 있습니다. 이는에서 AWS 청구서를 구성하기 위해 AWS Billing and Cost Management 제공하는 것과 동일한 태그입니다. 비용 할당 태그 사용에 대한 자세한 내용은 AWS Billing 사용자 설명서의 사용자 정의 청구 보고서용 비용 할당 태그 사용을 참조하세요.

각 태그는 사용자가 정의하는 키(태그의 이름)와 값으로 구성됩니다. 상태 확인에 태그를 추가할 때는 키와 값에 대해 다음 값을 가진 태그 하나를 추가하는 것이 좋습니다.

- 키 - 이름
- 값 - 상태 확인에 지정하고자 하는 이름

이름(Name) 태그의 값은 Route 53 콘솔의 상태 확인 목록에 표시되어 상태 확인을 즉시 서로 구별할 수 있게 해줍니다. 상태 확인에 대한 다른 태그를 보려면 상태 확인을 선택한 다음 [Tags] 탭을 선택합니다.

태그에 대한 자세한 내용은 다음 주제들을 참조하십시오.

- Route 53 콘솔에서 상태 확인을 추가하거나 편집할 때 이름 태그를 추가, 편집 또는 삭제하려면 상태 확인의 생성 및 업데이트 섹션을 참조하세요.
- Route 53 리소스 태그 지정의 개요는 Amazon Route 53 리소스 태그 지정 섹션을 참조하세요.

태그 제한

태그에 적용되는 기본 제한은 다음과 같습니다.

- 리소스당 최대 태그 수 - 새 콘솔의 경우 50개, 이전 콘솔의 경우 10개입니다.
- 최대 키 길이 - 유니코드 128자
- 최대 값 길이 - 유니코드 256자
- 키 및 값에 유효한 값 - UTF-8 문자 세트의 대문자 및 소문자, 숫자, 공백, 그리고 / = + - 및 @
- 태그 키와 값은 대/소문자를 구분합니다
- 키 또는 값에 `aws:` 접두사를 사용하지 마세요. 전용입니다 AWS .

상태 확인에 대한 태그의 추가, 편집 및 삭제

다음 절차는 Route 53 콘솔에서 상태 확인에 대해 태그를 사용하는 방법을 보여줍니다.

> **Note**
>
> Route 53용 상태 확인 콘솔을 업데이트하고 있습니다. 전환 기간 동안에는 기존 콘솔을 계속 사용할 수 있습니다.

사용 중인 콘솔의 탭을 선택합니다.

- 새로운 콘솔
- 이전 콘솔

New console

상태 확인에 태그를 추가하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 상태 확인을 선택합니다.
3. 태그를 추가할 상태 확인의 연결된 ID를 선택합니다.
4. 하단 페이지에서 태그 탭을 선택하고 관리를 선택한 다음 새 태그 추가를 선택합니다.
5. 키 필드에 태그 이름을 입력하고 값 필드에 값을 입력합니다.
6. 저장(Save)을 선택합니다.

상태 확인에 대한 태그를 편집하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 상태 확인을 선택합니다.
3. 상태 확인의 연결된 ID를 선택합니다.
4. 하단 창에서 태그 탭을 선택한 다음 관리를 선택합니다.
5. 이제 태그를 편집하고 추가할 수 있습니다.
6. 저장(Save)을 선택합니다.

상태 확인에 대한 태그를 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 상태 확인을 선택합니다.
3. 상태 확인의 연결된 ID를 선택합니다.
4. 하단 창에서 태그 탭을 선택한 다음 관리를 선택합니다.
5. 삭제할 태그 옆에 있는 제거를 선택합니다.

6. 저장(Save)을 선택합니다.

Old console

상태 확인에 태그를 추가하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 상태 확인(Health Checks)을 선택합니다.
3. 하나의 상태 확인을 선택하거나, 여러 개의 상태 확인을 선택해 같은 태그를 1개 이상의 상태 확인에 추가합니다.
4. 하단 창에서 [Tags] 탭을 선택한 다음, [Add/Edit Tags]를 선택합니다.
5. [Add/Edit Tags] 대화 상자에서, [Key] 필드에 태그 이름을 입력하고 [Value] 필드에 값을 입력합니다.
6. [Apply changes]를 선택합니다.

상태 확인에 대한 태그를 편집하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 상태 확인(Health Checks)을 선택합니다.
3. 상태 확인을 선택합니다.

   같은 태그를 공유하는 여러 개의 상태 확인을 선택하는 경우에는 모든 태그를 동시에 편집할 수 없습니다. 그러나 태그가 있는 상태 확인과 태그가 없는 최소 1개의 상태 확인을 선택하면 여러 개의 상태 확인에 표시되는 태그의 값을 편집할 수 있다는 점에 유의하십시오.

   예를 들어 Cost Center 태그가 있는 여러 개의 상태 확인과 그렇지 않은 것 한 개를 선택했다고 가정합시다. 태그를 추가하는 옵션을 선택하고 키에 Cost Center를, 값으로 777을 지정합니다. 이미 Cost Center 태그가 있는 상태 확인에 대해 Route53는 값을 777로 변경합니다. Cost Center 태그가 없는 상태 확인 1건에 대해 Route 53는 하나를 추가하고 값을 777로 변경합니다.
4. 하단 창에서 [Tags] 탭을 선택한 다음, [Add/Edit Tags]를 선택합니다.
5. [Add/Edit Tags] 대화 상자에서 값을 편집합니다.
6. 저장(Save)을 선택합니다.

상태 확인에 대한 태그를 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 상태 확인(Health Checks)을 선택합니다.
3. 하나의 상태 확인을 선택하거나, 여러 개의 상태 확인을 선택해 같은 태그를 1개 이상의 상태 확인으로부터 삭제합니다.
4. 하단 창에서 [Tags] 탭을 선택한 다음, [Add/Edit Tags]를 선택합니다.
5. [Add/Edit Tags] 대화 상자에서 삭제하고자 하는 태그 옆의 *X*를 선택합니다.
6. 저장(Save)을 선택합니다.

Amazon Route 53 API가 2012-12-12 이전 버전인 상태 확인 사용하기

상태 확인은 Amazon Route 53 API 2012-12-12 버전부터 지원됩니다. 호스팅 영역에 상태 확인이 구성된 레코드가 포함되어 있는 경우 2012-12-12 이후 버전의 API만 사용하는 것이 좋습니다. API가 이전 버전인 상태 확인을 사용할 경우에는 다음과 같은 제한이 있음을 유념하십시오.

- `ChangeResourceRecordSets` 작업은 `EvaluateTargetHealth`, `Failover` 또는 `HealthCheckId` 요소를 포함하는 레코드를 생성 또는 삭제할 수 없습니다.
- `ListResourceRecordSets` 작업은 이러한 요소를 포함하는 레코드를 나열할 수 있지만 요소는 출력에 포함되지 않습니다. 대신에 응답의 `Value` 요소는 레코드에 지원되지 않는 속성이 포함되어 있다는 메시지를 담고 있습니다.

상태 확인의 상태 모니터링 및 알림 수신

Amazon Route 53 콘솔에서 상태 확인의 상태를 모니터링합니다. CloudWatch 경보를 설정하여 상태 확인의 상태가 변경될 때 자동 알림을 수신할 수도 있습니다.

주제

상태 확인의 상태 및 상태 확인 실패 이유 보기

Route 53 콘솔에서 Route 53 상태 확인 프로그램에서 보고하는 대로 상태 확인의 상태(정상 또는 비정상)를 볼 수 있습니다. 계산된 상태 확인을 제외한 모든 상태 확인의 경우, 마지막 상태 확인 실패의 이유도 볼 수 있습니다(예: 상태 확인 프로그램이 엔드포인트와의 연결을 설정하지 못함).

> **Note**
>
> Route 53용 상태 확인 콘솔을 업데이트하고 있습니다. 전환 기간 동안에는 기존 콘솔을 계속 사용할 수 있습니다.

사용 중인 콘솔의 탭을 선택합니다.

- 새로운 콘솔
- 이전 콘솔

New console

상태 확인의 상태와 마지막 실패 이유를 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 상태 확인을 선택합니다.

3. 모든 상태 확인의 상태에 대한 개요, 즉 정상 또는 비정상은 상태(Status) 열에서 확인할 수 있습니다. 자세한 내용은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 단원을 참조하십시오.
4. 계산된 상태 확인을 제외한 모든 상태 확인의 경우 지정된 엔드포인트의 상태를 확인 중인 Route 53 상태 확인 프로그램의 상태를 볼 수 있습니다.
5. 세부 정보를 보려는 상태 확인의 연결된 ID를 선택합니다.
6. 하단 창에서 상태 확인 프로그램 탭을 선택합니다.

> **Note**
>
> 새 상태 확인은 Route 53 상태 확인 프로그램에 전파되어야 상태 확인 상태 및 마지막 오류 이유가 상태(Status) 열에 표시됩니다. 전달이 끝날 때까지 해당 열의 메시지에 어떤 상태도 사용할 수 없다고 나타납니다.

7. 표에는 다음 값이 포함됩니다.

   Health checker IP

   상태 확인을 수행한 Route 53 상태 확인 프로그램의 IP 주소입니다.

   Last checked

   상태 확인 날짜 및 시간 또는 마지막 실패 날짜 및 시간입니다.

   상태 표시기

   상태 확인의 현재 상태 또는 마지막 상태 확인 실패 이유입니다.

Old console

상태 확인의 상태와 마지막 실패 이유를 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 상태 확인(Health Checks)을 선택합니다.
3. 모든 상태 확인의 상태에 대한 개요, 즉 정상 또는 비정상은 상태(Status) 열에서 확인할 수 있습니다. 자세한 내용은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 단원을 참조하십시오.

4. 계산된 상태 확인을 제외한 모든 상태 확인의 경우 지정된 엔드포인트의 상태를 확인 중인 Route 53 상태 확인 프로그램의 상태를 볼 수 있습니다. 상태 확인을 선택합니다.
5. 하단 창에서 상태 확인(Health Checks) 탭을 선택합니다.

> **Note**
>
> 새 상태 확인은 Route 53 상태 확인 프로그램에 전파되어야 상태 확인 상태 및 마지막 오류 이유가 상태(Status) 열에 표시됩니다. 전달이 끝날 때까지 해당 열의 메시지에 어떤 상태도 사용할 수 없다고 나타납니다.

6. 상태 확인의 현재 상태를 보고자 하는지, 아니면 마지막 실패의 날짜 및 시간, 그리고 실패의 이유를 보고자 하는지 선택합니다. 상태(Status) 탭의 표는 다음 값들을 포함합니다.

   Health checker IP

   상태 확인을 수행한 Route 53 상태 확인 프로그램의 IP 주소입니다.

   Last checked

   상태 확인의 날짜 및 시간 또는 마지막 실패의 날짜 및 시간(상태(Status) 탭 맨 위에서 선택하는 옵션에 따라 달라짐)입니다.

   Status

   상태 확인의 현재 상태 또는 마지막 상태 확인 실패의 이유(상태(Status) 탭 맨 위에서 선택하는 옵션에 따라 달라짐)입니다.

상태 확인 프로그램과 엔드포인트 사이의 지연 시간 모니터링

상태 확인을 생성할 때 (다른 상태 확인의 상태가 아니라) 엔드포인트의 상태를 모니터링하고 지연 시간 그래프(Latency graphs) 옵션을 선택하면 Route 53 콘솔의 CloudWatch 그래프에서 다음 값을 볼 수 있습니다.

- Route 53 상태 확인 프로그램이 엔드포인트와의 TCP 연결을 설정하는 데 걸린 평균 시간(밀리초)입니다.
- Route 53 상태 확인 프로그램이 HTTP 또는 HTTPS 요청에 대한 응답의 첫 번째 바이트를 수신하는 데 걸린 평균 시간(ms)입니다.
- Route 53 상태 확인 프로그램이 SSL/TLS 핸드셰이크를 완료하는 데 걸린 평균 시간(ms)입니다.

> **Note**
>
> 기존 상태 확인에 대한 지연 시간 모니터링을 활성화할 수 없습니다.

> **Important**
>
> 상태 확인 프로그램은 16개의 중복 가용 영역에서 실행됩니다. 배포, 업데이트, 유지 관리 등으로 인해 가용 영역을 사용할 수 없는 경우가 많습니다. 상태 확인 시스템은 고객의 영향 없이 이를 고려하도록 설계되었습니다.

> **Note**
>
> Route 53용 상태 확인 콘솔을 업데이트하고 있습니다. 전환 기간 동안에는 기존 콘솔을 계속 사용할 수 있습니다.

사용 중인 콘솔의 탭을 선택합니다.

- 새로운 콘솔
- 이전 콘솔

New console

Route 53 상태 확인 프로그램과 엔드포인트 사이의 지연 시간을 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 상태 확인을 선택합니다.
3. 지표를 보려는 상태 확인에 연결된 ID를 선택합니다. 엔드포인트의 상태를 모니터링하는 상태 확인과 어떤 지연 시간 그래프(Latency graphs) 옵션이 활성화되어 있는지에 대한 지연 시간 데이터만 볼 수 있습니다.
4. 하단 창에서 지표 탭을 선택합니다.
5. 지연 시간 그래프를 표시하려는 시간 범위와 지리적 리전을 선택합니다.

   그래프는 지정된 시간 범위에 대한 상태를 표시합니다.

TCP connection time(HTTP 및 TCP만 해당)

선택한 지리적 리전에 있는 Route 53 상태 확인 프로그램이 엔드포인트와의 TCP 연결을 설정하는 데 걸린 평균 시간(ms)입니다.

Time to first byte(HTTP 및 HTTPS만 해당)

선택한 지리적 리전에 있는 Route 53 상태 확인 프로그램이 HTTP 또는 HTTPS 요청에 대한 응답의 첫 번째 바이트를 수신하는 데 걸린 평균 시간(ms)입니다.

Time to complete SSL handshake(HTTPS만 해당)

선택한 지리적 리전에 있는 Route 53 상태 확인 프로그램이 SSL/TLS 핸드셰이크를 완료하는 데 걸린 평균 시간(ms)입니다.

6. 더 큰 그래프를 보고 다른 설정을 지정하려면 그래프 오른쪽 상단의 점 3개를 선택합니다. 다음과 같은 설정을 변경할 수 있습니다.

통계

CloudWatch가 데이터에 대해 수행하는 계산을 변경합니다.

시간 범위

서로 다른 기간, 예를 들면, 하룻밤 사이 또는 지난 주 동안에 상태 확인의 상태가 어떠했는지 표시합니다.

기간

그래프에서 데이터 요소들 간의 간격을 변경합니다.

다음을 참조하세요.

- 상태 확인을 생성했다면, 데이터가 그래프에 나타날 때까지, 그리고 상태 확인 지표가 사용 가능한 지표 목록에 나타날 때까지 기다려야 할 수도 있습니다.
- 그래프는 자동으로 새로 고침되지 않습니다. 표시 내용을 업데이트하려면 새로 고침 () 아이콘을 선택합니다.
- 연결 시간 제한과 같이 어떤 이유로 상태 확인에 실패하는 경우 Route 53는 지연 시간을 측정할 수 없고 지연 시간 데이터가 해당 기간 동안 그래프에서 누락됩니다.

Old console

Route 53 상태 확인 프로그램과 엔드포인트 사이의 지연 시간을 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 상태 확인(Health Checks)을 선택합니다.
3. 적용 가능한 상태 확인 행을 선택합니다. 엔드포인트의 상태를 모니터링하는 상태 확인과 어떤 지연 시간 그래프(Latency graphs) 옵션이 활성화되어 있는지에 대한 지연 시간 데이터만 볼 수 있습니다.
4. 하단 창에서 지연 시간(Latency) 탭을 선택합니다.
5. 지연 시간 그래프를 표시하려는 시간 범위와 지리적 리전을 선택합니다.

   그래프는 지정된 시간 범위에 대한 상태를 표시합니다.

   TCP connection time(HTTP 및 TCP만 해당)

   선택한 지리적 리전에 있는 Route 53 상태 확인 프로그램이 엔드포인트와의 TCP 연결을 설정하는 데 걸린 평균 시간(ms)입니다.

   Time to first byte(HTTP 및 HTTPS만 해당)

   선택한 지리적 리전에 있는 Route 53 상태 확인 프로그램이 HTTP 또는 HTTPS 요청에 대한 응답의 첫 번째 바이트를 수신하는 데 걸린 평균 시간(ms)입니다.

   Time to complete SSL handshake(HTTPS만 해당)

   선택한 지리적 리전에 있는 Route 53 상태 확인 프로그램이 SSL/TLS 핸드셰이크를 완료하는 데 걸린 평균 시간(ms)입니다.

   > **Note**
   >
   > 1개 이상의 상태 확인을 선택하면, 그래프는 각 상태 확인을 별도의 컬러 코드 라인으로 표시합니다.

6. 더 큰 그래프를 보고 설정을 변경하려면 그래프를 클릭합니다. 다음과 같은 설정을 변경할 수 있습니다.

통계

CloudWatch가 데이터에 대해 수행하는 계산을 변경합니다.

시간 범위

서로 다른 기간, 예를 들면, 하룻밤 사이 또는 지난 주 동안에 상태 확인의 상태가 어떠했는지 표시합니다.

기간

그래프에서 데이터 요소들 간의 간격을 변경합니다.

다음을 참조하세요.

- 상태 확인을 생성했다면, 데이터가 그래프에 나타날 때까지, 그리고 상태 확인 지표가 사용 가능한 지표 목록에 나타날 때까지 기다려야 할 수도 있습니다.
- 그래프는 자동으로 새로 고침되지 않습니다. 표시 내용을 업데이트하려면 새로 고침 () 아이콘을 선택합니다.
- 연결 시간 제한과 같이 어떤 이유로 상태 확인에 실패하는 경우 Route 53는 지연 시간을 측정할 수 없고 지연 시간 데이터가 해당 기간 동안 그래프에서 누락됩니다.

CloudWatch를 이용한 상태 확인 모니터링

Route 53 상태 확인은 CloudWatch 지표와 통합되므로 다음 작업을 수행할 수 있습니다.

- 상태 확인이 적절하게 구성되었는지 확인합니다.
- 상태 확인의 상태를 지정된 기간 동안 검토합니다.
- 상태 확인의 상태가 비정상일 때 Amazon SNS 알림을 보내도록 CloudWatch를 구성합니다. 상태 확인이 실패하는 시점부터 연결된 SNS 알림을 수신하는 시점까지는 몇 분의 시간이 경과할 수도 있다는 점에 유의하세요.

자세한 내용은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 단원을 참조하십시오.

주제

상태 확인의 상태 보기

> **Note**
>
> Route 53용 상태 확인 콘솔을 업데이트하고 있습니다. 전환 기간 동안에는 기존 콘솔을 계속 사용할 수 있습니다.

사용 중인 콘솔의 탭을 선택합니다.

- 새로운 콘솔
- 이전 콘솔

New console

상태 확인의 상태를 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 상태 확인을 선택합니다.
3. 지표를 보려는 상태 확인에 연결된 ID를 선택합니다.
4. 하단 창에서 지표 탭을 선택합니다.

   2개의 그래프에 지난 한 시간 동안의 상태가 1분 간격으로 표시됩니다.

   Health check status

   그래프는 엔드포인트 상태에 대한 Route 53 평가를 표시합니다. 1은 정상 상태를 나타내고 0은 비정상 상태를 표시합니다.

Health checkers that report the endpoint healthy (%)

엔드포인트만 모니터링하는 상태 확인의 경우 그래프는 선택한 엔드포인트를 정상이라고 판단하는 Route 53 상태 확인 프로그램의 비율을 표시합니다.

상태 확인이 비활성화되면 이 지표를 사용할 수 없습니다.

Number of healthy child health checks

계산된 상태 확인에 대해서만 이 그래프는 상태가 정상인 하위 상태 확인의 수를 표시합니다.

5. 더 큰 그래프를 보고 다른 설정을 지정하려면 오른쪽 상단의 점 3개를 선택한 다음 확대를 선택합니다. 다음과 같은 설정을 변경할 수 있습니다.

   통계

   CloudWatch가 데이터에 대해 수행하는 계산을 변경합니다.

   시간 범위

   서로 다른 기간, 예를 들면, 하룻밤 사이 또는 지난 주 동안에 상태 확인의 상태가 어떠했는지 표시합니다.

   기간

   그래프에서 데이터 요소들 간의 간격을 변경합니다.

   다음을 참조하세요.

   - 상태 확인을 생성했다면, 데이터가 그래프에 나타날 때까지, 그리고 상태 확인 지표가 사용 가능한 지표 목록에 나타날 때까지 기다려야 할 수도 있습니다.
   - 그래프는 자동으로 새로 고침되지 않습니다. 표시 내용을 업데이트하려면 새로 고침 () 아이콘을 선택합니다.

Old console

상태 확인의 상태를 보려면(새 콘솔)

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.

2. 탐색 창에서 상태 확인(Health Checks)을 선택합니다.
3. 적용 가능한 상태 확인 행을 선택합니다.
4. 하단 창에서 모니터링(Monitoring) 탭을 선택합니다.

   2개의 그래프에 지난 한 시간 동안의 상태가 1분 간격으로 표시됩니다.

   Health check status

   그래프는 엔드포인트 상태에 대한 Route 53 평가를 표시합니다. 1은 정상 상태를 나타내고 0은 비정상 상태를 표시합니다.

   Health checkers that report the endpoint healthy (%)

   엔드포인트만 모니터링하는 상태 확인의 경우 그래프는 선택한 엔드포인트를 정상이라고 판단하는 Route 53 상태 확인 프로그램의 비율을 표시합니다.

   상태 확인이 비활성화되면 이 지표를 사용할 수 없습니다.

   Number of healthy child health checks

   계산된 상태 확인에 대해서만 이 그래프는 상태가 정상인 하위 상태 확인의 수를 표시합니다.

   > **Note**
   >
   > 1개 이상의 상태 확인을 선택하면, 그래프는 각 상태 확인을 별도의 컬러 코드 라인으로 표시합니다.

5. 더 큰 그래프를 보고 설정을 변경하려면 그래프를 클릭합니다. 다음과 같은 설정을 변경할 수 있습니다.

   통계

   CloudWatch가 데이터에 대해 수행하는 계산을 변경합니다.

   시간 범위

   서로 다른 기간, 예를 들면, 하룻밤 사이 또는 지난 주 동안에 상태 확인의 상태가 어떠했는지 표시합니다.

기간

그래프에서 데이터 요소들 간의 간격을 변경합니다.

다음을 참조하세요.

- 상태 확인을 생성했다면, 데이터가 그래프에 나타날 때까지, 그리고 상태 확인 지표가 사용 가능한 지표 목록에 나타날 때까지 기다려야 할 수도 있습니다.
- 그래프는 자동으로 새로 고침되지 않습니다. 표시 내용을 업데이트하려면 새로 고침 () 아이콘을 선택합니다.

상태 확인 경보 보기

> **Note**
>
> Route 53용 상태 확인 콘솔을 업데이트하고 있습니다. 전환 기간 동안에는 기존 콘솔을 계속 사용할 수 있습니다.

사용 중인 콘솔의 탭을 선택합니다.

- 새로운 콘솔
- 이전 콘솔

New console

CloudWatch 경보 상태를 확인하고 Amazon Route 53 경보를 편집하려면

1. Route 53 콘솔의 탐색 창에서 상태 확인을 선택합니다.
2. 경보를 보려는 상태 확인에 연결된 ID를 선택합니다.
3. 세부 정보 페이지 하단에서 경보 탭을 선택합니다.

   경보 목록에는 선택한 상태 확인을 위해 생성한 모든 Route 53 경보가 포함되어 있습니다.

   상태(State) 열은 각 경보의 현재 상태를 보여줍니다.

정상

CloudWatch는 엔드포인트가 경보 임계치를 충족하지 않는다고 판정하기에 충분한 통계치를 Route 53 상태 확인으로부터 축적했습니다.

데이터 부족

CloudWatch는 엔드포인트가 경보 임계치를 충족하는지 여부를 판정하기에 충분한 통계치를 축적하지 않았습니다. 새 경보의 초기 상태입니다. 또한 CloudWatch 지표를 사용할 수 없게 되거나, 연결된 경보를 삭제하지 않고 상태 확인을 삭제한 경우 경보 상태가 데이터 부족(INSUFFICIENT DATA)으로 변경됩니다.

경보

CloudWatch는 엔드포인트가 경보 임계치를 충족한다고 판정하여 지정된 이메일 주소로 알림을 보내기에 충분한 통계치를 Route 53 상태 확인으로부터 축적했습니다.

4. 경보에 대한 자세한 정보(예: 경보 업데이트 기록 및 상태 변경 내역)를 제공하는 CloudWatch 콘솔에서 경보를 보려면, 경보에 연결된 이름을 선택합니다. CloudWatch 콘솔에서 경보를 편집할 수도 있습니다.
5. CloudWatch 콘솔에서 새 CloudWatch 경보를 생성하려면 CloudWatch 경보 생성을 선택합니다. 자세한 내용은 CloudWatch 사용 설명서의 권장 경보 찾기 및 생성을 참조하세요.

Old console

CloudWatch 경보 상태를 확인하고 Amazon Route 53 경보를 편집하려면

1. Route 53 콘솔의 탐색 창에서 상태 확인(Health Checks)을 선택합니다.
2. 상태 확인 행을 선택합니다.
3. 세부 정보 창(다음의 x 상태 확인 선택됨(Health Checks Selected))에서 오른쪽 캐럿 ( ) 아이콘을 선택합니다.

   CloudWatch 경보 목록에는 현재 AWS 계정을 사용하여 생성한 모든 Route 53 경보가 포함되어 있습니다.

   상태(State) 열은 각 경보의 현재 상태를 보여줍니다.

정상

CloudWatch는 엔드포인트가 경보 임계치를 충족하지 않는다고 판정하기에 충분한 통계치를 Route 53 상태 확인으로부터 축적했습니다.

데이터 부족

CloudWatch는 엔드포인트가 경보 임계치를 충족하는지 여부를 판정하기에 충분한 통계치를 축적하지 않았습니다. 새 경보의 초기 상태입니다. 또한 CloudWatch 지표를 사용할 수 없게 되거나, 연결된 경보를 삭제하지 않고 상태 확인을 삭제한 경우 경보 상태가 데이터 부족(INSUFFICIENT DATA)으로 변경됩니다.

경보

CloudWatch는 엔드포인트가 경보 임계치를 충족한다고 판정하여 지정된 이메일 주소로 알림을 보내기에 충분한 통계치를 Route 53 상태 확인으로부터 축적했습니다.

4. 경보를 위한 설정을 보거나 편집하려면 경보의 이름을 선택합니다.
5. 경보에 대한 자세한 정보(예: 경보 업데이트 기록 및 상태 변경 내역)를 제공하는 CloudWatch 콘솔에서 경보를 보려면, 경보에 대한 더 많은 옵션(More Options) 열에서 보기(View)를 선택합니다.
6. 다른 AWS 서비스에 대한 경보를 포함하여 현재 AWS 계정을 사용하여 생성한 모든 CloudWatch 경보를 보려면 모든 CloudWatch 경보 보기를 선택합니다.
7. 현재 AWS 계정에서 현재 사용하고 있지 않은 지표를 포함하여 사용 가능한 모든 CloudWatch 지표를 보려면 모든 CloudWatch 지표 보기를 선택합니다.

CloudWatch 콘솔에서 상태 확인 지표 보기

CloudWatch 콘솔에서 Route 53 지표를 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/cloudwatch/ CloudWatch 콘솔을 엽니다.
2. 현재 리전을 미국 동부(버지니아 북부)(US East (N. Virginia))로 변경합니다. 다른 모든 리전을 현재 리전으로 선택하는 경우 Route 53 지표는 사용할 수 없습니다.
3. 탐색 창에서 지표(Metrics)를 선택합니다.
4. 모든 지표(All metrics) 탭에서 [Route 53]을 선택합니다.
5. 상태 확인 지표(Health Check Metrics)를 선택합니다.

6. CloudWatch 콘솔에서 SNS 알림을 설정할 수도 있습니다. 자세한 내용은 CloudWatch 사용 설명서의 권장 경보 생성을 참조하세요.

SNS 알림을 사용하여 경보 생성

> **Note**
>
> 다음 절차는 이전 콘솔에만 적용됩니다. 새 콘솔은 CloudWatch 콘솔로 이동하여 경보를 생성합니다. 자세한 내용은 CloudWatch 사용 설명서의 권장 경보 찾기 및 생성을 참조하세요.

상태 확인의 상태가 비정상일 때 Amazon SNS 알림을 수신하려면(이전 콘솔)

1. Route 53 콘솔의 탐색 창에서 상태 확인(Health Checks)을 선택합니다.
2. 적용 가능한 상태 확인 행을 선택합니다.
3. 하단 창에서 경보(Alarms) 탭을 선택합니다.

   표에는 이 상태 확인에 대해 이미 생성한 경보가 나와 있습니다.
4. 경보 생성(Create Alarm)을 선택합니다.
5. 다음 값을 지정하세요.

   Alarm name

   Route 53가 표시할 이름을 경보(Alarms) 탭에 있는 이름(Name) 열에 입력합니다.

   Alarm description

   (선택 사항) 경보에 대한 설명을 입력합니다. 이 값은 CloudWatch 콘솔에 표시됩니다.

   Send notification

   이 상태 확인의 상태가 경보를 트리거하는 경우 Route 53가 알림을 보내도록 할지 선택합니다.

   Notification target("Send notification"이 "Yes"일 때만)

   CloudWatch가 기존 SNS 주제로 알림을 보내도록 하려면 목록에서 해당 주제를 선택합니다.

   CloudWatch가 알림을 보내지만 기존 SNS 주제로는 보내지 않도록 하려면 다음 중 하나를 수행합니다.

- CloudWatch가 이메일 알림을 보내도록 하려는 경우 - 새로운 SNS 주제(New SNS topic)를 선택하고 이 절차를 계속 진행합니다.
- CloudWatch가 다른 방법으로 알림을 보내도록 하려는 경우 - 새 브라우저 탭을 열고 Amazon SNS 콘솔로 이동한 후 새 주제를 생성합니다. 그런 다음, Route 53 콘솔로 돌아가서 알림 대상(Notification target) 목록에서 새 주제 이름을 선택하고 이 절차를 계속 진행합니다.

주제 이름(Topic name)(새로운 Amazon SNS 주제를 생성하기로 선택할 때만 해당)

새 Amazon SNS 주제의 이름을 입력합니다.

수신인 이메일 주소(Recipient email addresses)(새로운 Amazon SNS 주제를 생성하기로 선택할 때만 해당)

상태 확인이 경보를 트리거할 때 Route 53가 SNS 알림을 보내도록 하려는 대상 이메일 주소를 입력합니다.

Alarm target

Route 53가 상태 확인을 위해 평가하도록 하려는 값을 선택합니다.

- 상태 확인 상태(Health check status) - Route 53 상태 확인 프로그램에서 상태 확인이 정상이거나 비정상이라고 보고함
- 해당 엔드포인트를 정상으로 보고한 상태 확인 프로그램(%)(Health checkers that report the endpoint healthy (%)) - 상태 확인의 상태가 정상이라고 보고하는 Route 53 상태 확인 프로그램의 비율
- 정상 하위 상태 확인 수(Number of healthy child health checks)(계산된 상태 확인만 해당) - 계산된 상태 확인에서 상태 확인의 상태가 정상이라고 보고하는 하위 상태 확인의 수
- TCP 연결 시간(TCP connection time)(HTTP 및 TCP 상태 확인만 해당) - Route 53 상태 확인 프로그램이 엔드포인트와의 TCP 연결을 설정하는 데 걸린 시간(ms)
- SSL 핸드셰이크 완료 시간(Time to complete SSL handshake)(HTTPS 상태 확인만 해당) - Route 53 상태 확인 프로그램이 SSL/TLS 핸드셰이크를 완료하는 데 걸린 시간(ms)
- 첫 번째 바이트 수신 시간(Time to first byte)(HTTP 및 HTTPS 상태 확인만 해당) - Route 53 상태 확인 프로그램이 HTTP 또는 HTTPS 요청에 대한 응답의 첫 번째 바이트를 수신하는 데 걸린 시간(ms)

Alarm target

지연 시간을 기준으로 한 경보 대상에 대해(TCP 연결 시간(TCP connection time), SSL 핸드셰이크 완료 시간(Time to complete SSL handshake), 첫 번째 바이트 수신 시간(Time to first

byte)), CloudWatch가 특정 리전의 Route 53 상태 확인 프로그램 또는 모든 리전(전역(Global))에 대한 지연 시간을 계산하도록 할지 선택합니다.

리전을 선택하면 Route 53가 분당 2회만 지연 시간을 측정하며, 모든 리전을 선택하는 경우보다 샘플 수는 적습니다. 따라서 범위를 벗어나는 값이 측정될 가능성이 많습니다. 허위 경보 알림을 예방하려면 상태 확인이 연속적으로 실패하여 CloudWatch가 알림을 보내야 하는 연속 실패 기간을 큰 수로 지정하는 것이 좋습니다.

처리 조건

다음 설정을 이용해 CloudWatch가 언제 경보를 트리거할지를 결정하세요.

Alarm target	권장 조건	설명
Health check status	최소 < 1	엔드포인트가 비정상이면 Route 53 상태 확인 프로그램이 보고합니다.
Health checkers that report the endpoint healthy (%)	평균 < 원하는 백분율	엔드포인트만 모니터링하는 상태 확인(Health checks that monitor an endpoint only) - Route 53는 상태 확인 프로그램 중 18% 미만이 정상 상태를 보고할 때 상태 확인의 상태가 비정상인 것으로 간주합니다. 이 지표의 샘플 개수(Sample Count)는 선택하지 마세요. Route 53가 더 많은 상태 확인 영역을 추가하면서 샘플 카운트의 범위가 변경될 수 있기 때문입니다. 평균은 상태 확인의 상태를 보고 중인 확인 프로그램의 비율을 항상 정확하게 나타냅니다.
Number of healthy child health checks	최소 < 정상 하위 상태 확인의 원하는 수	최소 통계는 가장 일반적인 값을 반환하며 최악의 경우를 가정한 시나리오를 나타냅니다.
TCP connection time	평균 > 원하는 시간(ms)	평균은 다른 통계보다 더 일관된 값입니다.

Alarm target	권장 조건	설명
Time to complete SSL handshake	평균 > 원하는 시간 (ms)	평균은 다른 통계보다 더 일관된 값입니다.
Time to first byte	평균 > 원하는 시간 (ms)	평균은 다른 통계보다 더 일관된 값입니다.

For at least ***x*** consecutive periods of ***y*** minutes/hours/day

Route 53에서 알림을 전송하기 전에 지정된 값이 몇 차례의 연속 시간 간격 동안 기준을 충족해야 하는지 지정합니다. 그런 다음 시간 간격의 길이를 지정합니다.

6. 생성(Create)을 선택하면 Amazon SNS가 새로운 SNS 주제에 관한 정보가 포함된 이메일을 전송합니다.
7. 이메일에서 구독 확인(Confirm subscription)을 선택합니다. CloudWatch 알림을 받으려면 구독을 확정해야 합니다.

DNS 방화벽을 사용하여 아웃바운드 DNS 트래픽 필터링

Route 53 Resolver DNS 방화벽을 사용하면 Virtual Private Cloud(VPC)에 대한 아웃바운드 DNS 트래픽을 필터링하고 제어할 수 있습니다. 이렇게 하려면 DNS 방화벽 규칙 그룹에 재사용 가능한 필터링 규칙 컬렉션을 생성하고 규칙 그룹을 VPC에 연결한 다음 DNS 방화벽 로그 및 지표 활동을 모니터링합니다. 활동에 따라 DNS 방화벽의 동작을 적절하게 조정할 수 있습니다.

DNS 방화벽을 사용하면 VPC의 아웃바운드 DNS 요청을 보호할 수 있습니다. 이러한 요청은 도메인 이름 해석을 위해 Resolver를 통해 라우팅됩니다. DNS 방화벽 보호의 주된 용도는 데이터의 DNS 유출을 방지하는 것입니다. DNS 유출은 공격자가 VPC 애플리케이션 인스턴스를 손상시킨 다음 DNS 조회를 사용하여 VPC에서 데이터를 제어하는 도메인으로 전송할 때 발생할 수 있습니다. DNS 방화벽을 사용하면 애플리케이션에서 쿼리할 수 있는 도메인을 모니터링하고 제어할 수 있습니다. 잘못된 것으로 알고 있는 도메인에 대한 액세스를 거부하고 다른 모든 쿼리가 통과하도록 허용할 수 있습니다. 또는 명시적으로 신뢰하는 도메인을 제외한 모든 도메인에 대한 액세스를 거부할 수 있습니다.

DNS 방화벽을 사용하여 VPC 엔드포인트 이름을 포함하여 프라이빗 호스팅 영역(공유 또는 로컬 호스팅 영역)의 리소스에 대한 해석 요청을 차단할 수도 있습니다. 또한 퍼블릭 또는 프라이빗 Amazon EC2 인스턴스 이름에 대한 요청을 차단할 수도 있습니다.

DNS 방화벽은 Route 53 Resolver 기능이며 사용할 Resolver 설정이 추가로 필요하지 않습니다.

AWS Firewall Manager 는 DNS 방화벽을 지원합니다.

Firewall Manager 를 사용하여 AWS Organizations계정에서 VPC의 DNS 방화벽 규칙 그룹 연결을 중앙에서 구성하고 관리할 수 있습니다. Firewall Manager는 Firewall Manager DNS 방화벽 정책 범위로 들어오는 VPC에 대한 연결을 자동으로 추가합니다. 자세한 내용은 AWS WAF AWS Firewall Manager, 및 AWS Shield Advanced 개발자 안내서AWS Firewall Manager의 섹션을 참조하세요.

DNS 방화벽의 작동 방식 AWS Network Firewall

DNS 방화벽과 Network Firewall 모두 다른 유형의 트래픽이 아닌 경우 도메인 이름 필터링을 제공합니다. DNS 방화벽과 Network Firewall 함께 사용하면 서로 다른 두 네트워크 경로에서 애플리케이션 계층 트래픽에 대한 도메인 기반 필터링을 구성할 수 있습니다.

- DNS 방화벽은 VPC 내의 애플리케이션에서 Route 53 Resolver를 통과하는 아웃바운드 DNS 쿼리에 대한 필터링을 제공합니다. 쿼리에 대한 사용자 지정 응답을 차단된 도메인 이름에 전송하도록 DNS 방화벽을 구성할 수도 있습니다.
- Network Firewall은 네트워크 및 애플리케이션 계층 트래픽 모두에 대한 필터링을 제공하지만 Route 53 Resolver에서 만든 쿼리는 표시하지 않습니다.

자세한 내용은 Network Firewall 개발자 안내서를 참조하세요.

Route 53 Resolver DNS 방화벽이 작동하는 방식

Route 53 Resolver DNS 방화벽을 사용하면 사이트에 대한 액세스를 제어하고 Route 53 Resolver를 통해 VPC에서 나가는 DNS 쿼리에 대한 DNS 수준 위협을 차단할 수 있습니다. DNS 방화벽을 사용하여 VPC와 연결하는 규칙 그룹에 도메인 이름 필터링 규칙을 정의합니다. 허용 또는 차단할 도메인 이름 목록 또는 DNS 터널링 및 도메인 생성 알고리즘(DGA) 기반 위협으로부터 보호하는 Route 53 Resolver DNS Firewall Advanced 규칙을 지정할 수 있습니다. 차단하는 DNS 쿼리에 대한 응답을 사용자 지정할 수 있습니다. 도메인 목록이 포함된 규칙의 경우 규칙을 미세 조정하여 MX 레코드와 같은 특정 쿼리 유형을 허용할 수도 있습니다.

DNS 방화벽은 도메인 이름만 필터링합니다. DNS 방화벽은 해당 이름을 차단할 IP 주소로 해석하지 않습니다. 또한 DNS 방화벽은 DNS 트래픽을 필터링하지만 HTTPS, SSH, TLS, FTP 등과 같은 다른 애플리케이션 계층 프로토콜을 필터링하지 않습니다.

Route 53 Resolver DNS 방화벽 구성 요소 및 설정

다음 중앙 구성 요소 및 설정을 사용하여 DNS 방화벽을 관리합니다.

DNS 방화벽 규칙 그룹

DNS 쿼리를 필터링하기 위한 DNS 방화벽 규칙의 명명된 재사용 가능한 컬렉션을 정의합니다. 규칙 그룹을 필터링 규칙으로 채운 후, 규칙 그룹을 하나 이상의 VPC와 연결합니다. 규칙 그룹을 VPC와 연결하면 VPC에 대해 DNS 방화벽 필터링을 활성화합니다. 그런 다음 Resolver가 규칙 그룹이 연결된 VPC에 대한 DNS 쿼리를 수신하면 Resolver는 필터링을 위해 쿼리를 DNS 방화벽으로 전달합니다.

여러 규칙 그룹을 단일 VPC 와 연결하는 경우 각 연결의 우선 순위를 설정하여 처리 순서를 표시합니다. DNS 방화벽은 우선 순위 설정에 따라 가장 낮은 숫자에서 높은 숫자 순으로 VPC 대한 규칙 그룹을 처리합니다.

자세한 내용은 DNS 방화벽 규칙 그룹 및 규칙 섹션을 참조하세요.

DNS 방화벽 규칙

DNS 방화벽 규칙 그룹의 DNS 쿼리에 대한 필터링 규칙을 정의합니다. 각 규칙은 도메인 목록 하나 또는 DNS 방화벽 보호와 도메인이 규칙의 도메인 사양과 일치하는 DNS 쿼리에 대해 수행할 작업을 지정합니다. 일치하는 쿼리에 대해 (도메인 목록만 있는 규칙)를 허용하거나 차단하거나 알릴 수

있습니다. 도메인 목록이 있는 규칙에서는 목록에 있는 도메인에 대한 쿼리 유형을 지정할 수도 있습니다. 예를 들어 특정 도메인 또는 도메인에 대한 MX 쿼리 유형을 차단하거나 허용할 수 있습니다. 차단된 쿼리에 대한 사용자 지정 응답을 정의할 수도 있습니다.

DNS 방화벽 규칙의 경우 일치하는 쿼리만 차단하거나 알릴 수 있습니다.

규칙 그룹의 각 규칙에는 규칙 그룹 내의 고유한 우선 순위 설정이 있습니다. DNS 방화벽은 우선 순위 설정에 따라 가장 낮은 숫자에서 높은 숫자 순으로 VPC 대한 규칙 그룹의 규칙을 처리합니다.

DNS 방화벽 규칙은 정의된 규칙 그룹의 컨텍스트에만 존재합니다. 규칙을 재사용하거나 규칙 그룹과 독립적으로 참조할 수 없습니다.

자세한 내용은 DNS 방화벽 규칙 그룹 및 규칙 섹션을 참조하세요.

도메인 목록

DNS 필터링에 사용할 도메인 사양의 명명된 재사용 가능한 컬렉션을 정의합니다. 규칙 그룹의 각 규칙에는 단일 도메인 목록이 필요합니다. 액세스를 허용할 도메인, 액세스를 거부할 도메인 또는 둘 모두의 조합을 지정하도록 선택할 수 있습니다. 자체 도메인 목록을 생성하고가 자동으로 AWS 관리하는 도메인 목록을 사용할 수 있습니다.

자세한 내용은 Route 53 Resolver DNS 방화벽 도메인 목록 단원을 참조하십시오.

도메인 리디렉션 설정(도메인 목록만 해당)

도메인 리디렉션 설정을 사용하면 DNS 방화벽 규칙을 구성하여 CNAME, DNAME 등과 같은 DNS 리디렉션 체인(기본값)의 모든 도메인을 검사하거나 첫 번째 도메인만 검사하고 나머지는 신뢰할 수 있습니다. 전체 DNS 리디렉션 체인을 검사하도록 선택한 경우 규칙에서 ALLOW로 설정된 도메인 목록에 후속 도메인을 추가해야 합니다. 전체 DNS 리디렉션 체인을 검사하도록 선택한 경우 후속 도메인을 도메인 목록에 추가하고 규칙을 수행할 작업인 ALLOW, BLOCK 또는 ALERT로 설정해야 합니다.

자세한 내용은 DNS 방화벽의 규칙 설정 단원을 참조하십시오.

쿼리 유형(도메인 목록만 해당)

쿼리 유형 설정을 사용하면 특정 DNS 쿼리 유형을 필터링하도록 DNS 방화벽 규칙을 구성할 수 있습니다. 쿼리 유형을 선택하지 않으면 규칙이 모든 DNS 쿼리 유형에 적용됩니다. 예를 들어 특정 도메인의 모든 쿼리 유형을 차단하지만 MX 레코드를 허용할 수 있습니다.

자세한 내용은 DNS 방화벽의 규칙 설정 단원을 참조하십시오.

DNS 방화벽 고급 보호

DNS 쿼리에서 알려진 위협 서명을 기반으로 의심스러운 DNS 쿼리를 감지합니다. 규칙 그룹의 각 규칙에는 단일 DNS Firewall Advanced 보호 설정이 필요합니다. 다음 중에서 보호를 선택할 수 있습니다.

- 도메인 생성 알고리즘(DGAs)

  공격자는 DGAs를 사용하여 많은 수의 도메인을 생성하여 맬웨어 공격을 시작합니다.

- DNS 터널링

  DNS 터널링은 공격자가 클라이언트에 대한 네트워크 연결 없이 DNS 터널을 사용하여 클라이언트에서 데이터를 유출하는 데 사용됩니다.

DNS Firewall Advanced 규칙에서는 위협과 일치하는 쿼리를 차단하거나 경고하도록 선택할 수 있습니다. 위협 방지 알고리즘은에서 관리 및 업데이트합니다 AWS.

자세한 내용은 Route 53 Resolver DNS 방화벽 고급 단원을 참조하십시오.

신뢰도 임계값(DNS 방화벽 고급 보호만 해당)

DNS 위협 방지를 위한 신뢰도 임계값입니다. DNS Firewall Advanced 규칙을 생성할 때이 값을 제공해야 합니다. 신뢰 수준 값은 다음을 의미합니다.

- 높음 - 오탐률이 낮은 가장 잘 확인된 위협만 탐지합니다.
- 중간 - 위협 탐지와 오탐지 간의 균형을 제공합니다.
- 낮음 - 위협에 대한 가장 높은 탐지율을 제공하지만 오탐지도 증가시킵니다.

자세한 내용은 DNS 방화벽의 규칙 설정 단원을 참조하십시오.

DNS 방화벽 규칙 그룹과 VPC 간의 연결

DNS 방화벽 규칙 그룹을 사용하여 VPC 대한 보호를 정의하고 VPC에 대해 확인자 DNS 방화벽 구성을 활성화합니다.

여러 규칙 그룹을 단일 VPC 와 연결하는 경우 연결의 우선 순위 설정을 통해 처리 순서를 나타냅니다. DNS 방화벽은 우선 순위 설정에 따라 가장 낮은 숫자에서 높은 숫자 순으로 VPC 대한 규칙 그룹을 처리합니다.

자세한 내용은 VPC에 대해 Route 53 Resolver DNS 방화벽 보호 활성화 섹션을 참조하세요.

VPC 대한 Resolver DNS 방화벽 구성

Resolver가 VPC 수준에서 DNS 방화벽 보호를 처리하는 방법을 지정합니다. 이 구성은 VPC 와 연결된 DNS 방화벽 규칙 그룹이 하나 이상 있을 때마다 적용됩니다.

이 구성은 DNS 방화벽이 쿼리를 필터링하지 못할 때 Route 53 Resolver가 쿼리를 처리하는 방법을 지정합니다. 기본적으로 Resolver는 DNS 방화벽에서 쿼리에 대한 응답을 받지 못하면 닫히지 않고 쿼리를 차단합니다.

자세한 내용은 DNS 방화벽 VPC 구성 단원을 참조하십시오.

DNS 방화벽 작업 모니터링

Amazon CloudWatch를 사용하여 DNS 방화벽 규칙 그룹에 의해 필터링되는 DNS 쿼리 수를 모니터링할 수 있습니다. CloudWatch는 원시 데이터를 수집하여 실시간에 가까운 읽기 가능한 지표로 처리합니다.

자세한 내용은 Amazon CloudWatch 를 사용하여 Route 53 Resolver DNS 방화벽 규칙 그룹 모니터링 단원을 참조하십시오.

이벤트를 사용하여 애플리케이션 구성 요소를 서로 연결하는 서버리스 서비스인 Amazon EventBridge를 사용하여 확장 가능한 이벤트 기반 애플리케이션을 구축할 수 있습니다.

자세한 내용은 를 사용하여 Route 53 Resolver DNS 방화벽 이벤트 관리 Amazon EventBridge 단원을 참조하십시오.

Route 53 Resolver DNS 방화벽이 DNS 쿼리를 필터링하는 방법

DNS 방화벽 규칙 그룹이 VPC의 Route 53 Resolver와 연결되어 있으면 방화벽에서 다음 트래픽을 필터링합니다.

- 해당 VPC 내에서 시작되어 VPC DNS를 통과하는 DNS 쿼리입니다.
- Resolver 엔드포인트를 온프레미스 리소스에서 DNS 방화벽을 자체 해석기와 연결한 동일한 VPC로 전달하는 DNS 쿼리입니다.

DNS 방화벽은 DNS 쿼리를 수신하면 구성한 규칙 그룹, 규칙 및 기타 설정을 사용하여 쿼리를 필터링하고 결과를 다시 Resolver에 발송합니다.

- DNS 방화벽은 일치하는 항목을 찾거나 모든 규칙 그룹을 소진할 때까지 VPC와 연결된 규칙 그룹을 사용하여 DNS 쿼리를 평가합니다. DNS 방화벽은 가장 낮은 숫자 설정부터 시작하여 연결에서 설정한 우선 순위에 따라 규칙 그룹을 평가합니다. 자세한 내용은 DNS 방화벽 규칙 그룹 및 규칙 및 VPC에 대해 Route 53 Resolver DNS 방화벽 보호 활성화 단원을 참조하세요.
- 각 규칙 그룹 내에서 DNS 방화벽은 일치하는 항목을 찾거나 모든 규칙을 소진할 때까지 각 규칙의 도메인 목록 또는 DNS 방화벽 고급 보호에 대해 DNS 쿼리를 평가합니다. DNS 방화벽은 가장 낮은

숫자 설정부터 시작하여 우선 순위에 따라 규칙을 평가합니다. 자세한 내용은 DNS 방화벽 규칙 그룹 및 규칙 단원을 참조하십시오.

- DNS 방화벽이 규칙의 도메인 목록과 일치하는 항목 또는 DNS Firewall Advanced 규칙 보호로 식별되는 이상을 발견하면 쿼리 평가를 종료하고 Resolver에 결과와 함께 응답합니다. 작업이 `alert`인 경우 DNS 방화벽은 구성된 Resolver 로그에도 알림을 발송합니다. 자세한 내용은 DNS 방화벽의 규칙 동작, Route 53 Resolver DNS 방화벽 도메인 목록, Route 53 Resolver DNS 방화벽 고급 섹션을 참조하세요.
- DNS 방화벽이 일치 항목을 찾지 못하고 모든 규칙 그룹을 평가하는 경우 평소대로 쿼리에 응답합니다.

Resolver는 DNS 방화벽의 응답에 따라 쿼리를 라우팅합니다. 드물게 DNS 방화벽이 응답하지 않는 경우 Resolver는 VPC의 구성된 DNS 방화벽 오류 모드를 적용합니다. 자세한 내용은 DNS 방화벽 VPC 구성 섹션을 참조하세요.

Route 53 Resolver DNS 방화벽을 사용하기 위한 고수준 단계

Amazon Virtual Private Cloud(VPC)에서 Route 53 Resolver DNS 방화벽 필터링을 구현하려면 다음과 같은 고수준 단계를 수행합니다.

- 필터링 접근 방식, 도메인 목록 또는 DNS 방화벽 보호 정의 - 쿼리를 필터링하는 방법을 결정하고, 필요한 도메인 사양을 식별하고, 쿼리를 평가하는 데 사용할 로직을 정의합니다. 예를 들어 잘못된 것으로 알려진 도메인 목록에 있는 쿼리를 제외한 모든 쿼리를 허용해야 할 수 있습니다. 아니면 반대로 월드 가든(walled garden) 접근법으로 알려진 것처럼 승인된 도메인 목록을 제외한 모든 것을 차단하고 싶을 수도 있습니다. 승인되거나 차단된 도메인 사양의 자체 목록을 생성하고 관리할 수 있으며가 AWS 자동으로 관리하는 도메인 목록을 사용할 수 있습니다. DNS 방화벽 보호의 경우 쿼리를 모두 차단하여 필터링하거나 위협(DGA, DNS 터널링)과 관련된 이상을 포함할 수 있는 도메인에 대한 의심스러운 쿼리 트래픽을 경고하여 DNS 방화벽 설정을 테스트할 수 있습니다. 자세한 내용은 Route 53 Resolver DNS 방화벽 도메인 목록 및 Route 53 Resolver DNS 방화벽 고급 단원을 참조하세요.
- 방화벽 규칙 그룹 생성(Create a firewall rule group) - DNS 방화벽에서 VPC에 대한 DNS 쿼리를 필터링하는 규칙 그룹을 생성합니다. 사용할 각 리전에 규칙 그룹을 생성해야 합니다. 여러 VPC에 대한 여러 필터링 시나리오에서 재사용하기 위해 필터링 동작을 둘 이상의 규칙 그룹으로 분리하려 할 수도 있습니다. 규칙 그룹에 대한 자세한 내용은 DNS 방화벽 규칙 그룹 및 규칙 단원을 참조하세요.
- 규칙 추가 및 구성 - 규칙 그룹에서 제공할 각 도메인 목록과 필터링 동작에 대한 규칙을 규칙 그룹에 규칙을 추가합니다. 규칙 그룹 내에서 올바른 순서로 처리되도록 규칙의 우선 순위 설정을 설정하여

먼저 평가할 규칙에 가장 낮은 우선 순위를 지정합니다. 규칙에 대한 자세한 내용은 DNS 방화벽 규칙 그룹 및 규칙 단원을 참조하세요.

- VPC에 규칙 그룹 연결 - DNS 방화벽 규칙 그룹을 사용하려면 이를 VPC와 연결합니다. VPC에 대한 규칙 그룹을 두 개 이상 사용하는 경우 규칙 그룹이 올바른 순서로 처리되도록 각 연결의 우선 순위를 설정하여 먼저 평가할 규칙 그룹에 가장 낮은 우선 순위를 지정합니다. 자세한 내용은 VPC와 Route 53 Resolver DNS 방화벽 규칙 그룹 간의 연결 관리 섹션을 참조하세요.
- (선택 사항) VPC 대한 방화벽 구성 변경 - DNS 방화벽이 쿼리에 대한 응답을 다시 보내지 못할 때 Route 53 Resolver가 쿼리를 차단하도록 하려면 Resolver에서 VPC의 DNS 방화벽 구성을 변경합니다. 자세한 내용은 DNS 방화벽 VPC 구성 섹션을 참조하세요.

여러 리전에서 Route 53 Resolver DNS 방화벽 규칙 그룹 사용

Route 53 Resolver DNS 방화벽은 리전 서비스이므로 한 AWS 리전에서 생성한 객체는 해당 리전에서만 사용할 수 있습니다. 2개 이상 리전에서 동일한 규칙 그룹을 사용하려면 각 리전에서 규칙을 생성해야 합니다.

규칙 그룹을 생성한 AWS 계정은 다른 AWS 계정과 공유할 수 있습니다. 자세한 내용은 AWS 계정 간에 Route 53 Resolver DNS 방화벽 규칙 그룹 공유 단원을 참조하십시오.

Route 53 Resolver DNS 방화벽의 리전 가용성

DNS 방화벽은 AWS 리전다음에서 사용할 수 있습니다.

- 아프리카(케이프타운)
- 아시아 태평양(홍콩)
- 아시아 태평양(하이데라바드)
- 아시아 태평양(자카르타)
- 아시아 태평양(말레이시아)
- 아시아 태평양(멜버른)
- 아시아 태평양(뭄바이)
- Asia Pacific (Osaka) Region
- 아시아 태평양(서울)
- 아시아 태평양(싱가포르)
- 아시아 태평양(시드니)

- 아시아 태평양(도쿄)
- 캐나다(중부) 리전
- 캐나다 서부(캘거리)
- Europe (Frankfurt) Region
- Europe (Ireland) Region
- Europe (London) Region
- 유럽(밀라노)
- Europe (Paris) Region
- 유럽(스페인)
- 유럽(스톡홀름)
- 유럽(취리히)
- 이스라엘(텔아비브)
- 중동(바레인)
- 중동(UAE)
- 남아메리카(상파울루)
- 미국 동부(버지니아 북부)
- 미국 동부(오하이오)
- 미국 서부(캘리포니아 북부)
- 미국 서부(오리건)
- 중국(베이징)
- 중국(닝샤)
- AWS GovCloud (US)

Route 53 Resolver DNS 방화벽 시작하기

DNS 방화벽 콘솔에는 다음의 DNS 방화벽 시작하기 단계를 안내하는 마법사가 있습니다.

- 사용하려는 각 규칙 집합에 대한 규칙 그룹을 생성합니다.
- 각 규칙에 대해 검사할 도메인 목록을 채웁니다. 자체 도메인 목록을 생성하고 AWS 관리형 도메인 목록을 사용할 수 있습니다.

- 규칙 그룹을 이를 사용할 VPC에 연결합니다.

Route 53 Resolver DNS 방화벽 월드 가든(walled garden) 예제

이 자습서에서는 신뢰할 수 있는 선별한 도메인 그룹을 제외한 모든 그룹을 차단하는 규칙 그룹을 만듭니다. 이를 폐쇄형 플랫폼 또는 월드 가든(walled garden) 접근법이라고 합니다.

콘솔 마법사를 사용하여 DNS 방화벽 규칙 그룹을 구성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.

   탐색 창에서 DNS 방화벽을 선택하여 Amazon VPC 콘솔에서 DNS 방화벽 규칙 그룹 페이지를 엽니다. 계속해서 3단계를 진행합니다.

   - 또는 -

   에 로그인 AWS Management Console 하고를 엽니다.

   https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창의 DNS 방화벽 아래에서 규칙 그룹을 선택합니다.
3. 탐색 모음에서 규칙 그룹에 대한 리전을 선택합니다.
4. 규칙 그룹(Rule groups) 페이지에서 규칙 그룹 추가(Add rule group)를 선택합니다.
5. 규칙 그룹 이름에 **`WalledGardenExample`**을 입력합니다.

   필요에 따라 태그 섹션에 태그의 키-값 페어를 입력합니다. 태그를 사용하면 AWS 리소스를 구성하고 관리할 수 있습니다. 자세한 내용은 Amazon Route 53 리소스 태그 지정 단원을 참조하십시오.
6. 규칙 그룹 추가를 선택합니다.
7. WalledGardenExample 세부 정보 페이지에서 규칙 탭을 선택한 다음 규칙 추가를 선택합니다.
8. 규칙 세부 정보 창에서 **`BlockAll`** 규칙 이름을 입력합니다.
9. 도메인 목록(Domain list) 창에서 내 도메인 목록 추가(Add my own domain list)를 선택합니다.
10. 새 도메인 목록 선택 또는 생성(Choose or create a new domain list)에서 새 도메인 목록 생성(Create new domain list)을 선택합니다.
11. **`AllDomains`** 도메인 목록 이름 입력을 입력한 다음 줄마다 도메인 하나 입력 텍스트 상자에 별표 **`*`**를 입력합니다.

12. 도메인 리디렉션 설정의 경우 기본값을 수락하고 쿼리 유형 - 선택 사항은 비워둡니다.
13. 작업에 대해 BLOCK을 선택한 다음 보낼 응답을 기본 설정 NODATA로 남겨 둡니다.
14. 규칙 추가(Add rule)를 선택합니다. 규칙 BlockAll은 WalledGardenExample 페이지의 규칙 탭에 표시됩니다.
15. WalledGardenExample 페이지에서 규칙 추가를 선택하여 규칙 그룹에 두 번째 규칙을 추가합니다.
16. 규칙 세부 정보 창에서 **`AllowSelectDomains`** 규칙 이름을 입력합니다.
17. 도메인 목록(Domain list) 창에서 내 도메인 목록 추가(Add my own domain list)(Add my own domain list)를 선택합니다.
18. 새 도메인 목록 선택 또는 생성(Choose or create a new domain list)에서 새 도메인 목록 생성(Create new domain list)을 선택합니다.
19. **`ExampleDomains`** 도메인 목록 이름을 입력합니다.
20. 줄마다 도메인 하나 입력 텍스트 상자의 첫 번째 줄에 **`example.com`**을 입력하고 두 번째 줄에 **`example.org`**를 입력합니다.

    > **Note**
    >
    > 규칙을 하위 도메인에도 적용하려면 해당 도메인도 목록에 추가해야 합니다. 예를 들어 example.com의 모든 하위 도메인을 추가하려면 **`*.example.com`**을 목록에 추가합니다.

21. 도메인 리디렉션 설정의 경우 기본값을 수락하고 쿼리 유형 - 선택 사항은 비워둡니다.
22. 작업에 대해 ALLOW를 선택합니다.
23. 규칙 추가를 선택합니다. 규칙은 WalledGardenExample 페이지의 규칙 탭에 모두 표시됩니다.
24. WalledGardenExample 페이지의 규칙 탭에서 우선순위 열에 나열된 번호를 선택하고 새 번호를 입력하여 규칙 그룹의 규칙 평가 순서를 조정할 수 있습니다. DNS 방화벽은 가장 낮은 우선순위 설정에 따라 규칙을 평가하므로 우선순위가 가장 낮은 규칙이 첫 번째로 평가됩니다. 이 예제에서는 DNS 방화벽이 먼저 도메인 선택 목록에 대한 DNS 쿼리를 식별하고 허용한 다음 나머지 쿼리를 모두 차단합니다.

    AllowSelectDomains의 우선순위가 낮아지도록 규칙 우선순위를 조정합니다.

이제 특정 도메인 쿼리만 허용하는 규칙 그룹이 생겼습니다. 이를 사용하려면 필터링 동작을 사용할 VPC에 연결합니다. 자세한 내용은 VPC와 Route 53 Resolver DNS 방화벽 규칙 그룹 간의 연결 관리 섹션을 참조하세요.

Route 53 Resolver DNS 방화벽 차단 목록 예제

이 자습서에서는 악의적이라고 알려진 도메인을 차단하는 규칙 그룹을 생성합니다. 차단 목록의 도메인에 허용되는 DNS 쿼리 유형도 추가합니다. 규칙 그룹은 Route 53 Resolver에서 다른 모든 아웃바운드 DNS 요청을 허용합니다.

콘솔 마법사를 사용하여 DNS 방화벽 차단 목록을 구성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.

   탐색 창에서 DNS 방화벽을 선택하여 Amazon VPC 콘솔에서 DNS 방화벽 규칙 그룹 페이지를 엽니다. 계속해서 3단계를 진행합니다.

   - 또는 -

   에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/vpc/ Amazon VPC 콘솔을 엽니다.
2. 탐색 창의 DNS 방화벽 아래에서 규칙 그룹을 선택합니다.
3. 탐색 모음에서 규칙 그룹에 대한 리전을 선택합니다.
4. 규칙 그룹(Rule groups) 페이지에서 규칙 그룹 추가(Add rule group)를 선택합니다.
5. 규칙 그룹 이름에 **`BlockListExample`**을 입력합니다.

   필요에 따라 태그 섹션에 태그의 키-값 페어를 입력합니다. 태그를 사용하면 AWS 리소스를 구성하고 관리할 수 있습니다. 자세한 내용은 Amazon Route 53 리소스 태그 지정 단원을 참조하십시오.
6. BlockListExample 세부 정보 페이지에서 규칙 탭을 선택한 다음 규칙 추가를 선택합니다.
7. 규칙 세부 정보 창에서 **`BlockList`** 규칙 이름을 입력합니다.
8. 도메인 목록(Domain list) 창에서 내 도메인 목록 추가(Add my own domain list)(Add my own domain list)를 선택합니다.
9. 새 도메인 목록 선택 또는 생성(Choose or create a new domain list)에서 새 도메인 목록 생성(Create new domain list)을 선택합니다.
10. **`MaliciousDomains`** 도메인 목록 이름을 입력한 다음 텍스트 상자에 차단할 도메인을 입력합니다. 예: **`example.org`**. 줄마다 도메인 하나를 입력합니다.

> **Note**
>
> 규칙을 하위 도메인에도 적용하려면 해당 도메인도 목록에 추가해야 합니다. 예를 들어 example.org의 모든 하위 도메인을 추가하려면 **`*.example.org`**를 목록에 추가합니다.

11. 도메인 리디렉션 설정의 경우 기본값을 수락하고 쿼리 유형 - 선택 사항은 비워둡니다.
12. 작업에 대해 BLOCK을 선택한 다음 보낼 응답을 기본 설정 NODATA로 남겨 둡니다.
13. 규칙 추가(Add rule)를 선택합니다. 규칙은 BlockListExample 페이지의 규칙 탭에 표시됩니다.
14. BlockedListExample 페이지의 규칙 탭에서 우선순위 열에 나열된 번호를 선택하고 새 번호를 입력하여 규칙 그룹의 규칙 평가 순서를 조정할 수 있습니다. DNS 방화벽은 가장 낮은 우선순위 설정에 따라 규칙을 평가하므로 우선순위가 가장 낮은 규칙이 첫 번째로 평가됩니다.

    BlockList가 있을 수 있는 다른 모든 규칙 전이나 후에 평가되도록 규칙 우선순위를 선택하고 조정합니다. 대부분의 경우 알려진 악성 도메인은 먼저 차단해야 합니다. 즉, 해당 도메인과 관련된 규칙은 우선 순위가 가장 낮아야 합니다.
15. BlockList 도메인에 대한 MX 레코드를 허용하는 규칙을 추가하려면 규칙 탭의 BlockedListExample 세부 정보 페이지에서 규칙 추가를 선택합니다.
16. 규칙 세부 정보 창에서 **`BlockList-allowMX`** 규칙 이름을 입력합니다.
17. 도메인 목록(Domain list) 창에서 내 도메인 목록 추가(Add my own domain list)를 선택합니다.
18. 새 도메인 목록 선택 또는 생성에서 **`MaliciousDomains`**을 선택합니다.
19. 도메인 리디렉션 설정의 경우 기본값을 수락합니다.
20. DNS 쿼리 유형 목록에서 MX: 메일 서버 지정을 선택합니다.
21. 작업에 대해 ALLOW를 선택합니다.
22. 규칙 추가를 선택합니다.
23. BlockedListExample 페이지의 규칙 탭에서 우선순위 열에 나열된 번호를 선택하고 새 번호를 입력하여 규칙 그룹의 규칙 평가 순서를 조정할 수 있습니다. DNS 방화벽은 가장 낮은 우선순위 설정에 따라 규칙을 평가하므로 우선순위가 가장 낮은 규칙이 첫 번째로 평가됩니다.

    BlockList-allowMX가 있을 수 있는 다른 모든 규칙 전이나 후에 평가되도록 규칙 우선순위를 선택하고 조정합니다. MX 쿼리를 허용하려면 BlockList-allowMX 규칙의 우선순위가 BlockList보다 낮은지 확인합니다.

이제 특정 악성 도메인 쿼리를 차단하지만 특정 DNS 쿼리 유형은 허용하는 규칙 그룹이 생겼습니다. 이를 사용하려면 필터링 동작을 사용할 VPC에 연결합니다. 자세한 내용은 VPC와 Route 53 Resolver DNS 방화벽 규칙 그룹 간의 연결 관리 섹션을 참조하세요.

DNS 방화벽 규칙 그룹 및 규칙

이 섹션에서는 VPC의 DNS 방화벽 동작을 정의하기 위해 구성할 수 있는 DNS 방화벽 규칙 그룹 및 규칙의 설정을 설명합니다. 또한 규칙 그룹 및 규칙의 설정을 관리하는 방법에 대해서도 설명합니다.

규칙 그룹을 원하는 방식으로 구성한 경우 규칙 그룹을 직접 사용하고, 계정 간 및 AWS Organizations의 조직 간에 규칙 그룹을 공유하고 관리할 수 있습니다.

- 규칙 그룹을 여러 VPC와 연결하여 조직 전체에서 일관된 동작을 실행할 수 있습니다. 자세한 내용은 VPC와 Route 53 Resolver DNS 방화벽 규칙 그룹 간의 연결 관리을 참조하세요.
- 조직 전체에서 일관된 DNS 쿼리 관리를 위해 계정 간에 규칙 그룹을 공유할 수 있습니다. 자세한 내용은 AWS 계정 간에 Route 53 Resolver DNS 방화벽 규칙 그룹 공유을 참조하세요.
- AWS Firewall Manager 정책에서 규칙 그룹을 관리 AWS Organizations 하여에서 조직 전반의 규칙 그룹을 사용할 수 있습니다. Firewall ManagerAWS Firewall Manager에 대한 자세한 내용은 AWS WAF AWS Firewall Manager, 및 AWS Shield Advanced 개발자 안내서의 섹션을 참조하세요.

DNS 방화벽의 규칙 그룹 설정

DNS 방화벽 규칙을 생성하거나 편집할 때 다음 값을 지정합니다.

명칭

대시보드에서 규칙 그룹을 쉽게 찾을 수 있게 해 주는 고유한 이름입니다.

(선택 사항) 설명

규칙 그룹에 대한 추가 컨텍스트를 제공하는 간단한 설명입니다.

리전

규칙 그룹을 생성할 때 선택하는 AWS 리전입니다. 한 리전에서 생성한 규칙 그룹은 해당 리전에서만 사용할 수 있습니다. 2개 이상 리전에서 동일한 규칙 그룹을 사용하려면 리전마다 규칙 그룹을 생성해야 합니다.

규칙

규칙 그룹 필터링 동작은 해당 규칙에 포함되어 있습니다. 자세한 내용은 다음 섹션을 참조하세요.

Tags

한 개 이상의 키와 해당 값을 지정합니다. 예를 들어 키에 Cost center를 지정하고 값에 456을 지정할 수 있습니다.

청구서를 구성하기 AWS 위해에서 AWS Billing and Cost Management 제공하는 태그입니다. 비용 할당 태그 사용에 대한 자세한 내용은 AWS Billing 사용 설명서의 비용 할당 태그 사용을 참조하세요.

DNS 방화벽의 규칙 설정

DNS 방화벽 규칙 그룹을 생성하거나 편집할 때 다음 값을 지정합니다.

명칭

규칙 그룹의 규칙에 대한 고유 식별자입니다.

(선택 사항) 설명

규칙에 대한 자세한 정보를 제공하는 간단한 설명입니다.

도메인 목록

규칙이 검사하는 도메인 목록입니다. 자신의 도메인 목록을 만들고 관리하거나 AWS 에서 대신 관리하는 도메인 목록에 가입할 수 있습니다. 자세한 내용은 Route 53 Resolver DNS 방화벽 도메인 목록 단원을 참조하십시오.

규칙에는 도메인 목록 또는 DNS Firewall Advanced 보호가 포함될 수 있지만 둘 다 포함될 수는 없습니다.

도메인 리디렉션 설정(도메인 목록만 해당)

DNS 방화벽 규칙에서 CNAME, DNAME 등과 같은 DNS 리디렉션 체인의 첫 번째 도메인 또는 모든 도메인(기본값)만 검사하도록 선택할 수 있습니다. 모든 도메인을 검사하도록 선택한 경우 DNS 리디렉션 체인의 후속 도메인을 도메인 목록에 추가하고 규칙을 수행할 작업인 ALLOW, BLOCK 또는 ALERT로 설정해야 합니다. 자세한 내용은 Route 53 Resolver DNS 방화벽 구성 요소 및 설정 단원을 참조하십시오.

쿼리 유형(도메인 목록만 해당)

규칙이 검사하는 DNS 쿼리 유형의 목록입니다. 유효한 값은 다음과 같습니다.

- A: IPv4 주소를 반환합니다.
- AAAA: Ipv6 주소를 반환합니다.

- CAA: 도메인에 대한 SSL/TLS 인증을 생성할 수 있는 CA를 제한합니다.
- CNAME: 다른 도메인 이름을 반환합니다.
- DS: 위임된 영역의 DNSSEC 서명 키를 식별하는 레코드입니다.
- MX: 메일 서버를 지정합니다.
- NAPTR: 정규 표현식을 기반으로 도메인 이름을 다시 작성합니다.
- NS: 권한 이름 서버입니다.
- PTR: IP 주소를 도메인 이름에 매핑합니다.
- SOA: 해당 영역의 권한 레코드를 시작합니다.
- SPF: 도메인에서 이메일을 보낼 권한이 있는 서버를 나열합니다.
- SRV: 서버를 식별하는 애플리케이션별 값입니다.
- TXT: 이메일 발신자와 애플리케이션별 값을 확인합니다.
- AAAA의 경우 DNS 유형 ID(예: 28)를 사용하여 정의하는 쿼리 유형입니다. 값은 TYPE*NUMBER*로 정의되어야 합니다. 여기서 *NUMBER*는 1~65334, 예를 들어 TYPE28일 수 있습니다. 자세한 내용은 DNS 레코드 유형 목록을 참조하세요.

  규칙당 하나의 쿼리 유형을 생성할 수 있습니다.

  > **Note**
  >
  > 쿼리 유형에 대한 작업 NXDOMAIN이 AAAA와 동일한 방화벽 차단 규칙을 설정한 경우, DNS64가 활성화될 때 생성된 합성 IPv6 주소에는 이 작업이 적용되지 않습니다.

DNS 방화벽 고급 보호

DNS 쿼리에서 알려진 위협 서명을 기반으로 의심스러운 DNS 쿼리를 감지합니다. 다음 중에서 보호를 선택할 수 있습니다.

- 도메인 생성 알고리즘(DGAs)

  공격자는 DGAs를 사용하여 많은 수의 도메인을 생성하여 맬웨어 공격을 시작합니다.

- DNS 터널링

  DNS 터널링은 공격자가 클라이언트에 대한 네트워크 연결 없이 DNS 터널을 사용하여 클라이언트에서 데이터를 유출하는 데 사용됩니다.

DNS Firewall Advanced 규칙에서는 위협과 일치하는 쿼리를 차단하거나 경고하도록 선택할 수 있습니다.

자세한 내용은 Route 53 Resolver DNS 방화벽 고급 단원을 참조하십시오.

규칙에는 DNS Firewall Advanced 보호 또는 도메인 목록이 포함될 수 있지만 둘 다 포함될 수는 없습니다.

신뢰도 임계값(DNS Firewall Advanced만 해당)

DNS Firewall Advanced의 신뢰도 임계값입니다. DNS Firewall Advanced 규칙을 생성할 때이 값을 제공해야 합니다. 신뢰 수준 값은 다음을 의미합니다.

- 높음 - 오탐률이 낮은 가장 잘 확인된 위협만 탐지합니다.
- 중간 - 위협 탐지와 오탐지 간의 균형을 제공합니다.
- 낮음 - 위협에 대한 가장 높은 탐지율을 제공하지만 오탐지도 증가시킵니다.

자세한 내용은 DNS 방화벽의 규칙 설정 단원을 참조하십시오.

작업

도메인 이름이 규칙의 도메인 목록에 있는 사양과 일치하는 DNS 쿼리를 DNS 방화벽이 처리하도록 하는 방법입니다. 자세한 내용은 DNS 방화벽의 규칙 동작 섹션을 참조하세요.

우선순위

처리 순서를 결정하는 규칙 그룹 내의 규칙에 대한 고유한 양의 정수 설정입니다. DNS Firewall은 우선 순위가 가장 낮은 설정에서 높은 설정 순으로 규칙 그룹의 규칙에 대해 DNS 쿼리를 검사합니다. 처리 순서를 변경하거나 다른 규칙을 위한 공간을 확보하려면 언제든 규칙의 우선 순위를 변경할 수 있습니다.

DNS 방화벽의 규칙 동작

DNS 방화벽이 DNS 쿼리와 규칙의 도메인 사양 간에 일치하는 항목을 찾으면 규칙에 지정된 작업이 쿼리에 적용됩니다.

생성하는 각 규칙에서 다음 옵션 중 하나를 지정해야 합니다.

- Allow - 쿼리 검사를 중지하고 통과하도록 허용합니다. DNS Firewall Advanced에는 사용할 수 없습니다.
- Alert - 쿼리 검사를 중지하고 통과하도록 허용한 다음 Route 53 Resolver 로그에 쿼리 알림을 기록합니다.
- Block - 쿼리 검사를 중지하고, 의도한 대상으로 이동하지 못하도록 차단하고, 쿼리에 대한 차단 작업을 Route 53 Resolver 로그에 기록합니다.

다음과 같이 구성된 차단 응답으로 회신합니다.

- NODATA - 쿼리가 성공했지만 응답을 사용할 수 없음을 나타내는 응답입니다.
- NXDOMAIN - 쿼리의 도메인 이름이 존재하지 않음을 나타내는 응답입니다.
- OVERRIDE - 응답에서 사용자 지정을 재정의합니다. 이 옵션은 다음과 같은 추가 설정이 필요합니다.
  - Record value - 쿼리에 대한 응답으로 반송하는 사용자 지정 DNS 레코드입니다.
  - Record type - DNS 레코드의 유형입니다. 이렇게 하면 레코드 값의 형식을 결정할 수 있습니다. 반드시 `CNAME`이어야 합니다.
  - Time to live in seconds - DNS 해석기 또는 웹 브라우저에서 재정의 레코드를 캐시하고 다시 수신되는 경우 이 쿼리에 대한 응답으로 사용하기 위해 권장되는 시간입니다. 기본적으로 이 값은 `0`이며 레코드는 캐시되지 않습니다.

쿼리 로그 구성 및 내용에 대한 자세한 사항은 Resolver 쿼리 로깅 및 Resolver 쿼리 로그에 표시되는 값 섹션을 참조하세요.

Alert를 사용하여 차단 규칙 테스트

차단 규칙을 처음 만들 때 Alert로 설정된 작업으로 규칙을 구성하여 테스트할 수 있습니다. 그런 다음 규칙이 경고하는 쿼리 수를 확인하여 작업을 Block으로 설정한 경우 몇 개나 차단했는지 확인할 수 있습니다.

DNS 방화벽 규칙 그룹 및 규칙 관리

콘솔에서 규칙 그룹 및 규칙을 관리하려면 이 섹션의 지침을 따르세요.

규칙 및 도메인 목록과 같은 DNS 방화벽 엔터티를 변경하면 DNS Firewall은 엔터티가 저장되고 사용되는 모든 곳에 변경 사항을 전파합니다. 변경 사항은 몇 초 이내에 적용되지만 변경 사항이 한 위치에는 적용되었는데 다른 위치에는 아직 적용되지 않았을 때 짧은 불일치 기간이 있을 수도 있습니다. 예를 들어, 차단 규칙에서 참조하는 도메인 목록에 도메인을 추가하는 경우 새 도메인이 VPC의 한 영역에서는 짧게 차단되는데 다른 영역에서 계속 허용될 수도 있습니다. 이러한 일시적인 불일치는 규칙 그룹 및 VPC 연결을 처음 구성할 때와 기존 설정을 변경할 때 발생할 수 있습니다. 일반적으로 이러한 유형의 불일치는 몇 초 동안만 일어납니다.

규칙 그룹 및 규칙 생성

규칙 그룹을 생성하고 규칙을 추가하려면 이 절차의 단계를 따릅니다.

규칙 그룹 및 규칙을 생성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.

   탐색 창에서 DNS 방화벽을 선택하여 Amazon VPC 콘솔에서 DNS 방화벽 규칙 그룹 페이지를 엽니다. 계속해서 3단계를 진행합니다.

   - 또는 -

   에 로그인 AWS Management Console 하고를 엽니다.

   https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창의 DNS 방화벽 아래에서 규칙 그룹을 선택합니다.
3. 탐색 모음에서 규칙 그룹에 대한 리전을 선택합니다.
4. 규칙 그룹 추가(Add rule group)를 선택한 다음, 마법사 지침에 따라 규칙 그룹 및 규칙 설정을 지정합니다.

   전달 규칙의 값에 대한 자세한 내용은 DNS 방화벽의 규칙 그룹 설정을 참조하세요.

   전달 규칙의 값에 대한 자세한 내용은 DNS 방화벽의 규칙 설정을 참조하세요.

규칙 그룹 및 규칙 보기 및 갱신

다음 절차에 따라 규칙 그룹과 할당된 규칙을 볼 수 있습니다. 규칙 그룹 및 규칙 설정을 업데이트할 수도 있습니다.

규칙 그룹을 보고 업데이트하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.

   탐색 창에서 DNS 방화벽을 선택하여 Amazon VPC 콘솔에서 DNS 방화벽 규칙 그룹 페이지를 엽니다. 계속해서 3단계를 진행합니다.

   - 또는 -

   에 로그인 AWS Management Console 하고를 엽니다.

   https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.

2. 탐색 창의 DNS 방화벽 아래에서 규칙 그룹을 선택합니다.
3. 탐색 모음에서 규칙 그룹에 대한 리전을 선택합니다.
4. 보거나 편집할 규칙 그룹을 선택한 다음 세부 정보 보기(View details)를 선택합니다.
5. 규칙 그룹의 페이지에서 설정을 보고 편집할 수 있습니다.

   전달 규칙의 값에 대한 자세한 내용은 DNS 방화벽의 규칙 그룹 설정을 참조하세요.

   전달 규칙의 값에 대한 자세한 내용은 DNS 방화벽의 규칙 설정을 참조하세요.

규칙 그룹 삭제

전달 규칙을 삭제하려면 다음 절차를 수행하세요.

> **Important**
>
> VPC PC와 연결된 규칙 그룹을 삭제하면 DNS 방화벽이 연결을 제거하고 규칙 그룹이 VPC에 제공한 보호를 중지합니다.

DNS 방화벽 엔터티 삭제

규칙 그룹에서 사용할 수 있는 도메인 목록이나 VPC와 연결할 수 있는 규칙 그룹과 같은 DNS 방화벽에서 사용할 수 있는 엔티티를 삭제하는 경우 DNS 방화벽은 해당 엔티티가 현재 사용 중인지 확인합니다. 사용 중인 것으로 확인되면 DNS 방화벽에서 경고를 표시합니다. DNS 방화벽은 거의 항상 엔터티가 사용 중인지 확인할 수 있습니다. 그러나 드물지만 이러한 작업을 수행할 수 없는 경우도 있습니다. 현재 아무 것도 엔터티를 사용하고 있지 않다는 것을 확인해야 하는 경우 해당 엔티티를 삭제하기 전에 해당 DNS 방화벽 구성에서 확인하세요. 엔터티가 참조된 도메인 목록인 경우에도 어떤 규칙 그룹도 해당 엔티티를 사용하고 있지 않음을 확인합니다. 엔터티가 규칙 그룹인 경우 해당 엔터티가 VPC와 연결되어 있지 않은지 확인합니다.

규칙 그룹을 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.

   탐색 창에서 DNS 방화벽을 선택하여 Amazon VPC 콘솔에서 DNS 방화벽 규칙 그룹 페이지를 엽니다. 계속해서 3단계를 진행합니다.

   - 또는 -

에 로그인 AWS Management Console 하고를 엽니다.

https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.

2. 탐색 창의 DNS 방화벽 아래에서 규칙 그룹을 선택합니다.
3. 탐색 모음에서 규칙 그룹에 대한 리전을 선택합니다.
4. 삭제하려는 규칙 그룹을 선택한 다음 삭제(Delete)를 선택하고 삭제를 확인합니다.

Route 53 Resolver DNS 방화벽 도메인 목록

도메인 목록(domain list)은 규칙 그룹 내부의 DNS 방화벽 규칙에서 사용하는 재사용 가능한 도메인 사양 집합입니다. 규칙 그룹을 VPC 와 연결하면 DNS 방화벽은 규칙에 사용되는 도메인 목록과 DNS 쿼리를 비교합니다. 일치하는 항목을 찾으면 일치 규칙의 작업에 따라 DNS 쿼리를 처리합니다. 규칙 그룹에 대한 자세한 내용은 DNS 방화벽 규칙 그룹 및 규칙 섹션을 참조하세요.

도메인 목록을 사용하면 명시적 도메인 사양을 해당 항목에 대해 수행하려는 작업과 구분할 수 있습니다. 여러 규칙에서 단일 도메인 목록을 사용할 수 있으며 도메인 목록에 대한 업데이트는 해당 도메인 목록을 사용하는 모든 규칙에 자동으로 영향을 줍니다.

도메인 목록은 두 가지 주요 범주로 나뉩니다.

- 가 자동으로 AWS 생성하고 유지 관리하는 관리형 도메인 목록입니다.
- 사용자가 생성하고 유지 관리하는 자체 도메인 목록입니다.

이 섹션에서는 사용자에게 제공되는 관리형 도메인 목록의 유형에 대해 설명하고 사용자가 원할 경우 자체 도메인 목록을 생성하고 관리하도록 필요한 지침을 제공합니다.

관리형 도메인 목록

관리형 도메인 목록에는 악의적인 활동 또는 기타 잠재적 위협과 연결된 도메인 이름이 포함되어 있습니다.는 이러한 목록을 AWS 유지 관리하여 Route 53 Resolver 고객이 DNS 방화벽을 사용할 때 아웃바운드 DNS 쿼리를 무료로 확인할 수 있도록 합니다.

끊임없이 변화하는 위협 환경을 놓치지 않고 파악하려면 많은 시간과 비용이 들 수 있습니다. 관리형 도메인 목록은 DNS Firewall을 구현하고 사용할 때 시간을 절약할 수 있습니다.는 새로운 취약성 및 위협이 발생할 때 목록을 AWS 자동으로 업데이트합니다. AWS 는 종종 공개 전에 새로운 취약성에 대해 알림을 받기 때문에 DNS 방화벽은 새로운 위협이 널리 알려지기 전에 완화 조치를 자주 배포할 수 있습니다.

관리형 도메인 목록은 일반적인 웹 위협으로부터 사용자를 보호하도록 설계되었으며 애플리케이션에 대한 또 다른 보안 계층을 추가해 줍니다. AWS 관리형 도메인 목록은 내부 소스와 RecordedFuture 모두에서 데이터를 AWS 소싱하며 지속적으로 업데이트됩니다. 그러나 AWS 관리형 도메인 목록은 선택한 AWS 리소스에 따라 결정 Amazon GuardDuty되는와 같은 다른 보안 제어를 대체하기 위한 것이 아닙니다.

프로덕션 환경에서 관리형 도메인 목록을 사용하기 전에 규칙 작업을 `Alert`로 설정하여 비프로덕션 환경에서 테스트하는 것이 가장 좋습니다. Route 53 Resolver DNS 방화벽 샘플 요청 또는 DNS 방화벽 로그와 결합된 Amazon CloudWatch 지표를 사용하여 규칙을 평가합니다. 규칙이 원하는 대로 수행되는 것에 만족하면 필요에 따라 작업 설정을 변경합니다.

사용 가능한 AWS 관리형 도메인 목록

이 섹션에서는 현재 사용할 수 있는 관리형 도메인 목록을 설명합니다. 이러한 목록이 지원되는 리전에 있는 경우 도메인 목록을 관리할 때와 규칙에 대한 도메인 목록을 지정할 때 도메인 목록이 콘솔에 표시됩니다. 로그에서 도메인 목록은 `firewall_domain_list_id field` 내에 기록됩니다.

AWS 는 사용 가능한 리전에서 Route 53 Resolver DNS 방화벽의 모든 사용자에게 다음과 같은 관리형 도메인 목록을 제공합니다.

- `AWSManagedDomainsMalwareDomainList` -- 맬웨어 전송, 맬웨어 호스팅 또는 맬웨어 배포와 관련된 도메인입니다.
- `AWSManagedDomainsBotnetCommandandControl` - 스팸 맬웨어에 감염된 컴퓨터의 네트워크 제어와 관련된 도메인입니다.
- `AWSManagedDomainsAggregateThreatList` - 멀웨어, 랜섬웨어, 봇넷, 스파이웨어 및 DNS 터널링을 포함한 여러 DNS 위협 범주와 연결된 도메인으로, 여러 유형의 위협을 차단하는 데 도움이 됩니다.는 여기에 나열된 다른 AWS 관리형 도메인 목록에 있는 모든 도메인을 `AWSManagedDomainsAggregateThreatList` 포함합니다.
- `AWSManagedDomainsAmazonGuardDutyThreatList`— Amazon GuardDuty DNS 보안 탐지 결과와 관련된 도메인. 도메인은 GuardDuty의 위협 인텔리전스 시스템에서만 제공되며 외부 서드 파티 소스에서 가져온 도메인은 포함되지 않습니다. 더 구체적으로, 현재 이 목록은 GuardDuty에서 내부적으로 생성되고 다음 탐지에 사용되는 도메인만 차단합니다. Impact:EC2/AbusedDomainRequest.Reputation, Impact:EC2/BitcoinDomainRequest.Reputation, Impact:EC2/MaliciousDomainRequest.Reputation, Impact:Runtime/AbusedDomainRequest.Reputation, Impact:Runtime/BitcoinDomainRequest.Reputation, Impact:Runtime/MaliciousDomainRequest.Reputation.

  자세한 내용은 Amazon GuardDuty 사용 설명서의 유형 찾기를 참조하세요.

AWS 관리형 도메인 목록은 다운로드하거나 찾아볼 수 없습니다. 지적 재산을 보호하기 위해 AWS 관리형 도메인 목록 내에서 개별 도메인 사양을 보거나 편집할 수 없습니다. 이러한 제한을 통해 악의적인 사용자가 게시된 목록을 교묘하게 회피하는 위협을 설계하지 못하도록 할 수 있습니다.

관리형 도메인 목록을 테스트하려면

관리형 도메인 목록을 테스트할 수 있도록 다음과 같은 도메인 세트를 제공합니다.

AWSManagedDomainsBotnetCommandandControl

- controldomain1.botnetlist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain2.botnetlist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain3.botnetlist.firewall.route53resolver.us-east-1.amazonaws.com

AWSManagedDomainsMalwareDomainList

- controldomain1.malwarelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain2.malwarelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain3.malwarelist.firewall.route53resolver.us-east-1.amazonaws.com

AWSManagedDomainsAggregateThreatList 및 AWSManagedDomainsAmazonGuardDutyThreatList

- controldomain1.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain2.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com
- controldomain3.aggregatelist.firewall.route53resolver.us-east-1.amazonaws.com

이러한 도메인은 차단되지 않은 경우 1.2.3.4로 확인됩니다. VPC에서 관리형 도메인 목록을 사용하는 경우 이러한 도메인을 쿼리하면 규칙의 차단 조치가 설정된 응답(예: NODATA)이 반환됩니다.

관리형 도메인 목록에 대한 자세한 내용은 AWS Support 센터에 문의하세요.

다음 표에는 AWS 관리형 도메인 목록의 리전 가용성이 나열되어 있습니다.

관리형 도메인 목록 리전 가용성

리전	관리형 도메인 목록을 사용할 수 있습니까?
아프리카(케이프타운)	예
아시아 태평양(홍콩)	예

리전	관리형 도메인 목록을 사용할 수 있습니까?
아시아 태평양(하이데라바드)	예
아시아 태평양(자카르타)	예
아시아 태평양(말레이시아)	예
아시아 태평양(멜버른)	예
아시아 태평양(뭄바이)	예
Asia Pacific (Osaka) Region	예
아시아 태평양(서울)	예
아시아 태평양(싱가포르)	예
아시아 태평양(시드니)	예
아시아 태평양(도쿄)	예
캐나다(중부) 리전	예
캐나다 서부(캘거리)	예
Europe (Frankfurt) Region	예
Europe (Ireland) Region	예

리전	관리형 도메인 목록을 사용할 수 있습니까?
Europe (London) Region	예
유럽(밀라노)	예
Europe (Paris) Region	예
유럽(스페인)	예
유럽(스톡홀름)	예
유럽(취리히)	예
이스라엘(텔아비브)	예
중동(바레인)	예
중동(UAE)	예
남아메리카(상파울루)	예
미국 동부(버지니아 북부)	예
미국 동부(오하이오)	예
미국 서부(캘리포니아 북부)	예
미국 서부(오리건)	예

리전	관리형 도메인 목록을 사용할 수 있습니까?
중국(베이징)	예
중국(닝샤)	예
AWS GovCloud (US)	예

추가 보안 고려 사항

AWS 관리형 도메인 목록은 일반적인 웹 위협으로부터 사용자를 보호하도록 설계되었습니다. 설명서에 따라 사용할 경우 이러한 목록에는 애플리케이션에 대한 또 다른 보안 계층이 추가됩니다. 그러나 관리형 도메인 목록은 사용자가 선택한 AWS 리소스에 따라 결정되는 보안 컨트롤을 대체하기 위한 것이 아닙니다. 의 리소스 AWS 가 제대로 보호되도록 하려면 공동 책임 모델의 지침을 참조하세요.

거짓 긍정 시나리오 완화

쿼리를 차단하기 위해 관리형 도메인 목록을 사용하는 규칙에서 거짓 긍정 시나리오가 발생하는 경우 다음 단계를 수행합니다.

1. Resolver 로그에서 거짓 긍정을 일으키는 규칙 그룹 및 관리형 도메인 목록을 식별합니다. 이렇게 하려면 DNS 방화벽이 차단하고 있지만 허용하려는 쿼리에 대한 로그를 찾습니다. 로그 레코드에는 규칙 그룹, 규칙 작업 및 관리형 목록이 나열됩니다. 로그에 대한 자세한 내용은 Resolver 쿼리 로그에 표시되는 값 섹션을 참조하세요.
2. 차단된 쿼리를 명시적으로 허용하는 규칙 그룹에 새 규칙을 생성합니다. 규칙을 만들 때 허용하려는 도메인 사양만 사용하여 자체 도메인 목록을 정의할 수 있습니다. 규칙 그룹 및 규칙 생성에 있는 규칙 그룹 및 규칙 관리에 대한 지침을 따르세요.
3. 관리형 목록을 사용하는 규칙보다 먼저 실행되도록 규칙 그룹 내에서 새 규칙의 우선 순위를 지정합니다. 이렇게 하려면 새 규칙에 더 낮은 숫자의 우선 순위 설정을 부여합니다.

규칙 그룹을 업데이트하면 새 규칙은 차단 규칙이 실행되기 전에 허용할 도메인 이름을 명시적으로 허용합니다.

자체 도메인 목록 관리

자체 도메인 목록을 생성하여 관리형 도메인 목록에서 찾을 수 없거나 직접 처리하는 것을 선호하는 도메인 범주를 지정할 수 있습니다.

이 섹션의 콘솔에서 설명하는 절차 외에도 규칙을 만들거나 업데이트할 때 Route 53 Resolver DNS 방화벽 규칙 관리 컨텍스트에서 도메인 목록을 만들 수 있습니다.

도메인 목록의 각 도메인 사양은 다음 요구 사항을 충족해야 합니다.

- 필요에 따라 *(별표)로 시작할 수 있습니다.
- 필요에 따른 시작 별표와 마침표를 제외하고 `A-Z`, `a-z`, `0-9`, `-`(하이픈)과 같은 문자만 포함해야 합니다.
- 1~255자 길이여야 합니다.

규칙 및 도메인 목록과 같은 DNS 방화벽 엔터티를 변경하면 DNS Firewall은 엔터티가 저장되고 사용되는 모든 곳에 변경 사항을 전파합니다. 변경 사항은 몇 초 이내에 적용되지만 변경 사항이 한 위치에는 적용되었는데 다른 위치에는 아직 적용되지 않았을 때 짧은 불일치 기간이 있을 수도 있습니다. 예를 들어, 차단 규칙에서 참조하는 도메인 목록에 도메인을 추가하는 경우 새 도메인이 VPC의 한 영역에서는 짧게 차단되는데 다른 영역에서 계속 허용될 수도 있습니다. 이러한 일시적인 불일치는 규칙 그룹 및 VPC 연결을 처음 구성할 때와 기존 설정을 변경할 때 발생할 수 있습니다. 일반적으로 이러한 유형의 불일치는 몇 초 동안만 일어납니다.

프로덕션 환경에서 사용하기 전에 도메인 목록을 테스트하세요.

프로덕션 환경에서 도메인 목록을 사용하기 전에 규칙 작업을 `Alert`로 설정하여 비프로덕션 환경에서 테스트하는 것이 가장 좋습니다. Amazon CloudWatch 지표 및 Resolver 로그를 사용하여 규칙을 평가합니다. 로그는 모든 경고 및 차단 작업에 대한 도메인 목록 이름을 제공합니다. 도메인 목록이 원하는 방식으로 DNS 쿼리와 일치하는 것이 만족스러우면 필요에 따라 규칙 작업 설정을 변경합니다. CloudWatch 지표 및 쿼리 로그에 대한 자세한 내용은 Amazon CloudWatch 를 사용하여 Route 53 Resolver DNS 방화벽 규칙 그룹 모니터링, Resolver 쿼리 로그에 표시되는 값, 및 Resolver 쿼리 로깅 구성 관리 섹션을 참조하세요.

도메인 목록을 추가하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.

탐색 창에서 DNS 방화벽을 선택하여 Amazon VPC 콘솔에서 DNS 방화벽 규칙 그룹 페이지를 엽니다. 계속해서 2단계를 진행합니다.

- 또는 -

에 로그인 AWS Management Console 하고를 엽니다.

https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.

2. 탐색 창에서 DNS 방화벽 아래에서 도메인 목록을 선택합니다. 도메인 목록(Domain lists) 페이지에서 기존 도메인 목록을 선택하고 편집할 수 있으며 자신의 도메인 목록을 추가할 수도 있습니다.
3. 도메인 목록을 추가하려면 도메인 목록 추가(Domain lists)를 선택합니다.
4. 도메인 목록의 이름을 입력한 다음 텍스트 상자에 한 줄에 하나씩 도메인 사양을 입력합니다.

   대량 업로드로 전환(Switch to bulk upload)을 켜는 경우 도메인 목록을 생성한 Amazon S3 버킷의 URI를 입력합니다. 이 도메인 목록에는 한 줄에 하나씩 도메인 이름이 있어야 합니다.

   > **Note**
   >
   > 도메인 이름이 중복되면 대량 가져오기가 실패합니다.

5. 도메인 목록 추가(Add Domain lists)를 선택합니다. 도메인 목록(Domain lists) 페이지에는 새 도메인 목록이 나열됩니다.

도메인 목록을 만들면 DNS 방화벽 규칙에서 이름을 기준으로 도메인 목록을 참조할 수 있습니다.

DNS 방화벽 엔터티 삭제

규칙 그룹에서 사용할 수 있는 도메인 목록이나 VPC와 연결할 수 있는 규칙 그룹과 같은 DNS 방화벽에서 사용할 수 있는 엔티티를 삭제하는 경우 DNS 방화벽은 해당 엔티티가 현재 사용 중인지 확인합니다. 사용 중인 것으로 확인되면 DNS 방화벽에서 경고를 표시합니다. DNS 방화벽은 거의 항상 엔터티가 사용 중인지 확인할 수 있습니다. 그러나 드물지만 이러한 작업을 수행할 수 없는 경우도 있습니다. 현재 아무 것도 엔터티를 사용하고 있지 않다는 것을 확인해야 하는 경우 해당 엔티티를 삭제하기 전에 해당 DNS 방화벽 구성에서 확인하세요. 엔터티가 참조된 도메인 목록인 경우에도 어떤 규칙 그룹도 해당 엔티티를 사용하고 있지 않음을 확인합니다. 엔터티가 규칙 그룹인 경우 해당 엔터티가 VPC와 연결되어 있지 않은지 확인합니다.

도메인 목록을 삭제하려면

1. 탐색 창에서 도메인 목록(Domain lists)을 선택합니다.
2. 탐색 모음에서 도메인 목록에 해당하는 리전을 선택합니다.
3. 삭제하려는 도메인 목록을 선택한 다음 삭제(Delete)를 선택하고 삭제를 확인합니다.

Route 53 Resolver DNS 방화벽 고급

DNS Firewall Advanced는 DNS 쿼리에서 알려진 위협 서명을 기반으로 의심스러운 DNS 쿼리를 감지합니다. DNS 방화벽 규칙에서 사용하는 규칙의 규칙 그룹 내에서 위협 유형을 지정할 수 있습니다. 규칙 그룹을 VPC와 연결하면 DNS 방화벽은 DNS 쿼리를 규칙에 플래그가 지정된 도메인과 비교합니다. 일치하는 항목을 찾으면 일치 규칙의 작업에 따라 DNS 쿼리를 처리합니다.

DNS Firewall Advanced는 요청 타임스탬프, 요청 및 응답 빈도, DNS 쿼리 문자열, 아웃바운드 및 인바운드 DNS 쿼리의 길이, 유형 또는 크기를 포함하여 DNS 페이로드의 다양한 키 식별자를 검사하여 의심스러운 DNS 위협 서명을 식별하여 작동합니다. 위협 서명 유형에 따라 차단하도록 정책을 구성하거나 쿼리를 로깅하고 알릴 수 있습니다. 확장된 위협 식별자 세트를 사용하면 더 광범위한 보안 커뮤니티에서 유지 관리하는 위협 인텔리전스 피드로 아직 분류되지 않을 수 있는 도메인 소스의 DNS 위협으로부터 보호할 수 있습니다.

현재 DNS Firewall Advanced는 다음과 같은 보호 기능을 제공합니다.

- 도메인 생성 알고리즘(DGAs)

  공격자는 DGAs를 사용하여 많은 수의 도메인을 생성하여 맬웨어 공격을 시작합니다.
- DNS 터널링

  DNS 터널링은 공격자가 클라이언트에 대한 네트워크 연결 없이 DNS 터널을 사용하여 클라이언트에서 데이터를 유출하는 데 사용됩니다.

규칙을 생성하는 방법을 알아보려면 규칙 그룹 및 규칙 생성 및 섹션을 참조하세요DNS 방화벽의 규칙 설정.

DNS 방화벽에 대한 로깅 구성

Amazon CloudWatch 지표와 Resolver 쿼리 로그를 사용하여 DNS 방화벽 규칙을 평가할 수 있습니다. 로그는 모든 경고 및 차단 작업에 대한 도메인 목록 이름을 제공합니다. Amazon CloudWatch에 대한

자세한 내용은 Amazon CloudWatch 를 사용하여 Route 53 Resolver DNS 방화벽 규칙 그룹 모니터링 섹션을 참조하세요.

DNS 방화벽을 활성화하여 VPC에 연결하고 로깅을 사용하도록 설정한 경우 `firewall_rule_group_id`, `firewall_rule_action` 및 `firewall_domain_list_id`는 로그 내에 제공되는 DNS 방화벽 관련 필드입니다.

> **Note**
>
> 쿼리 로그의 추가 DNS 방화벽 필드에는 DNS 방화벽 규칙으로 차단된 쿼리만 표시됩니다.

VPC에서 시작되는 DNS 방화벽 규칙으로 필터링하는 DNS 쿼리 로깅을 시작하려면 Amazon Route 53 콘솔에서 다음 태스크를 수행합니다.

DNS 방화벽에 대한 Resolver 쿼리 로깅을 구성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. Route 53 콘솔 메뉴를 확장합니다. 콘솔의 왼쪽 상단 모서리에서 세 개의 가로 막대 (☰) 아이콘을 선택합니다.
3. Resolver 메뉴에서쿼리 로깅(Query logging)을 선택합니다.
4. 리전 선택기에서 쿼리 로깅 구성을 생성할 AWS 리전을 선택합니다.

   이 리전은 쿼리를 로그하려는 DNS 방화벽과 연결된 VPC를 생성한 리전과 동일해야 합니다. 여러 리전에 VPC가 있는 경우 리전별로 쿼리 로깅 구성을 하나 이상 생성해야 합니다.
5. 쿼리 로깅 구성(Configure query logging)을 선택합니다.
6. 다음 값을 지정하세요.

   쿼리 로깅 구성 이름

   쿼리 로깅 구성의 이름을 입력합니다. 이 이름은 쿼리 로깅 구성 목록의 콘솔에 표시됩니다. 나중에 이 구성을 찾는 데 도움이 되는 이름을 입력합니다.

쿼리 로그 대상

Resolver가 쿼리 로그를 전송할 AWS 리소스 유형을 선택합니다. 옵션(CloudWatch Logs 로그 그룹, S3 버킷, Kinesis Data Firehose 전송 스트림) 중에서 선택하는 방법에 대한 자세한 내용은 AWS Resolver 쿼리 로그를 보낼 수 있는 리소스 섹션을 참조하세요.

리소스 유형을 선택한 후 해당 유형의 다른 리소스를 생성하거나 현재 AWS 계정에서 생성한 기존 리소스를 선택할 수 있습니다.

> **Note**
>
> 쿼리 로깅 구성을 만드는 리전, 곧 4단계에서 선택한 AWS 리전에서 생성된 리소스만 선택할 수 있습니다. 새 리소스를 생성하도록 선택하면 해당 리소스가 동일한 리전에서 생성됩니다.

쿼리를 로그할 VPC

이 쿼리 로깅 구성은 선택한 VPC에서 시작된 DNS 쿼리를 로그합니다. 해석기에서 쿼리를 로그할 현재 리전에서 각 VPC에 대한 확인란을 선택한 다음 선택을 선택합니다.

> **Note**
>
> VPC 로그 전송은 특정 대상 유형에 대해 한 번만 사용할 수 있습니다. 로그는 동일한 유형의 여러 대상으로 전송될 수 없습니다. 예를 들어, VPC 로그는 두 개의 Amazon S3 대상으로 전송될 수 없습니다.

7. 쿼리 로깅 구성(Configure query logging)을 선택합니다.

> **Note**
>
> 쿼리 로깅 구성을 생성한 후 몇 분 내에 VPC의 리소스가 만든 DNS 쿼리를 로그에서 확인할 있어야 합니다.

AWS 계정 간에 Route 53 Resolver DNS 방화벽 규칙 그룹 공유

AWS 계정 간에 DNS 방화벽 규칙 그룹을 공유할 수 있습니다. 규칙 그룹을 공유하려면 AWS Resource Access Manager ()를 사용합니다AWS RAM. DNS 방화벽 콘솔은 AWS RAM 콘솔과 통합됩니다. 에 대한 자세한 내용은 Resource Access Manager 사용 설명서를 AWS RAM참조하세요.

다음 사항에 유의하세요.

공유된 규칙 그룹을 VPC에 연결

다른 AWS 계정이 계정과 규칙 그룹을 공유한 경우 생성한 규칙 그룹을 연결하는 것과 동일한 방식으로 VPCs와 연결할 수 있습니다. 자세한 내용은 VPC와 Route 53 Resolver DNS 방화벽 규칙 그룹 간의 연결 관리 단원을 참조하십시오.

공유된 규칙 그룹 삭제 또는 공유 해제

규칙 그룹을 다른 계정과 공유한 다음 규칙 그룹을 삭제하거나 공유를 중지하는 경우 DNS 방화벽은 규칙 그룹과 해당 VPC 간에 다른 계정이 생성한 모든 연결을 제거합니다.

규칙 그룹 및 연결에 대한 최대 설정

공유된 규칙 그룹 및 VPC와의 연결은 규칙 그룹이 공유되는 계정의 수에 포함됩니다.

현재 DNS 방화벽 할당량은 Route 53 Resolver DNS 방화벽의 할당량 섹션을 참조하세요.

권한

규칙 그룹을 다른 AWS 계정과 공유하려면 PutFirewallRuleGroupPolicy 작업을 사용할 권한이 있어야 합니다.

규칙 그룹이 공유되는 AWS 계정에 대한 제한 사항

규칙 그룹이 공유되는 계정은 규칙 그룹을 변경하거나 삭제할 수 없습니다.

태그 지정

규칙 그룹을 생성한 계정만 규칙 그룹의 태그를 추가하거나 삭제하거나 볼 수 있습니다.

규칙 그룹의 현재 공유 상태를 보고(규칙 그룹을 공유한 계정 또는 규칙 그룹이 공유되는 계정 포함) 규칙 그룹을 다른 계정과 공유하려면 다음 절차를 수행하세요.

공유 상태를 보고 규칙 그룹을 다른 AWS 계정과 공유하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.

2. 탐색 창에서 Rule groups(규칙 그룹)를 선택합니다.
3. 탐색 모음에서 규칙 그룹을 생성한 리전을 선택합니다.

   현재 계정이 생성하거나 현재 계정과 공유되는 규칙 그룹의 현재 공유 상태가 Sharing status(공유 상태) 열에 표시됩니다.

   - 공유되지 않음: 현재 AWS 계정이 규칙 그룹을 생성했으며 규칙 그룹이 다른 계정과 공유되지 않습니다.
   - 나와 공유됨(Shared by me): 현재 계정이 규칙 그룹을 생성하고 하나 이상의 계정과 공유했습니다.
   - 나와 공유 상태(Shared with me): 다른 계정이 규칙 그룹을 생성하고 현재 계정과 공유했습니다.
4. 공유 정보를 표시하거나 다른 계정과 공유할 규칙 그룹의 이름을 선택합니다.

   규칙 그룹(Rule group): ***## ## ##(rule group name)*** 페이지에서 소유자(Owner) 아래의 값은 규칙 그룹을 생성한 계정의 ID를 나타냅니다. Sharing status(공유 상태)의 값이 나와 공유 상태가 아닐 경우 현재 계정입니다. 이 경우 소유자(Owner)는 규칙 그룹을 생성하고 현재 계정과 공유한 계정입니다.
5. 공유(Share)를 선택하여 추가 정보를 보거나 규칙 그룹을 다른 계정과 공유합니다. 공유 상태의 값에 따라 AWS RAM 콘솔에 페이지가 나타납니다.

   - 공유하지 않음: 리소스 공유 생성 페이지가 표시됩니다. 규칙 그룹을 다른 계정, 조직 단위(OU) 또는 조직과 공유하는 방법에 대한 자세한 내용은 이 단계를 참조하세요.
   - 나와 공유됨(Shared by me): 공유 리소스(Shared resources) 페이지에 현재 계정이 소유하고 다른 계정과 공유한 규칙 그룹 및 다른 리소스가 표시됩니다.
   - 나와 공유 상태(Shared with me): 공유 리소스(Shared resources) 페이지에 다른 계정이 소유하고 현재 계정과 공유한 규칙 그룹 및 다른 리소스가 표시됩니다.
6. 규칙 그룹을 다른 AWS 계정, OU 또는 조직과 공유하려면 다음 값을 지정합니다.

   > **Note**
   >
   > 공유 설정을 업데이트할 수 없습니다. 다음 설정 중 하나라도 변경하려면 규칙 그룹을 새로운 설정과 다시 공유한 후 이전 공유 설정을 제거해야 합니다.

   설명

   규칙 그룹을 공유한 이유를 기억나게 해주는 간단한 설명을 입력합니다.

리소스

공유할 규칙 그룹의 확인란을 선택합니다.

보안 주체

AWS 계정 번호, OU 이름 또는 조직 이름을 입력합니다.

Tags

한 개 이상의 키와 해당 값을 지정합니다. 예를 들어 키에 Cost center를 지정하고 값에 456을 지정할 수 있습니다.

이는에서 AWS 청구서를 구성하기 위해 AWS Billing and Cost Management 제공하는 태그입니다. 다른 용도로도 태그를 사용할 수 있습니다. 비용 할당 태그 사용에 대한 자세한 내용은 AWS Billing 사용 설명서의 비용 할당 태그 사용을 참조하세요.

VPC에 대해 Route 53 Resolver DNS 방화벽 보호 활성화

하나 이상의 규칙 그룹을 VPC와 연결하여 VPC 대해 DNS 방화벽 보호를 활성화합니다. VPC가 DNS 방화벽 규칙 그룹과 연결될 때마다 Route 53 Resolver는 다음과 같은 DNS 방화벽 보호 기능을 제공합니다.

- Resolver는 DNS 방화벽을 통해 VPC의 아웃바운드 DNS 쿼리를 라우팅하고, DNS 방화벽은 연결된 규칙 그룹을 사용하여 쿼리를 필터링합니다.
- Resolver는 VPC의 DNS 방화벽 구성에서 설정을 적용합니다.

VPC에 DNS 방화벽 보호를 제공하려면 다음을 수행합니다.

- DNS 방화벽 규칙 그룹과 VPC 간의 연결을 생성하고 관리합니다. 규칙 그룹에 대한 자세한 내용은 DNS 방화벽 규칙 그룹 및 규칙 단원을 참조하세요.
- 예를 들어 DNS 방화벽이 DNS 쿼리에 대한 응답을 제공하지 않는 경우 오류 발생 시 Resolver가 VPC 대한 DNS 쿼리를 처리하게 하는 방법을 구성합니다.

VPC와 Route 53 Resolver DNS 방화벽 규칙 그룹 간의 연결 관리

규칙 그룹의 VPC 연결을 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.

   탐색 창에서 DNS 방화벽을 선택하여 Amazon VPC 콘솔에서 DNS 방화벽 규칙 그룹 페이지를 엽니다.

   - 또는 -

   에 로그인 AWS Management Console 하고를 엽니다.

   https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창의 DNS 방화벽 아래에서 규칙 그룹을 선택합니다.
3. 탐색 모음에서 규칙 그룹에 대한 리전을 선택합니다.
4. 연결할 규칙 그룹을 선택합니다.
5. 세부 정보 보기를 선택합니다. 규칙 그룹 페이지가 표시됩니다.
6. 맨 아래에 규칙 및 관련 VPC가 포함된 탭 세부 정보 영역이 표시됩니다. 연결된 VPC(Associated VPCs) 탭을 선택합니다.

규칙 그룹을 VPC 와 연결하려면

1. 이전 절차 규칙 그룹의 VPC 연결을 보려면(To view a rule group's VPC associations)에 있는 지침에 따라 규칙 그룹의 VPC 연결을 찾습니다.
2. 연결된 VPC(Associated VPCs) 탭에서 VPC 연결을 선택합니다.
3. 드롭다운 메뉴에서 규칙 그룹과 연결할 VPC를 찾습니다. 해당 VPC를 선택한 다음 연결을 선택합니다.

규칙 그룹 페이지에서 VPC는 연결된 VPC(Associated VPCs) 탭에 나열됩니다. 처음에는 연결의 상태(Status)에서 업데이트 중을 보고합니다. 연결이 완료되면 상태가 완료로 변경됩니다.

규칙 그룹과 VPC 간의 연결을 제거하려면

1. 이전 절차 규칙 그룹의 VPC 연결을 보려면(To view a rule group's VPC associations)에 있는 지침에 따라 규칙 그룹의 VPC 연결을 찾습니다.

2. 목록에서 제거할 VPC 선택한 다음 연결 해제(Disassociate)를 선택합니다. 확인한 다음 작업을 확인합니다.

규칙 그룹 페이지에서 VPC는 연결된 VPC(Associated VPCs) 탭에 연결 해제 중(Disassociating) 상태로 나열됩니다. 작업이 완료되면 DNS 방화벽이 목록을 업데이트하여 VPC를 제거합니다.

DNS 방화벽 VPC 구성

VPC 대한 DNS 방화벽 구성은 Route 53 Resolver가 DNS 방화벽이 손상되거나 응답하지 않거나 영역에서 사용할 수 없는 경우와 같은 오류 시 쿼리를 허용할지 또는 차단할지 여부를 결정합니다. Resolver는 DNS 방화벽 규칙 그룹이 하나 이상 VPC와 연결될 때마다 VPC의 방화벽 구성을 적용합니다.

VPC를 구성하여 오류 열기 또는 오류 닫기를 수행할 수 있습니다.

- 기본적으로 오류 모드는 닫혀 있습니다. 즉, Resolver가 DNS 방화벽에서 응답을 받지 못하는 모든 쿼리를 차단하고 `SERVFAIL` DNS 응답을 보냅니다. 이 접근 방식은 가용성보다 보안을 우선합니다.
- 오류 열기를 사용하도록 설정하면 Resolver가 DNS 방화벽에서 응답을 받지 못하는 경우 쿼리를 허용합니다. 이 접근 방식은 보안보다 가용성을 우선합니다.

VPC 대한 DNS 방화벽 구성을 변경하려면(콘솔)

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53resolver/ Resolver 콘솔을 엽니다.
2. Resolver의 탐색 창에서 VPC를 선택합니다.
3. VPC페이지에서 VPC를 찾아 편집합니다. 필요에 따라 DNS 방화벽 구성을 오류 열기나 오류 닫기로 변경합니다.

VPC에 대한 DNS 방화벽 동작을 변경하려면(API)

- UpdateFirewallConfig를 호출하고 `FirewallFailOpen`을 활성화하거나 비활성화하여 VPC 방화벽 구성을 업데이트합니다.

ListFirewallConfigs를 호출하여 API를 통해 VPC 방화벽 구성의 목록을 검색할 수 있습니다.

Amazon Route 53 Profiles란?

Route 53 Profiles를 사용하면 여러 VPCs하고 관리할 수 있습니다 AWS 계정. 프로파일을 사용하면 여러 VPC의 DNS 설정을 단일 VPC에 대해 관리하는 것만큼 쉽게 관리할 수 있으며 프로파일을 업데이트할 때 해당 설정이 프로파일에 연결된 모든 VPC에 전파됩니다. 를 사용하여 동일한 리전 AWS 계정의와 프로필을 공유할 수도 있습니다 AWS RAM. 현재 프로파일에 연결할 수 있는 Route 53 지원 리소스는 다음과 같습니다.

- 프라이빗 호스팅 영역 및 해당 영역에 지정된 설정.
- Route 53 Resolver 규칙(전달 및 시스템 모두).
- DNS 방화벽 규칙 그룹.

일부 VPC 구성은 프로파일에서 직접 관리됩니다. 구성은 다음과 같습니다.

- Resolver 규칙에 대한 역방향 DNS 조회 구성.
- DNS 방화벽 실패 모드 구성.
- DNSSEC 검증 구성.

예를 들어 프로파일이 연결된 모든 VPC에 대해 DNS 방화벽 실패 모드 구성을 활성화할 수 있지만 VPC의 기존 DNSSEC 검증 구성을 유지할 수 있습니다.

> **Important**
>
> 이전 구성에 대해 프로파일 설정을 활성화하고 프로파일을 VPC에 연결하면 프로파일 설정이 즉시 적용됩니다.

AWS CloudFormation 를 사용하여 새로 프로비저닝된 VPCs.

VPC당 하나의 프로파일을 연결할 수 있으며 프로파일당 연결 가능한 리소스 수는 달라질 수 있습니다. 자세한 내용은 Route 53 Profiles의 할당량 단원을 참조하십시오.

Route 53 Profile 설정의 우선순위 지정 방법

마이그레이션 또는 기타 테스트 목적으로 프로파일에 대한 로컬 DNS 설정 및 연결을 설정할 수 있습니다. DNS 쿼리가 VPC와 직접 연결된 프라이빗 호스팅 영역에 대한 Resolver 규칙과 프로파일과 연결된

프라이빗 호스팅 영역에 대한 Resolver 규칙 모두와 일치하는 경우 로컬 DNS 설정이 우선합니다. 충돌하는 도메인 이름에 대해 DNS 쿼리를 수행하면 가장 구체적인 도메인 이름이 승리합니다. 다음 표에는 평가 순서의 예가 나와 있습니다.

DNS 쿼리	프로파일 규칙	VPC 규칙	평가된 규칙
example.com	example.com	example.com	로컬 VPC
test.example.com	test.example.com	example.com	프로필
marketing.example.com	없음	marketing.example.com	로컬 VPC

Route 53 Profiles 리전 가용성

리전 가용성 및 엔드포인트를 보려면 AWS 일반 참조 가이드의 Route 53에 대한 서비스 엔드포인트를 참조하세요.

Route 53 Profiles 사용을 위한 개략적인 단계

Amazon Virtual Private Cloud VPC에서 Amazon Route 53 Profiles을 구현하려면 다음과 같은 개략적인 단계를 수행합니다.

1. 빈 프로파일 생성 - 첫 번째 단계는 DNS 리소스를 연결할 수 있는 빈 프로파일을 생성하는 것입니다. 자세한 내용은 Route 53 Profiles 생성 단원을 참조하십시오.
2. 프로파일에 DNS 리소스 연결 - 현재 프로파일에 연결할 수 있는 리소스는 프라이빗 호스팅 영역, Route 53 Resolver 규칙, 전달 및 시스템, DNS 방화벽 규칙 그룹입니다. 자세한 내용은 DNS 방화벽 규칙 그룹을 Route 53 Profile에 연결, 프라이빗 호스팅 영역을 Route 53 Profile에 연결, Resolver 규칙을 Route 53 Profile에 연결 섹션을 참조하세요.
3. 프로파일에 대한 일부 VPC 설정 구성 - 프로파일에 연결된 호스팅 영역과 같은 일부 DNS 설정이 VPC에 즉시 적용됩니다. DNSSEC 검증, Resolver 역방향 DNS 조회, DNS 방화벽 실패 모드 구성의 경우 다음 옵션 중 하나를 선택할 수 있습니다.
   - DNSSEC 검증의 경우 로컬 VPC 구성(기본값)을 사용하거나 검증을 활성화하거나 프로파일에 연결된 모든 VPC에 대한 검증을 비활성화하도록 선택할 수 있습니다.

- Resolver 역방향 DNS 조회 구성의 경우 이를 활성화하거나 비활성화하거나 로컬에서 VPC에 대해 정의된 자동 정의 규칙(기본값)을 사용할 수 있습니다.
- DNS 방화벽 장애 모드 구성의 경우 이를 활성화하거나 비활성화하거나 VPC에 대해 로컬로 정의된 장애 모드 구성(기본값)을 사용할 수 있습니다.

자세한 내용은 Route 53 Profile 구성 편집 단원을 참조하십시오.

4. 프로파일을 하나 이상의 VPC에 연결 - 프로파일을 사용하려면 하나 이상의 VPC에 연결합니다. 자세한 내용은 Route 53 Profile을 VPC에 연결 단원을 참조하십시오.

Route 53 Profiles 생성

Route 53 Profiles을 생성하려면 이 주제의 지침을 따르세요. 탭을 선택하여 Route 53 콘솔을 사용하여 Route 53 프로파일을 생성하거나, 또는를 선택합니다 AWS CLI.

- 콘솔
- CLI

Console

Route 53 Profile을 생성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 프로필을 선택합니다.
3. 탐색 모음에서 프로파일을 생성하려는 리전을 선택합니다.
4. 프로파일의 이름을 입력하고 선택적으로 태그를 추가한 다음 프로파일 생성을 선택합니다.

   이렇게 하면 리소스를 연결할 수 있는 기본 구성이 포함된 빈 프로파일이 생성됩니다. 리소스를 프로파일에 연결한 후 여러 VPC에 연결하고 일부 Resolver 구성이 VPC에 적용되는 방식을 편집합니다.

CLI

다음과 같은 AWS CLI 명령을 실행하고 name에 대한 자체 값을 사용하여 프로파일을 생성할 수 있습니다.

```
aws route53profiles create-profile --name test
```

다음은 명령을 실행한 후에 생성되는 출력 예시입니다.

```
{
    "Profile": {
        "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-6ffe47d5example",
        "ClientToken": "2ca1a304-32b3-4f5f-bc4c-EXAMPLE11111",
        "CreationTime": 1710850903.578,
        "Id": "rp-6ffe47d5example",
        "ModificationTime": 1710850903.578,
        "Name": "test",
        "OwnerId": "123456789012",
        "ShareStatus": "NOT_SHARED",
        "Status": "COMPLETE",
        "StatusMessage": "Created Profile"
    }
}
```

프로파일을 다른 리소스와 연결하고 프로파일의 VPC 구성을 편집하려면 다음 절차를 참조하세요.

주제

- DNS 방화벽 규칙 그룹을 Route 53 Profile에 연결
- 프라이빗 호스팅 영역을 Route 53 Profile에 연결
- Resolver 규칙을 Route 53 Profile에 연결
- Route 53 Profile 구성 편집
- Route 53 Profile을 VPC에 연결

DNS 방화벽 규칙 그룹을 Route 53 Profile에 연결

Route 53 콘솔을 사용하여 DNS 방화벽 규칙 그룹을 Route 53 프로파일에 연결하려면 탭을 선택합니다 AWS CLI. 또는

- 콘솔
- CLI

Console

DNS 방화벽 규칙 그룹을 연결하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 모음에서 프로파일을 생성한 리전을 선택합니다.
3. 탐색 창에서 프로파일을 선택하고 프로파일 테이블에서 작업하려는 프로파일의 연결된 이름을 선택합니다.
4. <Profile name> 페이지에서 DNS 방화벽 규칙 그룹 탭을 선택한 다음 연결을 선택합니다.
5. DNS 방화벽 규칙 그룹 섹션에서 이전에 생성한 규칙 그룹을 최대 10개까지 선택할 수 있습니다. 10개 이상의 규칙 그룹을 연결하려면 API를 사용합니다. 자세한 내용은 AssociateResourceToProfile을 참조하세요.

   새 규칙 그룹을 생성하려면 규칙 그룹 및 규칙 생성 섹션을 참조하세요.
6. Next(다음)를 선택합니다.
7. 우선순위 정의 페이지에서 미리 할당된 우선순위 번호를 클릭하고 새 우선순위를 입력하여 규칙 그룹이 처리되는 순서를 설정할 수 있습니다. 우선순위에 허용되는 값은 100~9900입니다.

   규칙 그룹은 가장 낮은 숫자 우선순위 설정부터 위로 올라가는 방식으로 평가됩니다. 처리 순서를 변경하거나 다른 규칙 그룹을 위한 공간을 확보하려면 언제든 규칙 그룹의 우선순위를 변경할 수 있습니다.

   제출을 선택합니다.
8. 연결 진행률은 DNS 방화벽 규칙 그룹 대화 상자의 상태 열에 표시됩니다.

CLI

다음과 같은 AWS CLI 명령을 실행하고 `name` `profile-id`, 및에 대한 자체 값을 사용하여 규칙 그룹을 프로파일에 연결할 수 있습니다. `resource-arn` `priority`

```
aws route53profiles associate-resource-to-profile --name test-
resource-association --profile-id rp-4987774726example --resource-arn
arn:aws:route53resolver:us-east-1:123456789012:firewall-rule-group/
rslvr-frg-cfe7f72example --resource-properties "{\"priority\": 102}"
```

다음은 명령을 실행한 후에 생성되는 출력 예시입니다.

```
{
    "ProfileResourceAssociation": {
        "CreationTime": 1710851216.613,
        "Id": "rpr-001913120a7example",
        "ModificationTime": 1710851216.613,
        "Name": "test-resource-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-
rule-group/rslvr-frg-cfe7f72example",
        "ResourceProperties": "{\"priority\":102}",
        "ResourceType": "FIREWALL_RULE_GROUP",
        "Status": "UPDATING",
        "StatusMessage": "Updating the Profile to DNS Firewall rule group
 association"
    }
}
```

프라이빗 호스팅 영역을 Route 53 Profile에 연결

이 절차의 단계에 따라 프라이빗 호스팅 영역을 프로파일에 연결합니다.

프라이빗 호스팅 영역을 연결하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 모음에서 프로파일을 생성한 리전을 선택합니다.
3. 탐색 창에서 프로파일을 선택하고 프로파일 테이블에서 작업하려는 프로파일의 연결된 이름을 선택합니다.
4. <Profile name> 페이지에서 프라이빗 호스팅 영역 탭을 선택한 다음 연결을 선택합니다.
5. 프라이빗 호스팅 영역 연결 페이지에서 이전에 생성한 프라이빗 호스팅 영역을 최대 10개까지 선택할 수 있습니다. 10개 이상의 프라이빗 호스팅 영역을 연결하려면 API를 사용합니다. 자세한 내용은 AssociateResourceToProfile을 참조하세요.

   프라이빗 호스팅 영역을 생성하려면 프라이빗 호스팅 영역 생성 섹션을 참조하세요.
6. 연결 선택
7. 연결 진행 상황은 프라이빗 호스팅 영역 페이지의 상태 열에 표시됩니다.

Resolver 규칙을 Route 53 Profile에 연결

이 절차의 단계에 따라 Resolver 규칙을 프로파일에 연결합니다.

Resolver 규칙을 연결하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 모음에서 프로파일을 생성한 리전을 선택합니다.
3. <Profile name> 페이지에서 Resolver 규칙 탭을 선택한 다음 연결을 선택합니다.
4. Resolver 규칙 연결 페이지의 Resolver 규칙 테이블에서 이전에 생성한 Resolver 규칙을 최대 10개까지 선택할 수 있습니다. 10개 이상의 Resolver 규칙을 연결하려면 API를 사용합니다. 자세한 내용은 AssociateResourceToProfile을 참조하세요.

   Resolver 규칙을 생성하려면 전달 규칙 생성 섹션을 참조하세요.
5. 연결 선택
6. 연결 진행률은 Resolver 규칙 페이지의 상태 열에 표시됩니다.

Route 53 Profile 구성 편집

리소스를 프로파일에 연결한 후 기본 VPC 구성을 편집하여 VPC에 적용되는 방식을 결정할 수 있습니다.

프로파일 구성을 편집하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 모음에서 프로파일을 생성한 리전을 선택합니다.
3. 탐색 창에서 프로파일을 선택하고 프로파일 테이블에서 작업하려는 프로파일의 연결된 이름을 선택합니다.
4. <Profile name> 페이지에서 구성 탭을 선택한 다음 편집을 선택합니다.
5. 구성 편집 페이지에서 VPC DNSSEC 구성, Resolver 역방향 DNS 조회 구성, DNS 방화벽 실패 모드 구성의 값 중 하나를 선택합니다.

   이 값에 대한 자세한 내용은 Route 53 Profile의 구성 설정을 참조하세요.
6. 업데이트를 선택합니다.

Route 53 Profile의 구성 설정

Route 53 Profile 구성을 편집할 때 다음 값을 지정합니다.

DNSSEC 구성

다음 값 중 하나를 선택합니다.

- 로컬 VPC DNSSEC 구성 사용 - 기본값

  이 프로파일에 연결된 모든 VPC가 로컬 DNSSEC 검증 구성을 유지하게 하려면 이 옵션을 선택합니다.

- DNSSEC 검증 활성화

  이 프로파일에 연결된 모든 VPC에서 DNSSEC 검증을 활성화하려면 이 옵션을 선택합니다.

- DNSSEC 검증 비활성화

  이 프로파일에 연결된 모든 VPC에서 DNSSEC 검증을 비활성화하려면 이 옵션을 선택합니다.

Resolver 역방향 DNS 조회 구성

다음 값 중 하나를 선택합니다.

- 활성화

  연결된 모든 VPC에서 역방향 DNS 조회를 위한 자동 정의 규칙을 생성하려면 이 옵션을 선택합니다.

- 활성화되지 않음

  연결된 모든 VPC에서 역방향 DNS 조회를 위한 자동 정의 규칙을 생성하지 않으려면 이 옵션을 선택합니다.

- 로컬 자동 정의 규칙 사용 - 기본값

  연결된 VPC에 대한 역방향 DNS 조회에 로컬 VPC 설정을 사용하려면 이 옵션을 선택합니다.

DNS 방화벽 실패 모드 구성

다음 값 중 하나를 선택합니다.

- 비활성화

  연결된 VPC에 대한 DNS 방화벽 실패 모드를 닫으려면 이 옵션을 선택합니다. 이 옵션을 사용하면 DNS 방화벽이 제대로 평가할 수 없는 모든 쿼리를 차단합니다.

- 활성화됨

  연결된 모든 VPC에 대해 DNS 방화벽 실패 모드를 열린 상태로 유지하려면 이 옵션을 선택합니다. 이 옵션을 사용하면 DNS 방화벽에서 쿼리를 제대로 평가할 수 없는 경우 쿼리를 진행할 수 있습니다.

- 로컬 실패 모드 설정 사용 - 기본값

  로컬 VPC DNS 방화벽 실패 모드 설정을 사용하려면 이 옵션을 선택합니다.

구성에 대한 자세한 내용은 다음 섹션을 참조하세요.

- Amazon Route 53에서 DNSSEC 검증 활성화
- 해석기의 역방향 DNS 쿼리에 대한 전달 규칙
- DNS 방화벽 VPC 구성

Route 53 Profile을 VPC에 연결

Route 53 Profile을 VPC에 연결하려면 이 항목의 지침을 따르세요. Route 53 콘솔을 사용하여 Route 53 프로파일을 VPC에 연결하려면 탭을 선택합니다 AWS CLI. 또는

- 콘솔
- CLI

Console

VPC를 연결하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 모음에서 프로파일을 생성한 리전을 선택합니다.
3. <Profile name> 페이지에서 VPC 탭을 선택한 다음 연결을 선택합니다.
4. VPC 연결 페이지에서 이전에 생성한 VPC를 최대 10개 선택할 수 있습니다. VPC를 10개 이상 연결하려면 API를 사용합니다. 자세한 내용은 AssociateProfile을 참조하세요.
5. 연결 선택
6. 연결 진행 상황은 VPC 페이지의 상태 열에 표시됩니다.

CLI

다음과 같은 AWS CLI 명령을 실행하고 name, profile-id및에 대한 자체 값을 사용하여 프로파일을 나열할 수 있습니다. resource-id

```
aws route53profiles associate-profile --name test-association --profile-id rp-4987774726example --resource-id vpc-0af3b96b3example
```

다음은 명령을 실행한 후에 생성되는 출력 예시입니다.

```
{
    "ProfileResourceAssociation": {
        "CreationTime": 1710851216.613,
        "Id": "rpr-001913120a7example",
        "ModificationTime": 1710851216.613,
        "Name": "test-resource-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-rule-group/rslvr-frg-cfe7f72example",
        "ResourceProperties": "{\"priority\":102}",
        "ResourceType": "FIREWALL_RULE_GROUP",
        "Status": "UPDATING",
        "StatusMessage": "Updating the Profile to DNS Firewall rule group association"
    }
}
```

Amazon Route 53 Profiles 보기 및 업데이트

콘솔 탭을 선택하여 Route 53 Profile을 보고 편집합니다. 소유하거나, 사용자가 공유하거나, 사용자에게 공유되는 프로필을 나열하는 AWS CLI 데 사용할 CLI 탭을 선택합니다.

- 콘솔
- CLI

Console

Route 53 Profiles 보기 및 업데이트

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 프로필을 선택합니다.
3. 보거나 편집하려는 프로파일의 이름 옆에 있는 버튼을 선택합니다.
4. <Profile name> 페이지에서 현재 연결된 DNS 리소스를 보고, 새 리소스를 연결하고, 태그와 VPC 구성을 편집할 수 있습니다.

CLI

다음과 같은 AWS CLI 명령을 실행하여 프로파일을 나열할 수 있습니다.

```
aws route53profiles list-profiles
```

다음은 명령을 실행한 후에 생성되는 출력 예시입니다.

```
{
    "ProfileSummaries": [
        {
            "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-4987774726example",
            "Id": "rp-4987774726example",
            "Name": "test",
            "ShareStatus": "NOT_SHARED"
        }
    ]
}
```

다음과 같은 AWS CLI 명령을 실행하고 `profile-association-id`에 대한 자체 값을 사용하여 프로파일이 연결된 특정 VPS에 대한 정보를 얻을 수 있습니다.

```
aws route53profiles get-profile-association --profile-association-id
rpassoc-489ce212fexample
```

다음은 명령을 실행한 후에 생성되는 출력 예시입니다.

```
   "ProfileAssociation": {
```

```
        "CreationTime": 1709338817.148,
        "Id": "rrpassoc-489ce212fexample",
        "ModificationTime": 1709338974.772,
        "Name": "test-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceId": "vpc-0af3b96b3example",
        "Status": "COMPLETE",
        "StatusMessage": "Created Profile Association"
    }   ]
}
```

Amazon Route 53 Profile 삭제

Route 53 콘솔 또는를 사용하여 Route 53 프로파일을 삭제하려면 탭을 선택합니다 AWS CLI.

- 콘솔
- CLI

Console

Route 53 Profile을 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 프로필을 선택합니다.
3. 삭제할 프로파일 이름 옆에 있는 버튼을 선택한 다음 삭제를 선택합니다.

   > **Important**
   >
   > VPC에 연결된 프로파일은 삭제할 수 없습니다. 또한 프로파일이 다른에 공유되면 프로파일 구성이 연결된 AWS 계정 VPCs는 해당 구성을 잃게 됩니다.

4. <Profile name> 삭제 대화 상자에 **`confirm`**를 입력한 다음 삭제를 선택합니다.

CLI

> **Important**
>
> VPC에 연결된 프로파일은 삭제할 수 없습니다. 또한 프로파일이 다른에 공유되면 프로파일 구성이 연결된 AWS 계정 VPCs는 해당 구성을 잃게 됩니다.

다음과 같은 AWS CLI 명령을 실행하고에 대한 자체 값을 사용하여 프로필을 삭제할 수 있습니다. `profile-id`

```
aws route53profiles delete-profile --profile-id rp-6ffe47d5example
```

다음은 명령을 실행한 후에 생성되는 출력 예시입니다.

```
{
    "Profile": {
        "Arn": "arn:aws:route53profiles:us-east-1:123456789012:profile/
rp-6ffe47d5example",
        "ClientToken": "0a15fec0-05d9-4f78-bec0-EXAMPLE11111",
        "CreationTime": 1710850903.578,
        "Id": "rp-6ffe47d5example",
        "ModificationTime": 1710850903.578,
        "Name": "test",
        "OwnerId": "123456789012",
        "ShareStatus": "NOT_SHARED",
        "Status": "DELETED",
        "StatusMessage": "Deleted Profile"
    }
}
```

Amazon Route 53 Profile과 연결된 Route 53 리소스 보기 및 업데이트

콘솔 탭을 선택하여 Route 53 Profile 리소스 연결을 확인하고 DNS 방화벽 규칙 그룹 우선순위를 선택적으로 편집합니다. 리소스 연결을 AWS CLI 나열하고 DNS 방화벽 규칙 그룹의 우선 순위에 대한 예제 업데이트를 보려면 사용할 CLI 탭을 선택합니다.

- 콘솔

- CLI

Console

프로파일과 연결된 리소스를 보고 업데이트하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 프로필을 선택합니다.
3. 탐색 모음에서 프로파일을 생성한 리전을 선택합니다.
4. 리소스 연결을 보거나 편집하려는 프로파일의 이름 옆에 있는 버튼을 선택합니다.
5. <Profile name> 페이지에서 DNS 방화벽 규칙 그룹, 프라이빗 호스팅 영역 또는 Resolver 규칙 중 하나를 보거나 편집하려는 리소스의 탭을 선택합니다.
6. 리소스의 탭 페이지에서 연결된 리소스의 이름, ARN, 상태를 볼 수 있습니다. 기어 아이콘을 선택하여 리소스 테이블에 표시되는 내용을 조정할 수도 있습니다.

   DNS 방화벽 규칙 그룹 탭 페이지에서 규칙 그룹 우선순위 항목을 선택하고 더 작거나 더 큰 수로 편집할 수도 있습니다. 규칙 그룹은 가장 낮은 우선순위 번호부터 가장 높은 우선순위 번호까지 순서대로 평가됩니다.

CLI

다음과 같은 AWS CLI 명령을 실행하고에 대한 자체 값을 사용하여 프로파일과 연결된 리소스를 나열할 수 있습니다. `profile-id`

```
aws route53profiles list-profile-resource-associations --profile-id
rp-4987774726example
```

다음은 명령을 실행한 후에 생성되는 출력 예시입니다.

```
{
    "ProfileResourceAssociations": [
        {
            "CreationTime": 1710851216.613,
            "Id": "rpr-001913120a7example",
            "ModificationTime": 1710851216.613,
            "Name": "test-resource-association",
            "OwnerId": "123456789012",
```

```
            "ProfileId": "rp-4987774726example",
            "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-
rule-group/rslvr-frg-cfe7f72example",
            "ResourceProperties": "{\"priority\":102}",
            "ResourceType": "FIREWALL_RULE_GROUP",
            "Status": "COMPLETE",
            "StatusMessage": "Completed creation of Profile to DNS Firewall rule
 group association"
        }
    ]
}
```

다음과 같은 AWS CLI 명령을 실행하고에 대한 자체 값을 사용하고 profile-resource-association-id 및에 대한 자체 값을 사용하여 프로파일에 연결된 DNS 방화벽 규칙 그룹의 우선 순위를 업데이트할 수 있습니다. --resource-properties

```
aws route53profiles update-profile-resource-association --profile-
resource-association-id rpr-001913120a7example --resource-properties
"{\"priority\": 105}"
```

다음은 명령을 실행한 후에 생성되는 출력 예시입니다.

```
{
    "ProfileResourceAssociation": {
        "CreationTime": 1710851216.613,
        "Id": "rpr-001913120a7example",
        "ModificationTime": 1710852303.798,
        "Name": "test-resource-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceArn": "arn:aws:route53resolver:us-east-1:123456789012:firewall-
rule-group/rslvr-frg-cfe7f72example",
        "ResourceProperties": "{\"priority\":105}",
        "ResourceType": "FIREWALL_RULE_GROUP",
        "Status": "UPDATING",
        "StatusMessage": "Updating the Profile to DNS Firewall rule group
 association"
    }
}
```

Amazon Route 53 Profile에서 리소스 연결 해제

프로파일을 삭제하기 전에 모든 리소스를 해당 프로파일에서 연결 해제해야 합니다.

Route 53 Profile에 연결된 리소스 연결을 해제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 프로필을 선택합니다.
3. 탐색 모음에서 리소스를 연결 해제하려는 프로파일이 생성된 리전을 선택합니다.
4. 리소스 연결을 해제하려는 프로파일의 이름 옆에 있는 버튼을 선택합니다.
5. <Profile name> 페이지에서 DNS 방화벽 규칙 그룹, 프라이빗 호스팅 영역 또는 Resolver 규칙 중 하나를 삭제하려는 리소스의 탭을 선택합니다.
6. 리소스의 탭 페이지에서 연결을 해제할 리소스를 선택한 다음 연결 해제를 선택합니다.
7. 리소스 연결 해제 대화 상자에서 **`confirm`**를 입력한 다음 연결 해제를 선택합니다.

Amazon Route 53 Profile에 연결된 VPC 보기

콘솔 탭을 선택하여 VPC 연결에 대한 Route 53 Profile을 보고 편집합니다. 프로파일과 VPC 연결을 나열하거나 특정 연결에 대한 정보를 가져오는 AWS CLI 데 사용할 CLI 탭을 선택합니다.

- 콘솔
- CLI

Console

프로파일에 연결된 VPC를 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 프로필을 선택합니다.
3. 탐색 모음에서 프로파일을 생성한 리전을 선택합니다.
4. 연결된 VPC를 보려는 프로파일의 이름 옆에 있는 버튼을 선택합니다.
5. <Profile name> 페이지에서 VPC 탭을 선택합니다.

6. VPC의 탭 페이지에서 연결된 VPC의 이름, ARN, 상태를 볼 수 있습니다.

CLI

다음과 같은 AWS CLI 명령을 실행하여 프로파일이 연결된 VPCs를 나열할 수 있습니다.

```
aws route53profiles list-profile-associations
```

다음은 명령을 실행한 후에 생성되는 출력 예시입니다.

```
{
    "ProfileAssociations": [
        {
            "CreationTime": 1709338817.148,
            "Id": "rpassoc-489ce212fexample",{
    "ProfileAssociations": [
        {
            "CreationTime": 1709338817.148,
            "Id": "rpassoc-489ce212fexample",
            "ModificationTime": 1709338974.772,
            "Name": "test-association",
            "OwnerId": "123456789012",
            "ProfileId": "rp-4987774726example",
            "ResourceId": "vpc-0af3b96b3example",
            "Status": "COMPLETE",
            "StatusMessage": "Created Profile Association"
        }
    ]
}
            "ModificationTime": 1709338974.772,
            "Name": "test-association",
            "OwnerId": "123456789012",
            "ProfileId": "rp-4987774726example",
            "ResourceId": "vpc-0af3b96b3example",
            "Status": "COMPLETE",
            "StatusMessage": "Created Profile Association"
        }
    ]
}
```

다음과 같은 AWS CLI 명령을 실행하고 `profile-association-id`에 대한 자체 값을 사용하여 프로파일이 연결된 특정 VPS에 대한 정보를 얻을 수 있습니다.

```
aws route53profiles get-profile-association --profile-association-id
rpassoc-489ce212fexample
```

다음은 명령을 실행한 후에 생성되는 출력 예시입니다.

```
   "ProfileAssociation": {
        "CreationTime": 1709338817.148,
        "Id": "rrpassoc-489ce212fexample",
        "ModificationTime": 1709338974.772,
        "Name": "test-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceId": "vpc-0af3b96b3example",
        "Status": "COMPLETE",
        "StatusMessage": "Created Profile Association"
    }   ]
}
```

Amazon Route 53 Profile에서 VPC 연결 해제

탭을 선택하여 Route 53 콘솔 또는를 사용하여 VPC에서 Route 53 프로파일의 연결을 해제합니다 AWS CLI.

- 콘솔
- CLI

Console

Route 53 Profile에 연결된 VPC를 연결 해제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 프로필을 선택합니다.
3. 탐색 모음에서 VPC를 연결 해제하려는 프로파일이 생성된 리전을 선택합니다.
4. VPC 연결을 해제하려는 프로파일의 이름 옆에 있는 버튼을 선택합니다.
5. <Profile name> 페이지에서 VPC 탭을 선택합니다.
6. 리소스의 VPC 탭 페이지에서 연결 해제하려는 VPC를 선택한 다음 연결 해제를 선택합니다.

7. 리소스 연결 해제 대화 상자에서 **confirm**를 입력한 다음 연결 해제를 선택합니다.

CLI

다음과 같은 AWS CLI 명령을 실행하고 `profile-id` 및에 대한 자체 값을 사용하여 VPC에서 프로파일을 연결 해제할 수 있습니다. `--resource-id`

```
aws route53profiles disassociate-profile --profile-id
rp-4987774726example --resource-id vpc-0af3b96b3example
```

다음은 명령을 실행한 후에 생성되는 출력 예시입니다.

```
"ProfileAssociation": {
        "CreationTime": 1710851336.527,
        "Id": "rpassoc-489ce212fexample",
        "ModificationTime": 1710851401.362,
        "Name": "test-association",
        "OwnerId": "123456789012",
        "ProfileId": "rp-4987774726example",
        "ResourceId": "vpc-0af3b96b3example",
        "Status": "DELETING",
        "StatusMessage": "Deleting Profile Association"
    }
```

공유 Route 53 Profiles 작업

다음을 통해 다른 계정과 프로파일을 공유할 수 있습니다.

- 읽기 전용 권한을 부여하면 다른 계정이 프로파일을 VPC에 연결할 수 있습니다. 이 경우 모든 DNS 리소스 및 구성이 연결된 VPC에 적용됩니다.
- 관리자 권한 부여. 이 경우 공유 프로파일이 있는 계정은 프로파일을 수정한 다음 VPC와 연결할 수 있습니다. 또한 소유자는 소비자 계정에서 수행할 수 있는 작업을 지정하는 데 사용 가능한 고객 관리형 권한을 생성할 수 있습니다. 자세한 내용은 AWS RAM 사용 설명서의 고객 관리형 권한을 참조하세요.

Amazon Route 53 Profile은 AWS Resource Access Manager (AWS RAM)와 통합되어 리소스 공유를 활성화합니다. AWS RAM 는 일부 Route 53 리소스를 다른 AWS 계정 또는를 통해 공유할 수 있는 서비스입니다 AWS Organizations. AWS RAM를 사용하면 리소스 공유를 생성하여 소유한 리소스를 공

유할 수 있습니다. 리소스 공유는 공유할 리소스와 공유 대상 소비자를 지정합니다. 소비자에는 다음이 포함될 수 있습니다.

- 특정 AWS 계정
- 의 조직 내 조직 단위 AWS Organizations
- 의 전체 조직 AWS Organizations

에 대한 자세한 내용은 AWS RAM 사용 설명서를 AWS RAM참조하세요.

이 항목에서는 소유한 리소스를 공유하는 방법과 공유 리소스를 사용하는 방법을 설명합니다.

내용

Route 53 Profiles 공유 권한 부여

IAM 보안 주체가 프로파일을 공유하려면 최소 권한 세트가 필요합니다. `AmazonRoute53ProfilesFullAccess` 관리형 IAM 정책을 사용하여 IAM 보안 주체가 공유 프로파일을 공유하고 사용하는 데 필요한 권한을 갖추게 하는 것이 좋습니다.

사용자 지정 IAM 정책을 사용하는 경우 `route53profiles:GetProfilePolicy` 및 `route53profiles:PutProfilePolicy` 작업이 필요합니다. 이는 권한 전용 IAM 작업입니다. IAM 보안 주체에게 이러한 권한이 부여되지 않은 경우 AWS RAM 서비스를 사용하여 프로필을 공유하려고 할 때 오류가 발생합니다.

Route 53 Profiles 공유를 위한 사전 조건

- Route 53 프로필을 공유하려면에서 소유해야 합니다 AWS 계정. 즉, 계정에서 리소스를 할당하거나 프로비저닝해야 합니다. 사용자와 공유된 Route 53 Profile을 공유할 수 없습니다.

- AWS Organizations의 조직 또는 조직 단위와 Route 53 Profile을 공유하려면 AWS Organizations와의 공유를 활성화해야 합니다. 자세한 내용은 AWS RAM 사용 설명서의 AWS Organizations과(와) 공유 활성화를 참조하세요.

Route 53 Profile 공유

소유한 프로필을 다른 사용자와 공유할 때 해당 사용자가 프로필의 DNS 관련 설정을 VPCs에 적용할 수 있도록 AWS 계정합니다. 따라서 관리 오버헤드를 최소화하면서 수천 개의 VPC에서 균일한 DNS 구성을 더 쉽게 적용할 수 있습니다.

Route 53 Profile을 공유하려면 리소스 공유에 추가해야 합니다. 리소스 공유는 AWS 계정전반에서 리소스를 공유할 수 있게 해주는 AWS RAM 리소스입니다. 리소스 공유는 공유할 리소스와 공유 대상 소비자를 지정합니다. Route 53 콘솔을 사용하여 Route 53 Profile을 공유하면 기존 리소스 공유에 추가됩니다. 새 리소스 공유에 Route 53 Profile을 추가하려면, 우선AWS RAM 콘솔을 사용해 리소스 공유를 만들어야 합니다.

의 조직에 속 AWS Organizations 해 있고 조직 내 공유가 활성화된 경우 조직의 소비자에게 공유된 Route 53 Profile에 대한 액세스 권한이 자동으로 부여됩니다. 그렇지 않으면 소비자는 리소스 공유에 가입하라는 초대장을 받고 초대를 수락한 후 공유된 Route 53 Profile의 액세스 권한을 받습니다.

Route 53 콘솔에서 소유한 Route 53 프로파일 공유를 시작하고 AWS RAM 콘솔에서 계속할 수 있습니다.

Route 53 콘솔을 사용하여 소유한 Route 53 Profile을 공유하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 프로필을 선택합니다.
3. 공유할 프로필을 선택하고 프로필 세부 정보 페이지에서 프로필 공유를 선택합니다.
4. AWS RAM 사용 설명서의 리소스 공유 생성 단계를 수행할 수 있는 AWS RAM 콘솔로 이동합니다.
5. 프로파일이 공유된 경우 프로파일 테이블에는 나와 공유됨 텍스트가 포함됩니다.

   프로파일을 공유하면 프로파일 테이블에 공유로 나열됩니다.

AWS RAM 콘솔을 사용하여 소유한 Route 53 Profile을 공유하려면

AWS RAM 사용 설명서의 리소스 공유 생성을 참조하세요.

를 사용하여 소유한 Route 53 Profile을 공유하려면 AWS CLI

create-resource-share 명령을 사용합니다.

공유된 Route 53 Profile 공유 해제

프로파일과 해당 프로파일의 구성이 연결된 VPC의 공유를 해제하면 해당 설정이 손실되고 VPC별 구성이 기본값으로 설정됩니다.

소유하고 있는 공유된 Route 53 Profile을 공유 해제하려면 리소스 공유에서 제거해야 합니다. 이를 위해 Route 53 콘솔, AWS RAM 콘솔 또는 AWS CLI를 사용할 수 있습니다.

Route 53 콘솔을 사용하여 소유한 공유 Route 53 Profile을 공유 해제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 프로필을 선택합니다.
3. 공유 해제하려는 프로파일의 연결된 이름을 선택하고 <Profile name> 페이지에서 공유 관리를 선택합니다.
4. AWS RAM 사용 설명서의 리소스 공유 업데이트 단계를 수행할 수 있는 AWS RAM 콘솔로 이동합니다.

AWS RAM 콘솔을 사용하여 소유한 공유 Route 53 Profile을 공유 해제하려면

AWS RAM 사용 설명서에서 리소스 공유 업데이트를 참조하세요.

를 사용하여 소유한 공유 Route 53 Profile을 공유 해제하려면 AWS CLI

disassociate-resource-share 명령을 사용합니다.

공유 Route 53 Profile 식별

소유자와 소비자는 Route 53 콘솔과 AWS CLI를 사용하여 공유된 Route 53 Profiles를 식별할 수 있습니다.

Route 53 콘솔을 사용하여 공유 Route 53 Profile을 식별하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 프로필을 선택합니다.

3. 프로파일이 공유된 경우 프로파일 테이블에는 나와 공유됨 텍스트가 포함됩니다.

   프로파일을 공유하면 프로파일 테이블에 공유로 나열됩니다.

를 사용하여 공유 Route 53 Profile을 식별하려면 AWS CLI

get-profile 또는 list-profile 명령을 사용합니다. 이 명령은 소유한 Route 53 Profiles 및 Route 53 Profiles 공유 상태에 대한 정보를 반환합니다.

공유 Route 53 Profiles에 대한 책임 및 권한

소유자에 대한 권한

프로파일 소유자는 소비자 계정에서 수행한 리소스 연결을 포함하여 프로파일 리소스 연결을 보고, 관리 및 삭제할 수 있습니다. 소유자는 자신이 소유한 VPC 연결을 보고 삭제할 수 있습니다. 또한 프로파일 소유자만 자신이 소유한 프로파일을 삭제할 수 있으며, 이에 따라 프로파일의 모든 리소스 연결도 자동으로 제거됩니다.

소비자에 대한 권한

공유 프로파일의 소비자에 대한 기본 권한은 읽기 전용입니다. 읽기 전용 권한을 사용하면 연결된 리소스를 보고 VPC에 연결할 수 있지만 리소스 연결을 관리할 수는 없습니다.

소유자는 AWS RAM 콘솔에서 고객 관리형 권한을 생성할 수도 있습니다. 자세한 내용은 AWS RAM 사용 설명서의 고객 관리형 권한 생성 및 사용을 참조하세요.

결제 및 측정

Route 53 Profiles은 VPC 연결 수를 기준으로 요금이 청구됩니다. 프로파일 소유자는 고객의 VPC 연결에 대한 청구서를 책임집니다.

인스턴스 할당량

프로파일 소유자와 소비자는 리전의 계정당 Route 53 Profiles 수를 제외하고 동일한 할당량을 공유합니다. 자세한 내용은 Route 53 Profiles의 할당량 섹션을 참조하세요.

Amazon Route 53 on Outposts란 무엇인가요?

AWS Outposts 는 AWS 인프라, 서비스, APIs 및 도구를 고객 온프레미스로 확장하는 완전관리형 서비스입니다. 이를 통해 고객은 에서와 동일한 프로그래밍 인터페이스를 사용하여 온프레미스 워크로드로 AWS 서비스를 실행할 수 있습니다 AWS 리전. 자세한 내용은 AWS Outposts 사용 설명서의 란 무엇입니까 AWS Outposts?를 참조하세요.

Route 53 on Outposts는 다음과 같은 두 가지 기능을 제공합니다.

- AWS Outposts에서 시작되는 모든 DNS 쿼리를 캐싱하는 해석기입니다.
- 인바운드 및 아웃바운드 엔드포인트를 배포할 때 Outpost와 온프레미스 DNS 해석기 간의 하이브리드 연결입니다.

자세한 내용은 Amazon Route 53 Resolver란 무엇인가요? 단원을 참조하십시오.

또한 Route 53 on Outposts는 가장 가까운 AWS 리전으로 왕복하는 대신 Outpost 내에서 쿼리를 해결할 수 있도록 하여 네트워크 지연 시간을 줄여줍니다.

> **Note**
>
> Outposts의 Route 53와 호환되지 않는 AWS Outposts 랙 버전이 있는 경우 AWS 계정 팀에 알림이 전송되고 업그레이드에 도움이 되도록 연락드릴 것입니다 AWS Outposts.

Amazon Route 53 on Outposts 기능

다음 표는 Route 53 on Outposts 기능을 Amazon Route 53 기능과 비교한 내용입니다.

Route 53 on Outposts와 Route 53 비교

Feature	Route 53 on Outposts의 이용 가능 여부
Route 53 Resolver	예. 해석기는 Outpost 랙에서 호스팅되는 애플리케이션,의 피어링된 VPC AWS 리전및 공개적으로 액세스할 수 있는 호스트 이름에 대한 레코드의 로컬 캐시를 유지합니다.

Feature	Route 53 on Outposts의 이용 가능 여부
상태 확인	아니요. 상태 확인은 AWS 리전에서 계산 및 보고됩니다. Outpost가 클라우드와의 연결을 끊으면 엔드포인트가 열리지 않아 백업으로 장애 조치를 수행할 수 없습니다.
해석기 엔드포인트	예. Outpost 랙의 해석기 엔드포인트를 사용하면 온프레미스의 DNS 서버에서 DNS 쿼리를 전달하고 수신할 수 있습니다. 엔드포인트에는 IPv4 엔드포인트 유형만 사용할 수 있습니다.
Route 53 Resolver DNS Firewall	사용할 수 없습니다.
트래픽 흐름	사용할 수 없습니다.

AWS Outposts 가 VPC에서 연결 해제될 때의 Route 53 Resolver 동작

AWS Outposts 가에서 연결 해제된 경우 Outpost AWS 리전의 Resolver는 다음과 같이 작동합니다.

- 컨트롤 플레인 변경은 불가능합니다.
- 상태 확인 및 DNS 장애 조치 기능은 사용할 수 없습니다.
- Outposts에서 로컬로 호스팅되는 리소스에 대한 DNS 쿼리는 해결되지만 Outpost가 연결이 끊긴 상태일 때 리소스의 IP 주소가 업데이트되면 응답이 유효하지 않을 수 있습니다.
- 리전 내 VPC에 호스팅된 리소스에 대한 DNS 쿼리는 확인할 수 있습니다. 그러나에 대한 Outpost 연결이 복원 AWS 리전 될 때까지 리소스에 액세스할 수 없습니다.
- 퍼블릭 DNS 리소스에 대한 DNS 쿼리는 Outpost의 Route 53 Resolver 캐시에서 사용할 수 있는 경우 확인할 수 있습니다.

AWS Outposts에서 Route 53 Resolver 시작하기

랙을 주문한 후 AWS Outposts 가이드의 생성 AWS Outposts에 설명된 대로 AWS Outposts 랙이 전달되면 Outpost에서 Resolver를 설정할 수 있습니다.

또한 API를 사용하여 Route 53 on Outposts를 관리할 수 있습니다. 자세한 내용은 Resolver on Outpost actions를 참조하세요.

> **Important**
>
> AWS Outposts에 해석기 캐시를 생성하는 데 최대 30~150분이 걸릴 수 있습니다.

AWS Outposts 랙을 전송한 후 Outposts의 Route 53에 옵트인할 수 있습니다.

Outpost의 해석기를 구성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 해석기를 확장한 다음 Outposts로 이동합니다.
3. 탐색 모음에서 AWS Outposts 가 위치한 리전을 선택합니다.
4. Outpost의 해석기 페이지에서 해석기 생성을 선택합니다.
5. 해석기 생성 페이지에서:
   - 아래에서 해석기를 생성 AWS Outposts 하려는를 AWS Outposts 선택합니다.
   - 해석기 이름 텍스트 상자에 해석기 이름을 입력합니다.
   - 해석기에 권장되는 인스턴스 유형이 Amazon EC2 인스턴스에 채워지면 하나를 선택합니다.

     인스턴스 유형에 대한 자세한 내용은 Outpost의 해석기 할당량 섹션을 참조하세요.
   - 인스턴스 수에서 VPC 해석기의 탄력적 인터페이스 인스턴스 개수를 선택합니다. 기본값은 4입니다.

     에 Resolver를 지원하는 인스턴스 유형이 AWS Outposts 없는 경우 Resolver를 생성할 수 없습니다.
6. Create Resolver(해석기 생성)를 선택합니다.

   Outpost의 해석기 페이지에서 해석기 생성을 모니터링할 수 있습니다.

인바운드 엔드포인트 생성

Outpost의 해석기를 생성한 후에는 인바운드 및 아웃바운드 엔드포인트를 모두 추가하여 온프레미스 네트워크와 주고받는 DNS 쿼리를 확인할 수 있습니다.

Outpost의 해석기에 대한 인바운드 엔드포인트를 구성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 해석기를 확장한 다음 Outposts로 이동합니다.
3. 탐색 모음에서 AWS Outposts 가 위치한 리전을 선택합니다.
4. 작동 중인 해석기 옆의 확인란을 선택하고 세부 정보 보기를 선택합니다.
5. 인바운드 엔드포인트 테이블에서 인바운드 엔드포인트 생성을 선택합니다.
6. 인바운드 엔드포인트 생성 페이지에서 해당 값을 입력합니다. 자세한 내용은 Outpost에서 인바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값 단원을 참조하십시오.
7. Create endpoint(엔드포인트 생성)을 선택합니다.

Outpost에서 인바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값

인바운드 엔드포인트를 생성하거나 편집할 때 다음 값을 지정합니다.

Outpost ID

AWS Outposts VPC에서 Resolver에 대한 엔드포인트를 생성하는 경우 ID입니다 AWS Outposts .

엔드포인트 이름

기억하기 쉬운 이름을 사용하면 대시보드에서 인바운드 엔드포인트를 쉽게 찾을 수 있습니다.

region-name 리전에 있는 VPC

네트워크의 모든 인바운드 DNS 쿼리가 Resolver로 가는 중에 이 VPC를 통과합니다.

이 엔드포인트에 대한 보안 그룹

이 아웃바운드 엔드포인트에 대한 액세스를 제어하는 데 사용할 하나 이상의 보안 그룹의 ID입니다. 지정한 보안 그룹에는 인바운드 규칙이 하나 이상 포함되어야 합니다. 인바운드 규칙은 포트 53에서 TCP 및 UDP 액세스를 허용해야 합니다. 엔드포인트를 만든 후에는 이 값을 변경할 수 없습니다.

자세한 내용은 Amazon VPC 사용 설명서의 VPC의 보안 그룹을 참조하세요.

IP 주소

네트워크에 있는 DNS 해석기가 DNS 쿼리를 전달할 IP 주소입니다. 중복성을 위해 최소 두 개의 IP 주소를 지정해야 합니다. 다음 사항에 유의하세요.

IP 주소 및 Amazon VPC 탄력적 네트워크 인터페이스

지정한 가용 영역, 서브넷 및 IP 주소의 각 조합에 대해 Resolver는 Amazon VPC 탄력적 네트워크 인터페이스를 생성합니다. 엔드포인트의 IP 주소별 초당 최대 동시 DNS 쿼리 수는 Route 53 Resolver의 할당량 섹션을 참조하세요. 각 탄력적 네트워크 인터페이스의 요금에 대한 정보는 Amazon Route 53 요금 페이지의 Amazon Route 53을 참조하세요.

> **Note**
>
> Resolver 엔드포인트에는 프라이빗 IP 주소가 있습니다. 이러한 IP 주소는 엔드포인트의 수명 기간 동안 변경되지 않습니다.

IP 주소마다 다음 값을 지정하세요. VPC in the region-name Region(region-name 리전에 있는 VPC)에서 지정한 VPC의 가용 영역에 각 IP 주소가 있어야 합니다.

가용 영역

DNS 쿼리가 VPC로 가는 도중 통과할 가용 영역. 지정한 가용 영역을 서브넷으로 구성해야 합니다.

서브넷

DNS 쿼리를 전달할 IP 주소가 포함된 서브넷입니다. 서브넷에는 사용 가능한 IP 주소가 있어야 합니다.

IPv4 주소에 대한 서브넷을 지정합니다. IPv6은 지원되지 않습니다.

IP 주소

DNS 쿼리를 전달하려는 IP 주소입니다.

Resolver가 지정된 서브넷의 사용 가능한 IP 주소 중에서 자동으로 IP 주소를 선택하도록 할지, 아니면 직접 IP 주소를 지정할지 선택합니다.

IP 주소를 직접 선택할 경우 IPv4 주소를 입력합니다. IPv6은 지원되지 않습니다.

Tags

한 개 이상의 키와 해당 값을 지정합니다. 예를 들어 키에 Cost center를 지정하고 값에 456을 지정할 수 있습니다.

다음은에서 청구서를 구성하기 위해 AWS Billing and Cost Management 제공하는 태그입니다. 다른 용도로도 태그를 사용할 수 있습니다 AWS . 비용 할당 태그 사용에 대한 자세한 내용은 AWS Billing 사용 설명서의 비용 할당 태그 사용을 참조하십시오.

아웃바운드 엔드포인트 생성

Route 53 Resolver를 선택하고 구성한 후에는 인바운드 및 아웃바운드 엔드포인트를 모두 추가하여 온프레미스 네트워크에 대한 DNS 쿼리를 확인할 수도 있습니다.

Outpost의 해석기에 대한 아웃바운드 엔드포인트를 구성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 해석기를 확장한 다음 Outposts로 이동합니다.
3. 탐색 모음에서 AWS Outposts 가 위치한 리전을 선택합니다.
4. 작동 중인 해석기 옆의 확인 표시를 선택하고 세부 정보 보기를 선택합니다.
5. 아웃바운드 엔드포인트 테이블에서 아웃바운드 엔드포인트 생성을 선택합니다.
6. 아웃바운드 엔드포인트 생성 페이지에서 해당 값을 입력합니다. 자세한 내용은 Outpost에서 인바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값 단원을 참조하십시오.
7. Create endpoint(엔드포인트 생성)을 선택합니다.

AWS Outposts에서 아웃바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값

인바운드 엔드포인트를 생성하거나 편집할 때 다음 값을 지정합니다.

Outpost ID

AWS Outposts VPC에서 Resolver에 대한 엔드포인트를 생성하는 경우 ID입니다 AWS Outposts .

엔드포인트 이름

기억하기 쉬운 이름을 사용하면 대시보드에서 인바운드 엔드포인트를 쉽게 찾을 수 있습니다.

region-name 리전에 있는 VPC

네트워크의 모든 인바운드 DNS 쿼리가 Resolver로 가는 중에 이 VPC를 통과합니다.

이 엔드포인트에 대한 보안 그룹

이 VPC에 대한 액세스를 제어하는 데 사용할 보안 그룹 하나 이상의 ID. 지정한 보안 그룹에는 인바운드 규칙이 하나 이상 포함되어야 합니다. 인바운드 규칙은 포트 53에서 TCP 및 UDP 액세스를 허용해야 합니다. 엔드포인트를 만든 후에는 이 값을 변경할 수 없습니다.

자세한 내용은 Amazon VPC 사용 설명서의 VPC의 보안 그룹을 참조하세요.

IP 주소

네트워크에 있는 DNS 해석기가 DNS 쿼리를 전달할 IP 주소입니다. 중복성을 위해 최소 두 개의 IP 주소를 지정해야 합니다. 다음 사항에 유의하세요.

IP 주소 및 Amazon VPC 탄력적 네트워크 인터페이스

지정한 가용 영역, 서브넷 및 IP 주소의 각 조합에 대해 Resolver는 Amazon VPC 탄력적 네트워크 인터페이스를 생성합니다. 엔드포인트의 IP 주소별 초당 최대 동시 DNS 쿼리 수는 Route 53 Resolver의 할당량 섹션을 참조하세요. 각 탄력적 네트워크 인터페이스의 요금에 대한 정보는 Amazon Route 53 요금 페이지의 "Amazon Route 53"을 참조하십시오.

> **Note**
>
> Resolver 엔드포인트에는 프라이빗 IP 주소가 있습니다. 이러한 IP 주소는 엔드포인트의 수명 기간 동안 변경되지 않습니다.

IP 주소마다 다음 값을 지정하세요. VPC in the region-name Region(region-name 리전에 있는 VPC)에서 지정한 VPC의 가용 영역에 각 IP 주소가 있어야 합니다.

가용 영역

DNS 쿼리가 VPC로 가는 도중 통과할 가용 영역. 지정한 가용 영역을 서브넷으로 구성해야 합니다.

서브넷

DNS 쿼리를 전달할 IP 주소가 포함된 서브넷입니다. 서브넷에는 사용 가능한 IP 주소가 있어야 합니다.

IPv4 주소에 대한 서브넷을 지정합니다. IPv6은 지원되지 않습니다.

IP 주소

DNS 쿼리를 전달하려는 IP 주소입니다.

Resolver가 지정된 서브넷의 사용 가능한 IP 주소 중에서 자동으로 IP 주소를 선택하도록 할지, 아니면 직접 IP 주소를 지정할지 선택합니다.

IP 주소를 직접 선택할 경우 IPv4 주소를 입력합니다. IPv6은 지원되지 않습니다.

Tags

한 개 이상의 키와 해당 값을 지정합니다. 예를 들어 키에 Cost center를 지정하고 값에 456을 지정할 수 있습니다.

이는에서 청구서를 구성하기 위해 AWS Billing and Cost Management 제공하는 태그입니다. 다른 용도로도 태그를 사용할 수 있습니다 AWS . 비용 할당 태그 사용에 대한 자세한 내용은 AWS Billing 사용 설명서의 비용 할당 태그 사용을 참조하십시오.

아웃바운드 엔드포인트에 대한 전달 규칙 생성

아웃바운드 엔드포인트에 대한 전달 규칙을 생성할 수도 있습니다. 자세한 내용은 전달 규칙을 생성하고 VPC 한 개 이상에 규칙을 연결하려면 단원을 참조하세요.

Outpost의 해석기 관리

Outpost의 해석기를 관리하려면 해당 절차를 수행합니다.

주제

- Outpost의 해석기 편집
- Outpost의 해석기 상태 보기
- Outpost의 해석기 삭제

Outpost의 해석기 편집

Outpost의 해석기를 편집하려면 다음 절차를 수행합니다.

Outpost의 해석기를 편집하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 해석기를 확장한 다음 Outposts로 이동합니다.
3. 탐색 모음에서 AWS Outposts 가 위치한 리전을 선택합니다.

4. 작동 중인 해석기 옆의 확인 표시를 선택하고 편집을 선택합니다.
5. 다음 정보를 편집할 수 있습니다.

   - 해석기 이름
   - 인스턴스 유형
   - 인스턴스의 수
6. 편집을 완료한 후 변경사항 저장을 선택합니다.

Outpost의 해석기 상태 보기

Outpost의 해석기 상태를 보려면 다음 절차를 수행합니다.

인바운드 엔드포인트의 상태를 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 해석기를 확장한 다음 Outposts로 이동합니다.
3. 탐색 모음에서 AWS Outposts 가 위치한 리전을 선택합니다.
4. 작동 중인 해석기 옆의 확인 표시를 선택하고 세부 정보 보기를 선택합니다.
5. Outpost의 해석기 페이지에 있는 상태 열에는 다음 값 중 하나가 포함됩니다.

   [생성 중]

   Outpost의 해석기가 현재 생성 중입니다.

   Operational(작동)

   Outpost의 해석기가 올바르게 구성되었습니다.

   업데이트 중

   Outpost의 해석기가 인스턴스 유형을 업데이트하고 있습니다.

   작업 필요

   이 해석기가 비정상 상태이므로 해석기가 자동으로 복구되지 않습니다. 문제를 해결하려면 인스턴스가 Outpost의 Resolver를 지원할 AWS Outposts 수 있는지 확인하는 것이 좋습니다.

   [삭제 중]

   Outpost의 해석기가 현재 삭제 중입니다.

실패한 생성

Outpost의 해석기 생성이 실패했습니다.

실패한 삭제

Outpost의 해석기 삭제가 실패했습니다. 이 문제를 해결하려면 몇 분 후에 다시 시도하세요.

Outpost의 해석기 삭제

> **Note**
>
> Outpost의 해석기를 삭제하려면 먼저 해석기와 관련된 모든 엔드포인트를 삭제해야 합니다.

Outpost의 해석기를 삭제하려면 다음 절차를 수행합니다.

Outpost의 해석기를 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 해석기를 확장한 다음 Outposts로 이동합니다.
3. 탐색 모음에서 AWS Outposts 가 위치한 리전을 선택합니다.
4. 작동 중인 해석기 옆의 확인란을 선택하고 삭제를 선택합니다.
5. 해석기 삭제 대화 상자에서 텍스트 상자에 **`delete`**를 입력하고 삭제를 선택합니다.

Outpost의 해석기에서 인바운드 엔드포인트 관리

Outpost의 해석기에서 인바운드 엔드포인트를 관리하려면 해당 절차를 수행합니다.

주제

- 인바운드 엔드포인트 보기 및 편집
- 인바운드 엔드포인트의 상태 보기
- 인바운드 엔드포인트 삭제

인바운드 엔드포인트 보기 및 편집

인바운드 엔드포인트의 설정을 보고 편집하려면 다음 절차를 수행하세요.

인바운드 엔드포인트의 설정을 보고 편집하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 해석기를 확장한 다음 Outposts로 이동합니다.
3. 탐색 모음에서 AWS Outposts 가 위치한 리전을 선택합니다.
4. 작동 중인 해석기 옆의 확인란을 선택하고 세부 정보 보기를 선택합니다.
5. 인바운드 엔드포인트 목록에서 설정을 보거나 편집하려는 엔드포인트의 옵션을 선택합니다.
6. 세부 정보 보기 또는 편집을 선택합니다.

   인바운드 엔드포인트의 값에 대한 자세한 내용은 Outpost에서 인바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값을 참조하세요.
7. 편집을 선택한 경우 해당 값을 입력하고 저장을 선택합니다.

인바운드 엔드포인트의 상태 보기

인바운드 엔드포인트의 상태를 보려면 다음 절차를 수행합니다.

인바운드 엔드포인트의 상태를 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 해석기를 확장한 다음 Outposts로 이동합니다.
3. 탐색 모음에서 AWS Outposts 가 위치한 리전을 선택합니다.
4. 작동 상태인 해석기 옆의 확인란을 선택하고 세부 정보 보기를 선택합니다.
5. 인바운드 엔드포인트 목록의 상태 열에는 다음 값 중 하나가 포함됩니다.

   [생성 중]

   Resolver가 이 엔드포인트에 대해 하나 이상의 Amazon VPC 네트워크 인터페이스를 생성 및 구성하고 있습니다.

Operational(작동)

이 엔드포인트의 Amazon VPC 네트워크 인터페이스가 올바르게 구성되어 있고 네트워크와 Resolver 사이의 인바운드 또는 아웃바운드 DNS 쿼리를 전달할 수 있습니다.

업데이트 중

하나 이상의 네트워크 인터페이스를 이 엔드포인트와 연결 또는 연결 해제하는 중입니다.

Auto recovering(자동 복구 중)

Resolver가 이 엔드포인트와 연결된 네트워크 인터페이스 중 하나 이상을 복구하려고 합니다. 복구 프로세스 중 IP 주소당(네트워크 인터페이스당) DNS 쿼리 수의 제한 때문에 엔드포인트가 제한된 용량으로 작동합니다. 현재 제한은 Route 53 Resolver의 할당량 섹션을 참조하세요.

작업 필요

이 엔드포인트가 정상 상태가 아니므로 Resolver가 자동으로 복구할 수 없습니다. 문제를 해결하려면 엔드포인트와 연관된 각 IP 주소를 점검하는 것이 좋습니다. 사용할 수 없는 각 IP 주소에 대해 다른 IP 주소를 추가한 다음 사용할 수 없는 IP 주소를 삭제하세요. 엔드포인트에는 항상 두 개 이상의 IP 주소가 포함되어야 합니다. 작업 필요 상태에는 다양한 원인이 있을 수 있습니다. 일반적인 두 가지 원인은 다음과 같습니다.

- 엔드포인트와 연결된 하나 이상의 네트워크 인터페이스가 Amazon VPC를 사용하여 삭제되었습니다.
- Resolver의 제어를 벗어난 어떤 이유로 인해 네트워크 인터페이스를 생성할 수 없습니다.

[삭제 중]

해석기가 이 엔드포인트 및 연관된 네트워크 인터페이스를 삭제하고 있습니다.

인바운드 엔드포인트 삭제

인바운드 엔드포인트를 삭제하려면 다음 절차를 수행하세요.

> **Important**
>
> 인바운드 엔드포인트를 삭제하면 더 이상 네트워크의 DNS 쿼리가 엔드포인트에 지정된 VPC의 Resolver로 전달되지 않습니다.

인바운드 엔드포인트를 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 해석기를 확장한 다음 Outposts로 이동합니다.
3. 탐색 모음에서 AWS Outposts 가 위치한 리전을 선택합니다.
4. 작동 상태인 해석기 옆의 확인란을 선택하고 세부 정보 보기를 선택합니다.
5. 삭제하려는 엔드포인트 옆의 확인란을 선택합니다.
6. Delete(삭제)를 선택합니다.
7. 엔드포인트를 삭제하도록 확인하려면 엔드포인트 이름을 입력하고 제출을 선택합니다.

Outpost의 해석기에서 아웃바운드 엔드포인트 관리

Outpost의 해석기에서 아웃바운드 엔드포인트를 관리하려면 해당 절차를 수행합니다.

주제

- 아웃바운드 엔드포인트 보기 및 편집
- 아웃바운드 엔드포인트의 상태 보기
- 아웃바운드 엔드포인트 삭제

아웃바운드 엔드포인트 보기 및 편집

아웃바운드 엔드포인트의 설정을 보고 편집하려면 다음 절차를 수행하세요.

아웃바운드 엔드포인트의 설정을 보고 편집하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 해석기를 확장한 다음 Outposts로 이동합니다.
3. 탐색 모음에서 AWS Outposts 가 위치한 리전을 선택합니다.
4. 작동 상태인 해석기 옆의 확인란을 선택하고 세부 정보 보기를 선택합니다.
5. 아웃바운드 엔드포인트 목록에서 설정을 보거나 편집하려는 엔드포인트 옆의 확인란을 선택합니다.
6. 세부 정보 보기 또는 편집을 선택합니다.

아웃바운드 엔드포인트의 값에 대한 자세한 내용은 AWS Outposts에서 아웃바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값 섹션을 참조하세요.

7. 편집을 선택한 경우 해당 값을 입력한 후 저장을 선택합니다.

아웃바운드 엔드포인트의 상태 보기

아웃바운드 엔드포인트의 상태를 보려면 다음 절차를 수행합니다.

아웃바운드 엔드포인트의 상태를 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 해석기를 확장한 다음 Outposts로 이동합니다.
3. 탐색 모음에서 AWS Outposts 가 위치한 리전을 선택합니다.
4. 작동 상태인 해석기 옆의 확인란을 선택하고 세부 정보 보기를 선택합니다.
5. 아웃바운드 엔드포인트 목록에서 상태 열에는 다음 값 중 하나가 포함됩니다.

   [생성 중]

   Resolver가 이 엔드포인트에 대해 하나 이상의 Amazon VPC 네트워크 인터페이스를 생성 및 구성하고 있습니다.

   Operational(작동)

   이 엔드포인트의 Amazon VPC 네트워크 인터페이스가 올바르게 구성되어 있고 네트워크와 Resolver 사이의 인바운드 또는 아웃바운드 DNS 쿼리를 전달할 수 있습니다.

   업데이트 중

   하나 이상의 네트워크 인터페이스를 이 엔드포인트와 연결 또는 연결 해제하는 중입니다.

   Auto recovering(자동 복구 중)

   Resolver가 이 엔드포인트와 연결된 네트워크 인터페이스 중 하나 이상을 복구하려고 합니다. 복구 프로세스 중 IP 주소당(네트워크 인터페이스당) DNS 쿼리 수의 제한 때문에 엔드포인트가 제한된 용량으로 작동합니다. 현재 제한은 Route 53 Resolver의 할당량 섹션을 참조하세요.

작업 필요

이 엔드포인트가 정상 상태가 아니므로 Resolver가 자동으로 복구할 수 없습니다. 문제를 해결하려면 엔드포인트와 연관된 각 IP 주소를 점검하는 것이 좋습니다. 사용할 수 없는 각 IP 주소에 대해 다른 IP 주소를 추가한 다음 사용할 수 없는 IP 주소를 삭제하세요. 엔드포인트에는 항상 두 개 이상의 IP 주소가 포함되어야 합니다. 작업 필요 상태에는 다양한 원인이 있을 수 있습니다. 일반적인 두 가지 원인은 다음과 같습니다.

- 엔드포인트와 연결된 하나 이상의 네트워크 인터페이스가 Amazon VPC를 사용하여 삭제되었습니다.
- Resolver의 제어를 벗어난 어떤 이유로 인해 네트워크 인터페이스를 생성할 수 없습니다.

[삭제 중]

해석기가 이 엔드포인트 및 연관된 네트워크 인터페이스를 삭제하고 있습니다.

아웃바운드 엔드포인트 삭제

엔드포인트를 삭제하려면 VPC와 연결된 모든 규칙부터 먼저 삭제해야 합니다.

아웃바운드 엔드포인트를 삭제하려면 다음 절차를 수행하세요.

> **Important**
>
> 아웃바운드 엔드포인트를 삭제하면 Resolver는 삭제된 아웃바운드 엔드포인트를 지정하는 규칙에 대해 더 이상 DNS 쿼리를 VPC에서 네트워크로 전달하지 않습니다.

아웃바운드 엔드포인트를 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 해석기를 확장한 다음 Outposts로 이동합니다.
3. 작동 상태인 해석기 옆의 확인란을 선택하고 세부 정보 보기를 선택합니다.
4. 아웃바운드 엔드포인트 목록에서 삭제하려는 엔드포인트의 옵션을 선택합니다.
5. Delete(삭제)를 선택합니다.
6. 엔드포인트를 삭제하도록 확인하려면 엔드포인트 이름을 입력하고 제출을 선택합니다.

를 사용하여 Amazon Route 53 및 Amazon Route 53 Resolver 리소스 생성 AWS CloudFormation

Amazon Route 53 및 Amazon Route 53 Resolver 는 AWS 리소스 및 인프라를 생성하고 관리하는 데 소요되는 시간을 줄일 수 있도록 리소스를 모델링하고 설정하는 데 도움이 되는 AWS CloudFormation 서비스와 통합됩니다. 원하는 모든 AWS 리소스를 설명하는 템플릿을 생성하고 해당 리소스를 AWS CloudFormation 프로비저닝하고 구성합니다.

를 사용하면 템플릿을 재사용하여 Route 53 및 Route 53 Resolver 리소스를 일관되고 반복적으로 설정할 AWS CloudFormation수 있습니다. 리소스를 한 번 설명한 다음 여러 AWS 계정 및 리전에서 동일한 리소스를 반복적으로 프로비저닝합니다.

Route 53, Route 53 Resolver 및 AWS CloudFormation 템플릿

Route 53, Route 53 Resolver 및 관련 서비스에 대한 리소스를 프로비저닝하고 구성하려면 AWS CloudFormation 템플릿을 이해해야 합니다. 템플릿은 JSON 또는 YAML로 서식 지정된 텍스트 파일입니다. 이러한 템플릿은 AWS CloudFormation 스택에서 프로비저닝하려는 리소스를 설명합니다. JSON 또는 YAML에 익숙하지 않은 경우 Designer를 사용하여 AWS CloudFormation AWS CloudFormation 템플릿을 시작할 수 있습니다. 자세한 내용은 AWS CloudFormation 사용 설명서에서 AWS CloudFormation Designer이란 무엇입니까?를 참조하세요.

Route 53는 AWS CloudFormation에서 다음 리소스 유형 생성을 지원합니다.

- `AWS::Route53::DNSSEC`
- `AWS::Route53::HealthCheck`
- `AWS::Route53::HostedZone`
- `AWS::Route53::KeySigningKey`
- `AWS::Route53::RecordSet`
- `AWS::Route53::RecordSetGroup`

Route 53 리소스에 대한 JSON 및 YAML 템플릿의 예를 비롯한 자세한 내용은 AWS CloudFormation 사용 설명서의 Amazon Route 53 리소스 유형 참조를 참조하십시오.

Route 53 Resolver는 AWS CloudFormation에서 다음 리소스 유형 생성을 지원합니다.

- `AWS::Route53Resolver::FirewallDomainList`

- `AWS::Route53Resolver::FirewallDomainList`
- `AWS::Route53Resolver::FirewallRuleGroupAssociation`
- `AWS::Route53Resolver::ResolverDNSSECConfig`
- `AWS::Route53Resolver::ResolverEndpoint`
- `AWS::Route53Resolver::ResolverQueryLoggingConfig`
- `AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation`
- `AWS::Route53Resolver::ResolverRule`
- `AWS::Route53Resolver::ResolverRuleAssociation`

Route 53 Resolver 리소스에 대한 JSON 및 YAML 템플릿의 예를 비롯한 자세한 내용은 AWS CloudFormation 사용 설명서의 Amazon Route 53 Resolver 리소스 유형 참조를 참조하십시오.

에 대해 자세히 알아보기 AWS CloudFormation

에 대해 자세히 알아보려면 다음 리소스를 AWS CloudFormation참조하세요.

- AWS CloudFormation
- AWS CloudFormation 사용 설명서
- AWS CloudFormation API Reference
- AWS CloudFormation 명령줄 인터페이스 사용 설명서

AWS SDKs를 사용하는 Route 53의 코드 예제

다음 코드 예제에서는 AWS 소프트웨어 개발 키트(SDK)와 함께 Route 53를 사용하는 방법을 보여줍니다.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

코드 예시

- AWS SDK 또는 CLI와 RegisterDomain 함께 사용
- AWS SDK 또는 CLI와 ViewBilling 함께 사용

AWS SDKs를 사용하는 Route 53의 코드 예제

다음 코드 예제에서는 AWS 소프트웨어 개발 키트(SDK)와 함께 Route 53를 사용하는 방법을 보여줍니다.

작업은 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 작업은 관련 시나리오의 컨텍스트에 따라 표시되며, 개별 서비스 함수를 직접적으로 호출하는 방법을 보여줍니다.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

코드 예시

- AWS SDKs 사용하는 Route 53의 기본 예제
  - AWS SDKs 사용하는 Route 53에 대한 작업
    - CLI로 ChangeResourceRecordSets 사용
    - CLI로 CreateHostedZone 사용
    - CLI로 DeleteHostedZone 사용
    - CLI로 GetHostedZone 사용
    - AWS SDK 또는 CLI와 ListHostedZones 함께 사용
    - CLI로 ListHostedZonesByName 사용
    - CLI로 ListQueryLoggingConfigs 사용

AWS SDKs 사용하는 Route 53의 기본 예제

다음 코드 예제에서는 AWS SDK에서 Amazon Route 53의 기본 사항을 사용하는 방법을 보여줍니다.

예시

- AWS SDKs 사용하는 Route 53에 대한 작업
  - CLI로 ChangeResourceRecordSets 사용
  - CLI로 CreateHostedZone 사용
  - CLI로 DeleteHostedZone 사용

- CLI로 GetHostedZone 사용
- AWS SDK 또는 CLI와 ListHostedZones 함께 사용
- CLI로 ListHostedZonesByName 사용
- CLI로 ListQueryLoggingConfigs 사용

AWS SDKs 사용하는 Route 53에 대한 작업

다음 코드 예제에서는 AWS SDKs를 사용하여 개별 Route 53 작업을 수행하는 방법을 보여줍니다. 각 예제에는 GitHub에 대한 링크가 포함되어 있습니다. 여기에서 코드 설정 및 실행에 대한 지침을 찾을 수 있습니다.

다음 예제에는 가장 일반적으로 사용되는 작업만 포함되어 있습니다. 전체 목록은 Amazon Route 53 API Reference를 참조하세요.

예시

- CLI로 ChangeResourceRecordSets 사용
- CLI로 CreateHostedZone 사용
- CLI로 DeleteHostedZone 사용
- CLI로 GetHostedZone 사용
- AWS SDK 또는 CLI와 ListHostedZones 함께 사용
- CLI로 ListHostedZonesByName 사용
- CLI로 ListQueryLoggingConfigs 사용

CLI로 **ChangeResourceRecordSets** 사용

다음 코드 예제는 ChangeResourceRecordSets의 사용 방법을 보여 줍니다.

CLI

AWS CLI

리소스 레코드 세트를 생성, 업데이트 또는 삭제하려면

다음 change-resource-record-sets 명령은 파일 C:\awscli\route53\change-resource-record-sets.json에서 hosted-zone-id Z1R8UBAEXAMPLE 및 JSON 형식 구성을 사용하여 리소스 레코드 세트를 생성합니다.

```
aws route53 change-resource-record-sets --hosted-zone-id Z1R8UBAEXAMPLE --change-batch file://C:\awscli\route53\change-resource-record-sets.json
```

자세한 내용은 Amazon Route 53 API 참조의 POST ChangeResourceRecordSets를 참조하세요.

JSON 파일의 구성은 생성하려는 리소스 레코드 세트의 종류에 따라 달라집니다.

BasicWeightedAliasWeighted AliasLatencyLatency AliasFailoverFailover Alias

기본 구문:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ]
      }
    },
    {...}
  ]
}
```

가중 구문:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
```

```
        "SetIdentifier": "unique description for this resource record set",
        "Weight": value between 0 and 255,
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ],
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

별칭 구문:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
 Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
 hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

가중 별칭 구문:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Weight": value between 0 and 255,
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
 Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
 hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

지연 시간 구문:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Region": "Amazon EC2 region name",
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
```

```
          {...}
        ],
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

지연 시간 별칭 구문:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Region": "Amazon EC2 region name",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
 Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
 hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

장애 조치 구문:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
```

```
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Failover": "PRIMARY" | "SECONDARY",
        "TTL": time to live in seconds,
        "ResourceRecords": [
          {
            "Value": "applicable value for the record type"
          },
          {...}
        ],
        "HealthCheckId": "ID of an Amazon Route 53 health check"
      }
    },
    {...}
  ]
}
```

장애 조치 별칭 구문:

```
{
  "Comment": "optional comment about the changes in this change batch request",
  "Changes": [
    {
      "Action": "CREATE"|"DELETE"|"UPSERT",
      "ResourceRecordSet": {
        "Name": "DNS domain name",
        "Type": "SOA"|"A"|"TXT"|"NS"|"CNAME"|"MX"|"PTR"|"SRV"|"SPF"|"AAAA",
        "SetIdentifier": "unique description for this resource record set",
        "Failover": "PRIMARY" | "SECONDARY",
        "AliasTarget": {
          "HostedZoneId": "hosted zone ID for your CloudFront distribution,
 Amazon S3 bucket, Elastic Load Balancing load balancer, or Amazon Route 53
 hosted zone",
          "DNSName": "DNS domain name for your CloudFront distribution, Amazon S3
 bucket, Elastic Load Balancing load balancer, or another resource record set in
 this hosted zone",
          "EvaluateTargetHealth": true|false
        },
        "HealthCheckId": "optional ID of an Amazon Route 53 health check"
      }
```

```
    },
    {...}
  ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 ChangeResourceRecordSets를 참조하세요.

PowerShell

PowerShell용 도구

예제 1: 이 예제에서는 www.example.com의 A 레코드를 생성하고 test.example.com의 A 레코드를 192.0.2.3에서 192.0.2.1로 변경합니다. 변경 TXT 유형 레코드의 값은 큰따옴표로 묶여야 합니다. 자세한 내용은 Amazon Route 53 설명서를 참조하세요. Get-R53Change cmdlet을 사용하여 변경 사항이 완료되는 시기를 확인할 수 있습니다.

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "TXT"
$change1.ResourceRecordSet.TTL = 600
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="item 1 item 2 item 3"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "DELETE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "test.example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.3"})

$change3 = New-Object Amazon.Route53.Model.Change
$change3.Action = "CREATE"
$change3.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change3.ResourceRecordSet.Name = "test.example.com"
$change3.ResourceRecordSet.Type = "A"
$change3.ResourceRecordSet.TTL = 600
$change3.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.1"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
```

```
 ChangeBatch_Comment="This change batch creates a TXT record for www.example.com.
 and changes the A record for test.example.com. from 192.0.2.3 to 192.0.2.1."
 ChangeBatch_Change=$change1,$change2,$change3
}

Edit-R53ResourceRecordSet @params
```

예제 2: 이 예제에서는 별칭 리소스 레코드 세트를 생성하는 방법을 보여줍니다. 'Z222222222'는 별칭 리소스 레코드 세트를 생성하는 Amazon Route 53 호스팅 영역의 ID입니다. 'example.com'은 별칭을 생성하려는 zone apex이고 'www.example.com'은 역시 별칭을 생성하려는 하위 도메인입니다. 'Z1111111111111'은 로드 밸런서의 호스팅 영역 ID의 예이고 'example-load-balancer-1111111111.us-east-1.elb.amazonaws.com'은 Amazon Route 53가 example.com 및 www.example.com에 대한 쿼리에 응답하는 로드 밸런서 도메인 이름의 예입니다. 자세한 내용은 Amazon Route 53 설명서를 참조하세요. Get-R53Change cmdlet을 사용하여 변경 사항이 완료되는 시기를 확인할 수 있습니다.

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z222222222"
```

```
 ChangeBatch_Comment="This change batch creates two alias resource record sets,
 one for the zone apex, example.com, and one for www.example.com, that both point
 to example-load-balancer-1111111111.us-east-1.elb.amazonaws.com."
 ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

예제 3: 이 예제는 www.example.com에 대한 두 개의 A 레코드를 생성합니다. 1/4(1/(1+3))의 경우 Amazon Route 53는 첫 번째 리소스 레코드 세트(192.0.2.9 및 192.0.2.10)에 대한 두 값으로 www.example.com 쿼리에 응답합니다. 3/4(3/(1+3))의 경우 Amazon Route 53는 두 번째 리소스 레코드 세트(192.0.2.11 및 192.0.2.12)의 두 값으로 www.example.com 쿼리에 응답합니다. 자세한 내용은 Amazon Route 53 설명서를 참조하세요. Get-R53Change cmdlet을 사용하여 변경 사항이 완료되는 시기를 확인할 수 있습니다.

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "www.example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Rack 2, Positions 4 and 5"
$change1.ResourceRecordSet.Weight = 1
$change1.ResourceRecordSet.TTL = 600
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.9"})
$change1.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.10"})

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "www.example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "Rack 5, Positions 1 and 2"
$change2.ResourceRecordSet.Weight = 3
$change2.ResourceRecordSet.TTL = 600
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.11"})
$change2.ResourceRecordSet.ResourceRecords.Add(@{Value="192.0.2.12"})

$params = @{
    HostedZoneId="Z1PA6795UKMFR9"
    ChangeBatch_Comment="This change creates two weighted resource record sets,
 each of which has two values."
    ChangeBatch_Change=$change1,$change2
```

```
}

Edit-R53ResourceRecordSet @params
```

예제 4: 이 예제는 example.com이 가중치 기반 별칭 리소스 레코드 세트를 생성하려는 도메인이라고 가정하여 가중치 기반 별칭 리소스 레코드 세트를 생성하는 방법을 보여줍니다. SetIdentifier는 두 개의 가중치 기반 별칭 리소스 레코드 세트를 서로 구분합니다. 이름 및 유형 요소는 두 리소스 레코드 세트에 대해 동일한 값을 갖기 때문에 이 요소가 필요합니다. Z1111111111111 및 Z3333333333333은 DNSName 값으로 지정된 ELB 로드 밸런서에 대한 호스팅 영역 ID의 예입니다. example-load-balancer-2222222222.us-east-1.elb.amazonaws.com 및 example-load-balancer-4444444444.us-east-1.elb.amazonaws.com은 Amazon Route 53가 example.com 쿼리에 응답하는 Elastic Load Balancing 도메인의 예입니다. 자세한 내용은 Amazon Route 53 설명서를 참조하세요. Get-R53Change cmdlet을 사용하여 변경 사항이 완료되는 시기를 확인할 수 있습니다.

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "1"
$change1.ResourceRecordSet.Weight = 3
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-2222222222.us-east-1.elb.amazonaws.com."
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "2"
$change2.ResourceRecordSet.Weight = 1
$change2.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z3333333333333"
```

```
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-4444444444.us-east-1.elb.amazonaws.com."
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $false

$params = @{
    HostedZoneId="Z5555555555"
    ChangeBatch_Comment="This change batch creates two weighted alias resource
 record sets. Amazon Route 53 responds to queries for example.com with the first
 ELB domain 3/4ths of the times and the second one 1/4th of the time."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

예제 5: 이 예제에서는 두 개의 지연 시간 별칭 리소스 레코드 세트를 생성합니다. 하나는 미국 서부(오리건) 리전(us-west-2)의 ELB 로드 밸런서용이고 다른 하나는 아시아 태평양(싱가포르) 리전(ap-southeast-1)의 로드 밸런서용입니다. 자세한 내용은 Amazon Route 53 설명서를 참조하세요. Get-R53Change cmdlet을 사용하여 변경 사항이 완료되는 시기를 확인할 수 있습니다.

```
$change1 = New-Object Amazon.Route53.Model.Change
$change1.Action = "CREATE"
$change1.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change1.ResourceRecordSet.Name = "example.com"
$change1.ResourceRecordSet.Type = "A"
$change1.ResourceRecordSet.SetIdentifier = "Oregon load balancer 1"
$change1.ResourceRecordSet.Region = us-west-2
$change1.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change1.ResourceRecordSet.AliasTarget.HostedZoneId = "Z1111111111111"
$change1.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-2222222222.us-west-2.elb.amazonaws.com"
$change1.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$change2 = New-Object Amazon.Route53.Model.Change
$change2.Action = "CREATE"
$change2.ResourceRecordSet = New-Object Amazon.Route53.Model.ResourceRecordSet
$change2.ResourceRecordSet.Name = "example.com"
$change2.ResourceRecordSet.Type = "A"
$change2.ResourceRecordSet.SetIdentifier = "Singapore load balancer 1"
$change2.ResourceRecordSet.Region = ap-southeast-1
$change2.ResourceRecordSet.AliasTarget = New-Object
 Amazon.Route53.Model.AliasTarget
$change2.ResourceRecordSet.AliasTarget.HostedZoneId = "Z2222222222222"
```

```
$change2.ResourceRecordSet.AliasTarget.DNSName = "example-load-
balancer-1111111111.ap-southeast-1.elb.amazonaws.com"
$change2.ResourceRecordSet.AliasTarget.EvaluateTargetHealth = $true

$params = @{
    HostedZoneId="Z5555555555"
    ChangeBatch_Comment="This change batch creates two latency resource
 record sets, one for the US West (Oregon) region and one for the Asia Pacific
 (Singapore) region."
    ChangeBatch_Change=$change1,$change2
}

Edit-R53ResourceRecordSet @params
```

- API 세부 정보는 AWS Tools for PowerShell Cmdlet 참조의 ChangeResourceRecordSets를 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

CLI로 **CreateHostedZone** 사용

다음 코드 예제는 CreateHostedZone의 사용 방법을 보여 줍니다.

CLI

AWS CLI

호스팅 영역 생성

다음 create-hosted-zone 명령은 호출자 참조 2014-04-01-18:47를 사용하여 example.com라는 호스팅 영역을 추가합니다. 선택적 주석에는 공백이 포함되므로 주석을 따옴표로 묶어야 합니다.

```
aws route53 create-hosted-zone --name example.com --caller-
reference 2014-04-01-18:47 --hosted-zone-config Comment="command-line version"
```

자세한 내용은 Amazon Route 53 개발자 안내서의 호스팅 영역 작업을 참조하세요.

- API 세부 정보는 AWS CLI 명령 참조의 CreateHostedZone을 참조하세요.

PowerShell

PowerShell용 도구

예제 1: 재사용 가능한 위임 세트와 연결된 'example.com'이라는 새 호스팅 영역을 생성합니다. 작업을 두 번 실행할 위험 없이 필요한 경우 요청을 재시도하려면 CallerReference 파라미터에 값을 제공해야 합니다. 호스팅 영역은 VPC에서 생성되므로 자동으로 비공개 상태이며, -HostedZoneConfig_PrivateZone 파라미터를 설정해서는 안 됩니다.

```
$params = @{
    Name="example.com"
    CallerReference="myUniqueIdentifier"
    HostedZoneConfig_Comment="This is my first hosted zone"
    DelegationSetId="NZ8X2CISAMPLE"
    VPC_VPCId="vpc-1a2b3c4d"
    VPC_VPCRegion="us-east-1"
}

New-R53HostedZone @params
```

- API 세부 정보는 AWS Tools for PowerShell Cmdlet 참조의 CreateHostedZone을 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

CLI로 **DeleteHostedZone** 사용

다음 코드 예제는 DeleteHostedZone의 사용 방법을 보여 줍니다.

CLI

AWS CLI

호스팅 영역을 삭제하려면

다음 delete-hosted-zone 명령은 Z36KTIQEXAMPLE이라는 id가 있는 호스팅 영역을 삭제합니다.

```
aws route53 delete-hosted-zone --id Z36KTIQEXAMPLE
```

- API 세부 정보는 AWS CLI 명령 참조의 DeleteHostedZone을 참조하세요.

PowerShell

PowerShell용 도구

예제 1: 지정된 ID로 호스팅 영역을 삭제합니다. -Force 스위치 파라미터를 추가하지 않으면 명령이 진행되기 전에 확인 메시지가 표시됩니다.

```
Remove-R53HostedZone -Id Z1PA6795UKMFR9
```

- API 세부 정보는 AWS Tools for PowerShell Cmdlet 참조의 DeleteHostedZone을 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

CLI로 **GetHostedZone** 사용

다음 코드 예제는 GetHostedZone의 사용 방법을 보여 줍니다.

CLI

AWS CLI

호스팅 영역에 대한 정보를 가져오려면

다음 get-hosted-zone 명령은 Z1R8UBAEXAMPLE이라는 id가 있는 호스팅 영역의 정보를 가져옵니다.

```
aws route53 get-hosted-zone --id Z1R8UBAEXAMPLE
```

- API 세부 정보는 AWS CLI 명령 참조의 GetHostedZone을 참조하세요.

PowerShell

PowerShell용 도구

예제 1: ID Z1D633PJN98FT9를 사용하여 호스팅 영역의 세부 정보를 반환합니다.

```
Get-R53HostedZone -Id Z1D633PJN98FT9
```

- API 세부 정보는 AWS Tools for PowerShell Cmdlet 참조의 GetHostedZone을 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **ListHostedZones** 함께 사용

다음 코드 예제는 ListHostedZones의 사용 방법을 보여 줍니다.

CLI

AWS CLI

현재 AWS 계정과 연결된 호스팅 영역을 나열하려면

다음 list-hosted-zones 명령은 현재 AWS 계정과 연결된 처음 100개의 호스팅 영역에 대한 요약 정보를 나열합니다.

```
aws route53 list-hosted-zones
```

100개를 초과한 호스팅 영역이 있거나 해당 영역을 100개 미만의 그룹으로 나열하려면 --max-items 파라미터를 포함합니다. 예를 들어, 호스팅 영역을 한 번에 하나씩 나열하려면 다음 명령을 사용합니다.

```
aws route53 list-hosted-zones --max-items 1
```

다음 호스팅 영역에 대한 정보를 보려면 이전 명령에 대한 응답에서 NextToken의 값을 가져와 --starting-token 파라미터에 포함합니다. 예를 들면 다음과 같습니다.

```
aws route53 list-hosted-zones --max-items 1 --starting-token Z3M3LMPEXAMPLE
```

- API 세부 정보는 AWS CLI 명령 참조의 ListHostedZones를 참조하세요.

PowerShell

PowerShell용 도구

예제 1: 모든 퍼블릭 및 프라이빗 호스팅 영역을 출력합니다.

```
Get-R53HostedZoneList
```

예제 2: ID NZ8X2CISAMPLE이 있는 재사용 가능한 위임 세트와 연결된 호스팅된 영역을 모두 출력합니다.

```
Get-R53HostedZoneList -DelegationSetId NZ8X2CISAMPLE
```

- API 세부 정보는 AWS Tools for PowerShell Cmdlet 참조의 ListHostedZones를 참조하세요.

Rust

SDK for Rust

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
async fn show_host_info(client: &aws_sdk_route53::Client) -> Result<(),
 aws_sdk_route53::Error> {
    let hosted_zone_count = client.get_hosted_zone_count().send().await?;

    println!(
        "Number of hosted zones in region : {}",
        hosted_zone_count.hosted_zone_count(),
    );

    let hosted_zones = client.list_hosted_zones().send().await?;

    println!("Zones:");

    for hz in hosted_zones.hosted_zones() {
        let zone_name = hz.name();
        let zone_id = hz.id();

        println!("  ID :   {}", zone_id);
        println!("  Name : {}", zone_name);
        println!();
    }

    Ok(())
}
```

- API 세부 정보는AWS SDK for Rust API reference의 ListHostedZones를 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

CLI로 **ListHostedZonesByName** 사용

다음 코드 예제는 ListHostedZonesByName의 사용 방법을 보여 줍니다.

CLI

AWS CLI

다음 명령은 도메인 이름별로 최대 100개의 호스팅 영역을 나열합니다.

```
aws route53 list-hosted-zones-by-name
```

출력:

```
{
  "HostedZones": [
      {
          "ResourceRecordSetCount": 2,
          "CallerReference": "test20150527-2",
          "Config": {
              "Comment": "test2",
              "PrivateZone": false
          },
          "Id": "/hostedzone/Z119WBBTVP5WFX",
          "Name": "2.example.com."
      },
      {
          "ResourceRecordSetCount": 2,
          "CallerReference": "test20150527-1",
          "Config": {
              "Comment": "test",
              "PrivateZone": false
          },
          "Id": "/hostedzone/Z3P5QSUBK4POTI",
```

```
            "Name": "www.example.com."
        }
    ],
    "IsTruncated": false,
    "MaxItems": "100"
}
```

다음 명령은 www.example.com으로 시작하는 이름을 기준으로 호스팅 영역을 나열합니다.

```
aws route53 list-hosted-zones-by-name --dns-name www.example.com
```

출력:

```
{
    "HostedZones": [
        {
            "ResourceRecordSetCount": 2,
            "CallerReference": "mwunderl20150527-1",
            "Config": {
                "Comment": "test",
                "PrivateZone": false
            },
            "Id": "/hostedzone/Z3P5QSUBK4POTI",
            "Name": "www.example.com."
        }
    ],
    "DNSName": "www.example.com",
    "IsTruncated": false,
    "MaxItems": "100"
}
```

- API 세부 정보는 AWS CLI 명령 참조의 ListHostedZonesByName을 참조하세요.

PowerShell

PowerShell용 도구

예제 1: 모든 퍼블릭 및 프라이빗 호스팅 영역을 도메인 이름별로 ASCII 순서로 반환합니다.

```
Get-R53HostedZonesByName
```

예제 2: 지정된 DNS 이름부터 시작하여 도메인 이름별로 ASCII 순서로 퍼블릭 및 프라이빗 호스팅 영역을 반환합니다.

```
Get-R53HostedZonesByName -DnsName example2.com
```

- API 세부 정보는 AWS Tools for PowerShell Cmdlet 참조의 ListHostedZonesByName을 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

CLI로 **ListQueryLoggingConfigs** 사용

다음 코드 예제는 ListQueryLoggingConfigs의 사용 방법을 보여 줍니다.

CLI

AWS CLI

쿼리 로깅 구성을 나열하려면

다음 list-query-logging-configs 예제에서는 호스팅 영역에 대한 AWS 계정의 처음 100개 쿼리 로깅 구성에 대한 정보를 나열합니다Z1OX3WQEXAMPLE.

```
aws route53 list-query-logging-configs \
    --hosted-zone-id Z1OX3WQEXAMPLE
```

출력:

```
{
    "QueryLoggingConfigs": [
        {
            "Id": "964ff34e-ae03-4f06-80a2-9683cexample",
            "HostedZoneId": "Z1OX3WQEXAMPLE",
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-
east-1:111122223333:log-group:/aws/route53/example.com:*"
        }
    ]
}
```

자세한 내용은 Amazon Route 53 개발자 안내서의 DNS 쿼리 로깅을 참조하세요.

- API 세부 정보는 AWS CLI 명령 참조의 ListQueryLoggingConfigs를 참조하세요.

PowerShell

PowerShell용 도구

예제 1: 이 예제는 현재 AWS 계정와 연결된 DNS 쿼리 로깅에 대한 모든 구성을 반환합니다.

```
Get-R53QueryLoggingConfigList
```

출력:

```
Id                                   HostedZoneId   CloudWatchLogsLogGroupArn
--                                   ------------   -------------------------
59b0fa33-4fea-4471-a88c-926476aaa40d Z385PDS6EAAAZR arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example1.com:*
ee528e95-4e03-4fdc-9d28-9e24ddaaa063 Z94SJHBV1AAAAZ arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example2.com:*
e38dddda-ceb6-45c1-8cb7-f0ae56aaaa2b Z3MEQ8T7AAA1BF arn:aws:logs:us-
east-1:111111111112:log-group:/aws/route53/example3.com:*
```

- API 세부 정보는 AWS Tools for PowerShell Cmdlet 참조의 ListQueryLoggingConfigs를 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDKs를 사용한 Route 53 도메인 등록의 코드 예제

다음 코드 예제에서는 AWS 소프트웨어 개발 키트(SDK)와 함께 Route 53 도메인 등록을 사용하는 방법을 보여줍니다.

기본 사항은 서비스 내에서 필수 작업을 수행하는 방법을 보여주는 코드 예제입니다.

작업은 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 작업은 관련 시나리오의 컨텍스트에 따라 표시되며, 개별 서비스 함수를 직접적으로 호출하는 방법을 보여줍니다.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

시작

Route 53 도메인 등록 소개

다음 코드 예제에서는 Route 53 도메인 등록을 사용하여 시작하는 방법을 보여 줍니다.

.NET

AWS SDK for .NET

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
public static class HelloRoute53Domains
{
    static async Task Main(string[] args)
    {
        // Use the AWS .NET Core Setup package to set up dependency injection for
 the Amazon Route 53 domain registration service.
        // Use your AWS profile name, or leave it blank to use the default
 profile.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonRoute53Domains>()
            ).Build();

        // Now the client is available for injection.
        var route53Client =
 host.Services.GetRequiredService<IAmazonRoute53Domains>();

        // You can use await and any of the async methods to get a response.
        var response = await route53Client.ListPricesAsync(new ListPricesRequest
 { Tld = "com" });
        Console.WriteLine($"Hello Amazon Route 53 Domains! Following are prices
 for .com domain operations:");
        var comPrices = response.Prices.FirstOrDefault();
        if (comPrices != null)
        {
```

```
            Console.WriteLine($"\tRegistration:
 {comPrices.RegistrationPrice?.Price} {comPrices.RegistrationPrice?.Currency}");
            Console.WriteLine($"\tRenewal: {comPrices.RenewalPrice?.Price}
 {comPrices.RenewalPrice?.Currency}");
        }
    }
}
```

- API 세부 정보는 AWS SDK for .NET API 참조의 ListPrices를 참조하십시오.

Java

SDK for Java 2.x

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.route53domains.Route53DomainsClient;
import software.amazon.awssdk.services.route53.model.Route53Exception;
import software.amazon.awssdk.services.route53domains.model.DomainPrice;
import software.amazon.awssdk.services.route53domains.model.ListPricesRequest;
import software.amazon.awssdk.services.route53domains.model.ListPricesResponse;
import java.util.List;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * This Java code examples performs the following operation:
 *
 * 1. Invokes ListPrices for at least one domain type, such as the “com” type
 * and displays the prices for Registration and Renewal.
```

```
 *
 */
public class HelloRoute53 {
    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

    public static void main(String[] args) {
        final String usage = "\n" +
                "Usage:\n" +
                "    <hostedZoneId> \n\n" +
                "Where:\n" +
                "    hostedZoneId - The id value of an existing hosted zone. \n";

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String domainType = args[0];
        Region region = Region.US_EAST_1;
        Route53DomainsClient route53DomainsClient =
 Route53DomainsClient.builder()
                .region(region)
                .build();

        System.out.println(DASHES);
        System.out.println("Invokes ListPrices for at least one domain type.");
        listPrices(route53DomainsClient, domainType);
        System.out.println(DASHES);
    }

    public static void listPrices(Route53DomainsClient route53DomainsClient,
 String domainType) {
        try {
            ListPricesRequest pricesRequest = ListPricesRequest.builder()
                    .maxItems(10)
                    .tld(domainType)
                    .build();

            ListPricesResponse response =
 route53DomainsClient.listPrices(pricesRequest);
            List<DomainPrice> prices = response.prices();
            for (DomainPrice pr : prices) {
                System.out.println("Name: " + pr.name());
```

```
                System.out.println(
                        "Registration: " + pr.registrationPrice().price() + " " +
 pr.registrationPrice().currency());
                System.out.println("Renewal: " + pr.renewalPrice().price() + " "
 + pr.renewalPrice().currency());
                System.out.println("Transfer: " + pr.transferPrice().price() + "
 " + pr.transferPrice().currency());
                System.out.println("Transfer: " + pr.transferPrice().price() + "
 " + pr.transferPrice().currency());
                System.out.println("Change Ownership: " +
 pr.changeOwnershipPrice().price() + " "
                        + pr.changeOwnershipPrice().currency());
                System.out.println(
                        "Restoration: " + pr.restorationPrice().price() + " " +
 pr.restorationPrice().currency());
                System.out.println(" ");
            }

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- API 세부 정보는 AWS SDK for Java 2.x API 참조의 ListPrices를 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
/**
 Before running this Kotlin code example, set up your development environment,
 including your credentials.
```

```
 For more information, see the following documentation topic:
 https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html
 */
suspend fun main(args: Array<String>) {
    val usage = """
        Usage:
           <domainType>

       Where:
           domainType - The domain type (for example, com).
    """

    if (args.size != 1) {
        println(usage)
        exitProcess(0)
    }

    val domainType = args[0]
    println("Invokes ListPrices using a Paginated method.")
    listPricesPaginated(domainType)
}

suspend fun listPricesPaginated(domainType: String) {
    val pricesRequest =
        ListPricesRequest {
            maxItems = 10
            tld = domainType
        }

    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        route53DomainsClient
            .listPricesPaginated(pricesRequest)
            .transform { it.prices?.forEach { obj -> emit(obj) } }
            .collect { pr ->
                println("Registration: ${pr.registrationPrice}
 ${pr.registrationPrice?.currency}")
                println("Renewal: ${pr.renewalPrice?.price}
 ${pr.renewalPrice?.currency}")
                println("Transfer: ${pr.transferPrice?.price}
 ${pr.transferPrice?.currency}")
                println("Restoration: ${pr.restorationPrice?.price}
 ${pr.restorationPrice?.currency}")
            }
```

```
    }
}
```

- API 세부 정보는 AWS SDK for Kotlin API 참조의 ListPrices를 참조하십시오.

코드 예제

- AWS SDKs를 사용한 Route 53 도메인 등록의 기본 예제
  - Route 53 도메인 등록 소개
  - AWS SDK를 사용한 Route 53 도메인 등록의 기본 사항 알아보기
  - AWS SDKs를 사용한 Route 53 도메인 등록 작업
    - AWS SDK 또는 CLI와 CheckDomainAvailability 함께 사용
    - AWS SDK 또는 CLI와 CheckDomainTransferability 함께 사용
    - AWS SDK 또는 CLI와 GetDomainDetail 함께 사용
    - AWS SDK 또는 CLI와 GetDomainSuggestions 함께 사용
    - AWS SDK 또는 CLI와 GetOperationDetail 함께 사용
    - AWS SDK 또는 CLI와 ListDomains 함께 사용
    - AWS SDK 또는 CLI와 ListOperations 함께 사용
    - AWS SDK와 ListPrices 함께 사용
    - AWS SDK 또는 CLI와 RegisterDomain 함께 사용
    - AWS SDK 또는 CLI와 ViewBilling 함께 사용

AWS SDKs를 사용한 Route 53 도메인 등록의 기본 예제

다음 코드 예제에서는 Amazon Route 53 domain registration SDKs에서의 기본 사항을 AWS 사용하는 방법을 보여줍니다.

예시

- Route 53 도메인 등록 소개
- AWS SDK를 사용한 Route 53 도메인 등록의 기본 사항 알아보기
- AWS SDKs를 사용한 Route 53 도메인 등록 작업
  - AWS SDK 또는 CLI와 CheckDomainAvailability 함께 사용
  - AWS SDK 또는 CLI와 CheckDomainTransferability 함께 사용

- AWS SDK 또는 CLI와 GetDomainDetail 함께 사용
- AWS SDK 또는 CLI와 GetDomainSuggestions 함께 사용
- AWS SDK 또는 CLI와 GetOperationDetail 함께 사용
- AWS SDK 또는 CLI와 ListDomains 함께 사용
- AWS SDK 또는 CLI와 ListOperations 함께 사용
- AWS SDK와 ListPrices 함께 사용
- AWS SDK 또는 CLI와 RegisterDomain 함께 사용
- AWS SDK 또는 CLI와 ViewBilling 함께 사용

Route 53 도메인 등록 소개

다음 코드 예제는 Route 53 도메인 등록 사용을 시작하는 방법을 보여 줍니다.

.NET

AWS SDK for .NET

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
public static class HelloRoute53Domains
{
    static async Task Main(string[] args)
    {
        // Use the AWS .NET Core Setup package to set up dependency injection for
 the Amazon Route 53 domain registration service.
        // Use your AWS profile name, or leave it blank to use the default
 profile.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonRoute53Domains>()
            ).Build();

        // Now the client is available for injection.
```

```
        var route53Client =
 host.Services.GetRequiredService<IAmazonRoute53Domains>();

        // You can use await and any of the async methods to get a response.
        var response = await route53Client.ListPricesAsync(new ListPricesRequest
 { Tld = "com" });
        Console.WriteLine($"Hello Amazon Route 53 Domains! Following are prices
 for .com domain operations:");
        var comPrices = response.Prices.FirstOrDefault();
        if (comPrices != null)
        {
            Console.WriteLine($"\tRegistration:
 {comPrices.RegistrationPrice?.Price} {comPrices.RegistrationPrice?.Currency}");
            Console.WriteLine($"\tRenewal: {comPrices.RenewalPrice?.Price}
 {comPrices.RenewalPrice?.Currency}");
        }
    }
}
```

- API 세부 정보는 AWS SDK for .NET API 참조의 ListPrices를 참조하십시오.

Java

SDK for Java 2.x

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.route53domains.Route53DomainsClient;
import software.amazon.awssdk.services.route53.model.Route53Exception;
import software.amazon.awssdk.services.route53domains.model.DomainPrice;
import software.amazon.awssdk.services.route53domains.model.ListPricesRequest;
import software.amazon.awssdk.services.route53domains.model.ListPricesResponse;
import java.util.List;

/**
 * Before running this Java V2 code example, set up your development
```

```
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * This Java code examples performs the following operation:
 *
 * 1. Invokes ListPrices for at least one domain type, such as the “com” type
 * and displays the prices for Registration and Renewal.
 *
 */
public class HelloRoute53 {
    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

    public static void main(String[] args) {
        final String usage = "\n" +
                "Usage:\n" +
                "    <hostedZoneId> \n\n" +
                "Where:\n" +
                "    hostedZoneId - The id value of an existing hosted zone. \n";

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String domainType = args[0];
        Region region = Region.US_EAST_1;
        Route53DomainsClient route53DomainsClient =
 Route53DomainsClient.builder()
                .region(region)
                .build();

        System.out.println(DASHES);
        System.out.println("Invokes ListPrices for at least one domain type.");
        listPrices(route53DomainsClient, domainType);
        System.out.println(DASHES);
    }

    public static void listPrices(Route53DomainsClient route53DomainsClient,
 String domainType) {
```

```
        try {
            ListPricesRequest pricesRequest = ListPricesRequest.builder()
                    .maxItems(10)
                    .tld(domainType)
                    .build();

            ListPricesResponse response =
 route53DomainsClient.listPrices(pricesRequest);
            List<DomainPrice> prices = response.prices();
            for (DomainPrice pr : prices) {
                System.out.println("Name: " + pr.name());
                System.out.println(
                        "Registration: " + pr.registrationPrice().price() + " " +
 pr.registrationPrice().currency());
                System.out.println("Renewal: " + pr.renewalPrice().price() + " "
 + pr.renewalPrice().currency());
                System.out.println("Transfer: " + pr.transferPrice().price() + "
 " + pr.transferPrice().currency());
                System.out.println("Transfer: " + pr.transferPrice().price() + "
 " + pr.transferPrice().currency());
                System.out.println("Change Ownership: " +
 pr.changeOwnershipPrice().price() + " "
                        + pr.changeOwnershipPrice().currency());
                System.out.println(
                        "Restoration: " + pr.restorationPrice().price() + " " +
 pr.restorationPrice().currency());
                System.out.println(" ");
            }

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- API 세부 정보는 AWS SDK for Java 2.x API 참조의 ListPrices를 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
/**
 Before running this Kotlin code example, set up your development environment,
 including your credentials.

 For more information, see the following documentation topic:
 https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html
 */
suspend fun main(args: Array<String>) {
    val usage = """
        Usage:
           <domainType>

       Where:
           domainType - The domain type (for example, com).
    """

    if (args.size != 1) {
        println(usage)
        exitProcess(0)
    }

    val domainType = args[0]
    println("Invokes ListPrices using a Paginated method.")
    listPricesPaginated(domainType)
}

suspend fun listPricesPaginated(domainType: String) {
    val pricesRequest =
        ListPricesRequest {
            maxItems = 10
            tld = domainType
```

```
        }

    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        route53DomainsClient
            .listPricesPaginated(pricesRequest)
            .transform { it.prices?.forEach { obj -> emit(obj) } }
            .collect { pr ->
                println("Registration: ${pr.registrationPrice}
 ${pr.registrationPrice?.currency}")
                println("Renewal: ${pr.renewalPrice?.price}
 ${pr.renewalPrice?.currency}")
                println("Transfer: ${pr.transferPrice?.price}
 ${pr.transferPrice?.currency}")
                println("Restoration: ${pr.restorationPrice?.price}
 ${pr.restorationPrice?.currency}")
            }
    }
}
```

- API 세부 정보는AWS SDK for Kotlin API 참조의 ListPrices를 참조하십시오.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK를 사용한 Route 53 도메인 등록의 기본 사항 알아보기

다음 코드 예제는 다음과 같은 작업을 수행하는 방법을 보여줍니다.

- 현재 도메인과 작년의 작업을 나열합니다.
- 작년의 결제 내역과 도메인 유형의 가격을 봅니다.
- 도메인 제안을 가져옵니다.
- 도메인 가용성 및 이전 가능성을 확인합니다.
- 선택 사항으로 도메인 등록을 요청할 수도 있습니다.
- 작업 세부 정보를 가져옵니다.
- 선택 사항으로 도메인 세부 정보를 가져올 수 있습니다.

.NET

AWS SDK for .NET

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

명령 프롬프트에서 대화형 시나리오를 실행합니다.

```
public static class Route53DomainScenario
{
    /*
    Before running this .NET code example, set up your development environment,
 including your credentials.

    This .NET example performs the following tasks:
        1. List current domains.
        2. List operations in the past year.
        3. View billing for the account in the past year.
        4. View prices for domain types.
        5. Get domain suggestions.
        6. Check domain availability.
        7. Check domain transferability.
        8. Optionally, request a domain registration.
        9. Get an operation detail.
       10. Optionally, get a domain detail.
   */

    private static Route53Wrapper _route53Wrapper = null!;
    private static IConfiguration _configuration = null!;

    static async Task Main(string[] args)
    {
        // Set up dependency injection for the Amazon service.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureLogging(logging =>
                logging.AddFilter("System", LogLevel.Debug)
                    .AddFilter<DebugLoggerProvider>("Microsoft",
 LogLevel.Information)
```

```
                    .AddFilter<ConsoleLoggerProvider>("Microsoft",
LogLevel.Trace))
                    .ConfigureServices((_, services) =>
            services.AddAWSService<IAmazonRoute53Domains>()
                .AddTransient<Route53Wrapper>()
            )
            .Build();

        _configuration = new ConfigurationBuilder()
            .SetBasePath(Directory.GetCurrentDirectory())
            .AddJsonFile("settings.json") // Load settings from .json file.
            .AddJsonFile("settings.local.json",
                true) // Optionally, load local settings.
            .Build();

        var logger = LoggerFactory.Create(builder =>
        {
            builder.AddConsole();
        }).CreateLogger(typeof(Route53DomainScenario));

        _route53Wrapper = host.Services.GetRequiredService<Route53Wrapper>();

        Console.WriteLine(new string('-', 80));
        Console.WriteLine("Welcome to the Amazon Route 53 domains example
scenario.");
        Console.WriteLine(new string('-', 80));

        try
        {
            await ListDomains();
            await ListOperations();
            await ListBillingRecords();
            await ListPrices();
            await ListDomainSuggestions();
            await CheckDomainAvailability();
            await CheckDomainTransferability();
            var operationId = await RequestDomainRegistration();
            await GetOperationalDetail(operationId);
            await GetDomainDetails();
        }
        catch (Exception ex)
        {
            logger.LogError(ex, "There was a problem executing the scenario.");
        }
```

```
        Console.WriteLine(new string('-', 80));
        Console.WriteLine("The Amazon Route 53 domains example scenario is
complete.");
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List account registered domains.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListDomains()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"1. List account domains.");
        var domains = await _route53Wrapper.ListDomains();
        for (int i = 0; i < domains.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {domains[i].DomainName}");
        }

        if (!domains.Any())
        {
            Console.WriteLine("\tNo domains found in this account.");
        }

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List domain operations in the past year.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListOperations()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"2. List account domain operations in the past
year.");
        var operations = await _route53Wrapper.ListOperations(
            DateTime.Today.AddYears(-1));
        for (int i = 0; i < operations.Count; i++)
        {
            Console.WriteLine($"\tOperation Id: {operations[i].OperationId}");
            Console.WriteLine($"\tStatus: {operations[i].Status}");
```

```
            Console.WriteLine($"\tDate: {operations[i].SubmittedDate}");
        }
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List billing in the past year.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListBillingRecords()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"3. View billing for the account in the past year.");
        var billingRecords = await _route53Wrapper.ViewBilling(
            DateTime.Today.AddYears(-1),
            DateTime.Today);
        for (int i = 0; i < billingRecords.Count; i++)
        {
            Console.WriteLine($"\tBill Date:
{billingRecords[i].BillDate.ToShortDateString()}");
            Console.WriteLine($"\tOperation: {billingRecords[i].Operation}");
            Console.WriteLine($"\tPrice: {billingRecords[i].Price}");
        }
        if (!billingRecords.Any())
        {
            Console.WriteLine("\tNo billing records found in this account for the
past year.");
        }
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List prices for a few domain types.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListPrices()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"4. View prices for domain types.");
        var domainTypes = new List<string> { "net", "com", "org", "co" };

        var prices = await _route53Wrapper.ListPrices(domainTypes);
        foreach (var pr in prices)
        {
```

```
            Console.WriteLine($"\tName: {pr.Name}");
            Console.WriteLine($"\tRegistration: {pr.RegistrationPrice?.Price}
{pr.RegistrationPrice?.Currency}");
            Console.WriteLine($"\tRenewal: {pr.RenewalPrice?.Price}
{pr.RenewalPrice?.Currency}");
            Console.WriteLine($"\tTransfer: {pr.TransferPrice?.Price}
{pr.TransferPrice?.Currency}");
            Console.WriteLine($"\tChange Ownership:
{pr.ChangeOwnershipPrice?.Price} {pr.ChangeOwnershipPrice?.Currency}");
            Console.WriteLine($"\tRestoration: {pr.RestorationPrice?.Price}
{pr.RestorationPrice?.Currency}");
            Console.WriteLine();
        }
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List domain suggestions for a domain name.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task ListDomainSuggestions()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"5. Get domain suggestions.");
        string? domainName = null;
        while (domainName == null || string.IsNullOrWhiteSpace(domainName))
        {
            Console.WriteLine($"Enter a domain name to get available domain
suggestions.");
            domainName = Console.ReadLine();
        }

        var suggestions = await _route53Wrapper.GetDomainSuggestions(domainName,
true, 5);
        foreach (var suggestion in suggestions)
        {
            Console.WriteLine($"\tSuggestion Name: {suggestion.DomainName}");
            Console.WriteLine($"\tAvailability: {suggestion.Availability}");
        }
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Check availability for a domain name.
```

```
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task CheckDomainAvailability()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"6. Check domain availability.");
        string? domainName = null;
        while (domainName == null || string.IsNullOrWhiteSpace(domainName))
        {
            Console.WriteLine($"Enter a domain name to check domain
availability.");
            domainName = Console.ReadLine();
        }

        var availability = await
_route53Wrapper.CheckDomainAvailability(domainName);
        Console.WriteLine($"\tAvailability: {availability}");
        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Check transferability for a domain name.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task CheckDomainTransferability()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"7. Check domain transferability.");
        string? domainName = null;
        while (domainName == null || string.IsNullOrWhiteSpace(domainName))
        {
            Console.WriteLine($"Enter a domain name to check domain
transferability.");
            domainName = Console.ReadLine();
        }

        var transferability = await
_route53Wrapper.CheckDomainTransferability(domainName);
        Console.WriteLine($"\tTransferability: {transferability}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
```

```
    /// Check transferability for a domain name.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task<string?> RequestDomainRegistration()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"8. Optionally, request a domain registration.");

        Console.WriteLine($"\tNote: This example uses domain request settings in
 settings.json.");
        Console.WriteLine($"\tTo change the domain registration settings, set the
 values in that file.");
        Console.WriteLine($"\tRemember, registering an actual domain will incur
 an account billing cost.");
        Console.WriteLine($"\tWould you like to begin a domain registration? (y/
n)");
        var ynResponse = Console.ReadLine();
        if (ynResponse != null && ynResponse.Equals("y",
 StringComparison.InvariantCultureIgnoreCase))
        {
            string domainName = _configuration["DomainName"];
            ContactDetail contact = new ContactDetail();
            contact.CountryCode =
 CountryCode.FindValue(_configuration["Contact:CountryCode"]);
            contact.ContactType =
 ContactType.FindValue(_configuration["Contact:ContactType"]);

            _configuration.GetSection("Contact").Bind(contact);

            var operationId = await _route53Wrapper.RegisterDomain(
                domainName,
                Convert.ToBoolean(_configuration["AutoRenew"]),
                Convert.ToInt32(_configuration["DurationInYears"]),
                contact);
            if (operationId != null)
            {
                Console.WriteLine(
                    $"\tRegistration requested. Operation Id: {operationId}");
            }

            return operationId;
        }

        Console.WriteLine(new string('-', 80));
```

```
        return null;
    }

    /// <summary>
    /// Get details for an operation.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task GetOperationalDetail(string? operationId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"9. Get an operation detail.");

        var operationDetails =
            await _route53Wrapper.GetOperationDetail(operationId);

        Console.WriteLine(operationDetails);

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Optionally, get details for a registered domain.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task<string?> GetDomainDetails()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"10. Get details on a domain.");

        Console.WriteLine($"\tNote: you must have a registered domain to get
details.");
        Console.WriteLine($"\tWould you like to get domain details? (y/n)");
        var ynResponse = Console.ReadLine();
        if (ynResponse != null && ynResponse.Equals("y",
StringComparison.InvariantCultureIgnoreCase))
        {
            string? domainName = null;
            while (domainName == null)
            {
                Console.WriteLine($"\tEnter a domain name to get details.");
                domainName = Console.ReadLine();
            }
```

```
            var domainDetails = await
 _route53Wrapper.GetDomainDetail(domainName);
            Console.WriteLine(domainDetails);
        }

        Console.WriteLine(new string('-', 80));
        return null;
    }
}
```

Route 53 도메인 등록 작업 시나리오에서 사용한 래퍼 메서드입니다.

```
public class Route53Wrapper
{
    private readonly IAmazonRoute53Domains _amazonRoute53Domains;
    private readonly ILogger<Route53Wrapper> _logger;
    public Route53Wrapper(IAmazonRoute53Domains amazonRoute53Domains,
 ILogger<Route53Wrapper> logger)
    {
        _amazonRoute53Domains = amazonRoute53Domains;
        _logger = logger;
    }


    /// <summary>
    /// List prices for domain type operations.
    /// </summary>
    /// <param name="domainTypes">Domain types to include in the results.</param>
    /// <returns>The list of domain prices.</returns>
    public async Task<List<DomainPrice>> ListPrices(List<string> domainTypes)
    {
        var results = new List<DomainPrice>();
        var paginatePrices = _amazonRoute53Domains.Paginators.ListPrices(new
 ListPricesRequest());
        // Get the entire list using the paginator.
        await foreach (var prices in paginatePrices.Prices)
        {
            results.Add(prices);
        }
        return results.Where(p => domainTypes.Contains(p.Name)).ToList();
    }
```

```
    /// <summary>
    /// Check the availability of a domain name.
    /// </summary>
    /// <param name="domain">The domain to check for availability.</param>
    /// <returns>An availability result string.</returns>
    public async Task<string> CheckDomainAvailability(string domain)
    {
        var result = await _amazonRoute53Domains.CheckDomainAvailabilityAsync(
            new CheckDomainAvailabilityRequest
            {
                DomainName = domain
            }
        );
        return result.Availability.Value;
    }


    /// <summary>
    /// Check the transferability of a domain name.
    /// </summary>
    /// <param name="domain">The domain to check for transferability.</param>
    /// <returns>A transferability result string.</returns>
    public async Task<string> CheckDomainTransferability(string domain)
    {
        var result = await _amazonRoute53Domains.CheckDomainTransferabilityAsync(
            new CheckDomainTransferabilityRequest
            {
                DomainName = domain
            }
        );
        return result.Transferability.Transferable.Value;
    }


    /// <summary>
    /// Get a list of suggestions for a given domain.
    /// </summary>
    /// <param name="domain">The domain to check for suggestions.</param>
    /// <param name="onlyAvailable">If true, only returns available domains.</
param>
    /// <param name="suggestionCount">The number of suggestions to return.
 Defaults to the max of 50.</param>
```

```
    /// <returns>A collection of domain suggestions.</returns>
    public async Task<List<DomainSuggestion>> GetDomainSuggestions(string domain,
bool onlyAvailable, int suggestionCount = 50)
    {
        var result = await _amazonRoute53Domains.GetDomainSuggestionsAsync(
            new GetDomainSuggestionsRequest
            {
                DomainName = domain,
                OnlyAvailable = onlyAvailable,
                SuggestionCount = suggestionCount
            }
        );
        return result.SuggestionsList;
    }


    /// <summary>
    /// Get details for a domain action operation.
    /// </summary>
    /// <param name="operationId">The operational Id.</param>
    /// <returns>A string describing the operational details.</returns>
    public async Task<string> GetOperationDetail(string? operationId)
    {
        if (operationId == null)
            return "Unable to get operational details because ID is null.";
        try
        {
            var operationDetails =
                await _amazonRoute53Domains.GetOperationDetailAsync(
                    new GetOperationDetailRequest
                    {
                        OperationId = operationId
                    }
                );

            var details = $"\tOperation {operationId}:\n" +
                          $"\tFor domain {operationDetails.DomainName} on
{operationDetails.SubmittedDate.ToShortDateString()}.\n" +
                          $"\tMessage is {operationDetails.Message}.\n" +
                          $"\tStatus is {operationDetails.Status}.\n";

            return details;
        }
        catch (AmazonRoute53DomainsException ex)
```

```
        {
            return $"Unable to get operation details. Here's why: {ex.Message}.";
        }
    }


    /// <summary>
    /// Initiate a domain registration request.
    /// </summary>
    /// <param name="contact">Contact details.</param>
    /// <param name="domainName">The domain name to register.</param>
    /// <param name="autoRenew">True if the domain should automatically renew.</
param>
    /// <param name="duration">The duration in years for the domain
 registration.</param>
    /// <returns>The operation Id.</returns>
    public async Task<string?> RegisterDomain(string domainName, bool autoRenew,
 int duration, ContactDetail contact)
    {
        // This example uses the same contact information for admin, registrant,
 and tech contacts.
        try
        {
            var result = await _amazonRoute53Domains.RegisterDomainAsync(
                new RegisterDomainRequest()
                {
                    AdminContact = contact,
                    RegistrantContact = contact,
                    TechContact = contact,
                    DomainName = domainName,
                    AutoRenew = autoRenew,
                    DurationInYears = duration,
                    PrivacyProtectAdminContact = false,
                    PrivacyProtectRegistrantContact = false,
                    PrivacyProtectTechContact = false
                }
            );
            return result.OperationId;
        }
        catch (InvalidInputException)
        {
            _logger.LogInformation($"Unable to request registration for domain
 {domainName}");
            return null;
```

```
        }
    }


    /// <summary>
    /// View billing records for the account between a start and end date.
    /// </summary>
    /// <param name="startDate">The start date for billing results.</param>
    /// <param name="endDate">The end date for billing results.</param>
    /// <returns>A collection of billing records.</returns>
    public async Task<List<BillingRecord>> ViewBilling(DateTime startDate,
DateTime endDate)
    {
        var results = new List<BillingRecord>();
        var paginateBilling = _amazonRoute53Domains.Paginators.ViewBilling(
            new ViewBillingRequest()
            {
                Start = startDate,
                End = endDate
            });

        // Get the entire list using the paginator.
        await foreach (var billingRecords in paginateBilling.BillingRecords)
        {
            results.Add(billingRecords);
        }
        return results;
    }


    /// <summary>
    /// List the domains for the account.
    /// </summary>
    /// <returns>A collection of domain summary records.</returns>
    public async Task<List<DomainSummary>> ListDomains()
    {
        var results = new List<DomainSummary>();
        var paginateDomains = _amazonRoute53Domains.Paginators.ListDomains(
            new ListDomainsRequest());

        // Get the entire list using the paginator.
        await foreach (var domain in paginateDomains.Domains)
        {
            results.Add(domain);
```

```
        }
        return results;
    }


    /// <summary>
    /// List operations for the account that are submitted after a specified
date.
    /// </summary>
    /// <returns>A collection of operation summary records.</returns>
    public async Task<List<OperationSummary>> ListOperations(DateTime
submittedSince)
    {
        var results = new List<OperationSummary>();
        var paginateOperations = _amazonRoute53Domains.Paginators.ListOperations(
            new ListOperationsRequest()
            {
                SubmittedSince = submittedSince
            });

        // Get the entire list using the paginator.
        await foreach (var operations in paginateOperations.Operations)
        {
            results.Add(operations);
        }
        return results;
    }


    /// <summary>
    /// Get details for a domain.
    /// </summary>
    /// <returns>A string with detail information about the domain.</returns>
    public async Task<string> GetDomainDetail(string domainName)
    {
        try
        {
            var result = await _amazonRoute53Domains.GetDomainDetailAsync(
                new GetDomainDetailRequest()
                {
                    DomainName = domainName
                });
            var details = $"\tDomain {domainName}:\n" +
```

```
                            $"\tCreated on
 {result.CreationDate.ToShortDateString()}.\n" +
                            $"\tAdmin contact is {result.AdminContact.Email}.\n" +
                            $"\tAuto-renew is {result.AutoRenew}.\n";

            return details;
        }
        catch (InvalidInputException)
        {
            return $"Domain {domainName} was not found in your account.";
        }
    }
}
```

- API 세부 정보는 AWS SDK for .NET API 참조의 다음 주제를 참조하십시오.
  - CheckDomainAvailability
  - CheckDomainTransferability
  - GetDomainDetail
  - GetDomainSuggestions
  - GetOperationDetail
  - ListDomains
  - ListOperations
  - ListPrices
  - RegisterDomain
  - ViewBilling

Java

SDK for Java 2.x

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * This example uses pagination methods where applicable. For example, to list
 * domains, the
 * listDomainsPaginator method is used. For more information about pagination,
 * see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/
pagination.html
 *
 * This Java code example performs the following operations:
 *
 * 1. List current domains.
 * 2. List operations in the past year.
 * 3. View billing for the account in the past year.
 * 4. View prices for domain types.
 * 5. Get domain suggestions.
 * 6. Check domain availability.
 * 7. Check domain transferability.
 * 8. Request a domain registration.
 * 9. Get operation details.
 * 10. Optionally, get domain details.
 */

public class Route53Scenario {
    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <domainType> <phoneNumber> <email> <domainSuggestion>
 <firstName> <lastName> <city>

                Where:
```

```
                    domainType - The domain type (for example, com).\s
                    phoneNumber - The phone number to use (for example,
+91.9966564xxx)      email - The email address to use.      domainSuggestion -
The domain suggestion (for example, findmy.accountants).\s
                    firstName - The first name to use to register a domain.\s
                    lastName -  The last name to use to register a domain.\s
                    city - the city to use to register a domain.\s
                    """;

        if (args.length != 7) {
            System.out.println(usage);
            System.exit(1);
        }

        String domainType = args[0];
        String phoneNumber = args[1];
        String email = args[2];
        String domainSuggestion = args[3];
        String firstName = args[4];
        String lastName = args[5];
        String city = args[6];
        Region region = Region.US_EAST_1;
        Route53DomainsClient route53DomainsClient =
Route53DomainsClient.builder()
                .region(region)
                .build();

        System.out.println(DASHES);
        System.out.println("Welcome to the Amazon Route 53 domains example
scenario.");
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("1. List current domains.");
        listDomains(route53DomainsClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("2. List operations in the past year.");
        listOperations(route53DomainsClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("3. View billing for the account in the past year.");
```

```
        listBillingRecords(route53DomainsClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("4. View prices for domain types.");
        listPrices(route53DomainsClient, domainType);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("5. Get domain suggestions.");
        listDomainSuggestions(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("6. Check domain availability.");
        checkDomainAvailability(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("7. Check domain transferability.");
        checkDomainTransferability(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("8. Request a domain registration.");
        String opId = requestDomainRegistration(route53DomainsClient,
domainSuggestion, phoneNumber, email, firstName,
                lastName, city);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("9. Get operation details.");
        getOperationalDetail(route53DomainsClient, opId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("10. Get domain details.");
        System.out.println("Note: You must have a registered domain to get
details.");
        System.out.println("Otherwise, an exception is thrown that states ");
        System.out.println("Domain xxxxxxx not found in xxxxxxx account.");
        getDomainDetails(route53DomainsClient, domainSuggestion);
        System.out.println(DASHES);
    }
```

```
   public static void getDomainDetails(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
           GetDomainDetailRequest detailRequest =
GetDomainDetailRequest.builder()
                   .domainName(domainSuggestion)
                   .build();

           GetDomainDetailResponse response =
route53DomainsClient.getDomainDetail(detailRequest);
           System.out.println("The contact first name is " +
response.registrantContact().firstName());
           System.out.println("The contact last name is " +
response.registrantContact().lastName());
           System.out.println("The contact org name is " +
response.registrantContact().organizationName());

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }

   public static void getOperationalDetail(Route53DomainsClient
route53DomainsClient, String operationId) {
       try {
           GetOperationDetailRequest detailRequest =
GetOperationDetailRequest.builder()
                   .operationId(operationId)
                   .build();

           GetOperationDetailResponse response =
route53DomainsClient.getOperationDetail(detailRequest);
           System.out.println("Operation detail message is " +
response.message());

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

```
   public static String requestDomainRegistration(Route53DomainsClient
route53DomainsClient,
           String domainSuggestion,
           String phoneNumber,
           String email,
           String firstName,
           String lastName,
           String city) {

       try {
           ContactDetail contactDetail = ContactDetail.builder()
                   .contactType(ContactType.COMPANY)
                   .state("LA")
                   .countryCode(CountryCode.IN)
                   .email(email)
                   .firstName(firstName)
                   .lastName(lastName)
                   .city(city)
                   .phoneNumber(phoneNumber)
                   .organizationName("My Org")
                   .addressLine1("My Address")
                   .zipCode("123 123")
                   .build();

           RegisterDomainRequest domainRequest = RegisterDomainRequest.builder()
                   .adminContact(contactDetail)
                   .registrantContact(contactDetail)
                   .techContact(contactDetail)
                   .domainName(domainSuggestion)
                   .autoRenew(true)
                   .durationInYears(1)
                   .build();

           RegisterDomainResponse response =
route53DomainsClient.registerDomain(domainRequest);
           System.out.println("Registration requested. Operation Id: " +
response.operationId());
           return response.operationId();

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
       return "";
```

```
    }

    public static void checkDomainTransferability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
        try {
            CheckDomainTransferabilityRequest transferabilityRequest =
CheckDomainTransferabilityRequest.builder()
                    .domainName(domainSuggestion)
                    .build();

            CheckDomainTransferabilityResponse response = route53DomainsClient
                    .checkDomainTransferability(transferabilityRequest);
            System.out.println("Transferability: " +
response.transferability().transferable().toString());

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void checkDomainAvailability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
        try {
            CheckDomainAvailabilityRequest availabilityRequest =
CheckDomainAvailabilityRequest.builder()
                    .domainName(domainSuggestion)
                    .build();

            CheckDomainAvailabilityResponse response = route53DomainsClient
                    .checkDomainAvailability(availabilityRequest);
            System.out.println(domainSuggestion + " is " +
response.availability().toString());

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void listDomainSuggestions(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
        try {
```

```
            GetDomainSuggestionsRequest suggestionsRequest =
GetDomainSuggestionsRequest.builder()
                    .domainName(domainSuggestion)
                    .suggestionCount(5)
                    .onlyAvailable(true)
                    .build();

            GetDomainSuggestionsResponse response =
route53DomainsClient.getDomainSuggestions(suggestionsRequest);
            List<DomainSuggestion> suggestions = response.suggestionsList();
            for (DomainSuggestion suggestion : suggestions) {
                System.out.println("Suggestion Name: " +
suggestion.domainName());
                System.out.println("Availability: " + suggestion.availability());
                System.out.println(" ");
            }

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void listPrices(Route53DomainsClient route53DomainsClient,
String domainType) {
        try {
            ListPricesRequest pricesRequest = ListPricesRequest.builder()
                    .tld(domainType)
                    .build();

            ListPricesIterable listRes =
route53DomainsClient.listPricesPaginator(pricesRequest);
            listRes.stream()
                    .flatMap(r -> r.prices().stream())
                    .forEach(content -> System.out.println(" Name: " +
content.name() +
                            " Registration: " +
content.registrationPrice().price() + " "
                            + content.registrationPrice().currency() +
                            " Renewal: " + content.renewalPrice().price() + " " +
content.renewalPrice().currency()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
```

```
            System.exit(1);
        }
    }

    public static void listBillingRecords(Route53DomainsClient
route53DomainsClient) {
        try {
            Date currentDate = new Date();
            LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
            ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
            LocalDateTime localDateTime2 = localDateTime.minusYears(1);
            Instant myStartTime = localDateTime2.toInstant(zoneOffset);
            Instant myEndTime = localDateTime.toInstant(zoneOffset);

            ViewBillingRequest viewBillingRequest = ViewBillingRequest.builder()
                    .start(myStartTime)
                    .end(myEndTime)
                    .build();

            ViewBillingIterable listRes =
route53DomainsClient.viewBillingPaginator(viewBillingRequest);
            listRes.stream()
                    .flatMap(r -> r.billingRecords().stream())
                    .forEach(content -> System.out.println(" Bill Date:: " +
content.billDate() +
                            " Operation: " + content.operationAsString() +
                            " Price: " + content.price()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void listOperations(Route53DomainsClient route53DomainsClient)
{
        try {
            Date currentDate = new Date();
            LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
            ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
            localDateTime = localDateTime.minusYears(1);
            Instant myTime = localDateTime.toInstant(zoneOffset);
```

```
            ListOperationsRequest operationsRequest =
 ListOperationsRequest.builder()
                    .submittedSince(myTime)
                    .build();

            ListOperationsIterable listRes =
 route53DomainsClient.listOperationsPaginator(operationsRequest);
            listRes.stream()
                    .flatMap(r -> r.operations().stream())
                    .forEach(content -> System.out.println(" Operation Id: " +
 content.operationId() +
                            " Status: " + content.statusAsString() +
                            " Date: " + content.submittedDate()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void listDomains(Route53DomainsClient route53DomainsClient) {
        try {
            ListDomainsIterable listRes =
 route53DomainsClient.listDomainsPaginator();
            listRes.stream()
                    .flatMap(r -> r.domains().stream())
                    .forEach(content -> System.out.println("The domain name is "
 + content.domainName()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- API 세부 정보는 AWS SDK for Java 2.x API 참조의 다음 주제를 참조하십시오.
  - CheckDomainAvailability
  - CheckDomainTransferability
  - GetDomainDetail

- GetDomainSuggestions
- GetOperationDetail
- ListDomains
- ListOperations
- ListPrices
- RegisterDomain
- ViewBilling

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:
https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html

This Kotlin code example performs the following operations:

1. List current domains.
2. List operations in the past year.
3. View billing for the account in the past year.
4. View prices for domain types.
5. Get domain suggestions.
6. Check domain availability.
7. Check domain transferability.
8. Request a domain registration.
9. Get operation details.
10. Optionally, get domain details.
 */
```

```
val DASHES: String = String(CharArray(80)).replace("\u0000", "-")

suspend fun main(args: Array<String>) {
    val usage = """
        Usage:
            <domainType> <phoneNumber> <email> <domainSuggestion> <firstName>
 <lastName> <city>
        Where:
           domainType - The domain type (for example, com).
           phoneNumber - The phone number to use (for example, +1.2065550100)

           email - The email address to use.
           domainSuggestion - The domain suggestion (for example,
 findmy.example).
           firstName - The first name to use to register a domain.
           lastName -  The last name to use to register a domain.
           city - The city to use to register a domain.
    """

    if (args.size != 7) {
        println(usage)
        exitProcess(1)
    }

    val domainType = args[0]
    val phoneNumber = args[1]
    val email = args[2]
    val domainSuggestion = args[3]
    val firstName = args[4]
    val lastName = args[5]
    val city = args[6]

    println(DASHES)
    println("Welcome to the Amazon Route 53 domains example scenario.")
    println(DASHES)

    println(DASHES)
    println("1. List current domains.")
    listDomains()
    println(DASHES)

    println(DASHES)
    println("2. List operations in the past year.")
```

```
    listOperations()
    println(DASHES)

    println(DASHES)
    println("3. View billing for the account in the past year.")
    listBillingRecords()
    println(DASHES)

    println(DASHES)
    println("4. View prices for domain types.")
    listAllPrices(domainType)
    println(DASHES)

    println(DASHES)
    println("5. Get domain suggestions.")
    listDomainSuggestions(domainSuggestion)
    println(DASHES)

    println(DASHES)
    println("6. Check domain availability.")
    checkDomainAvailability(domainSuggestion)
    println(DASHES)

    println(DASHES)
    println("7. Check domain transferability.")
    checkDomainTransferability(domainSuggestion)
    println(DASHES)

    println(DASHES)
    println("8. Request a domain registration.")
    val opId = requestDomainRegistration(domainSuggestion, phoneNumber, email,
firstName, lastName, city)
    println(DASHES)

    println(DASHES)
    println("9. Get operation details.")
    getOperationalDetail(opId)
    println(DASHES)

    println(DASHES)
    println("10. Get domain details.")
    println("Note: You must have a registered domain to get details.")
    println("Otherwise an exception is thrown that states ")
    println("Domain xxxxxxx not found in xxxxxxx account.")
```

```
    getDomainDetails(domainSuggestion)
    println(DASHES)
}

suspend fun getDomainDetails(domainSuggestion: String?) {
    val detailRequest =
        GetDomainDetailRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response = route53DomainsClient.getDomainDetail(detailRequest)
        println("The contact first name is
 ${response.registrantContact?.firstName}")
        println("The contact last name is
 ${response.registrantContact?.lastName}")
        println("The contact org name is
 ${response.registrantContact?.organizationName}")
    }
}

suspend fun getOperationalDetail(opId: String?) {
    val detailRequest =
        GetOperationDetailRequest {
            operationId = opId
        }
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response = route53DomainsClient.getOperationDetail(detailRequest)
        println("Operation detail message is ${response.message}")
    }
}

suspend fun requestDomainRegistration(
    domainSuggestion: String?,
    phoneNumberVal: String?,
    emailVal: String?,
    firstNameVal: String?,
    lastNameVal: String?,
    cityVal: String?,
): String? {
    val contactDetail =
        ContactDetail {
            contactType = ContactType.Company
            state = "LA"
            countryCode = CountryCode.In
```

```
            email = emailVal
            firstName = firstNameVal
            lastName = lastNameVal
            city = cityVal
            phoneNumber = phoneNumberVal
            organizationName = "My Org"
            addressLine1 = "My Address"
            zipCode = "123 123"
        }

    val domainRequest =
        RegisterDomainRequest {
            adminContact = contactDetail
            registrantContact = contactDetail
            techContact = contactDetail
            domainName = domainSuggestion
            autoRenew = true
            durationInYears = 1
        }

    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response = route53DomainsClient.registerDomain(domainRequest)
        println("Registration requested. Operation Id: ${response.operationId}")
        return response.operationId
    }
}

suspend fun checkDomainTransferability(domainSuggestion: String?) {
    val transferabilityRequest =
        CheckDomainTransferabilityRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response =
 route53DomainsClient.checkDomainTransferability(transferabilityRequest)
        println("Transferability: ${response.transferability?.transferable}")
    }
}

suspend fun checkDomainAvailability(domainSuggestion: String) {
    val availabilityRequest =
        CheckDomainAvailabilityRequest {
            domainName = domainSuggestion
        }
```

```
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response =
 route53DomainsClient.checkDomainAvailability(availabilityRequest)
        println("$domainSuggestion is ${response.availability}")
    }
}

suspend fun listDomainSuggestions(domainSuggestion: String?) {
    val suggestionsRequest =
        GetDomainSuggestionsRequest {
            domainName = domainSuggestion
            suggestionCount = 5
            onlyAvailable = true
        }
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response =
 route53DomainsClient.getDomainSuggestions(suggestionsRequest)
        response.suggestionsList?.forEach { suggestion ->
            println("Suggestion Name: ${suggestion.domainName}")
            println("Availability: ${suggestion.availability}")
            println(" ")
        }
    }
}

suspend fun listAllPrices(domainType: String?) {
    val pricesRequest =
        ListPricesRequest {
            tld = domainType
        }

    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        route53DomainsClient
            .listPricesPaginated(pricesRequest)
            .transform { it.prices?.forEach { obj -> emit(obj) } }
            .collect { pr ->
                println("Registration: ${pr.registrationPrice}
 ${pr.registrationPrice?.currency}")
                println("Renewal: ${pr.renewalPrice?.price}
 ${pr.renewalPrice?.currency}")
                println("Transfer: ${pr.transferPrice?.price}
 ${pr.transferPrice?.currency}")
                println("Restoration: ${pr.restorationPrice?.price}
 ${pr.restorationPrice?.currency}")
```

```
            }
    }
}

suspend fun listBillingRecords() {
    val currentDate = Date()
    val localDateTime =
 currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    val localDateTime2 = localDateTime.minusYears(1)
    val myStartTime = localDateTime2.toInstant(zoneOffset)
    val myEndTime = localDateTime.toInstant(zoneOffset)
    val timeStart: Instant? = myStartTime?.let { Instant(it) }
    val timeEnd: Instant? = myEndTime?.let { Instant(it) }

    val viewBillingRequest =
        ViewBillingRequest {
            start = timeStart
            end = timeEnd
        }

    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        route53DomainsClient
            .viewBillingPaginated(viewBillingRequest)
            .transform { it.billingRecords?.forEach { obj -> emit(obj) } }
            .collect { billing ->
                println("Bill Date: ${billing.billDate}")
                println("Operation: ${billing.operation}")
                println("Price: ${billing.price}")
            }
    }
}

suspend fun listOperations() {
    val currentDate = Date()
    var localDateTime =
 currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    localDateTime = localDateTime.minusYears(1)
    val myTime: java.time.Instant? = localDateTime.toInstant(zoneOffset)
    val time2: Instant? = myTime?.let { Instant(it) }
    val operationsRequest =
        ListOperationsRequest {
            submittedSince = time2
```

```
        }

    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        route53DomainsClient
            .listOperationsPaginated(operationsRequest)
            .transform { it.operations?.forEach { obj -> emit(obj) } }
            .collect { content ->
                println("Operation Id: ${content.operationId}")
                println("Status: ${content.status}")
                println("Date: ${content.submittedDate}")
            }
    }
}

suspend fun listDomains() {
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        route53DomainsClient
            .listDomainsPaginated(ListDomainsRequest {})
            .transform { it.domains?.forEach { obj -> emit(obj) } }
            .collect { content ->
                println("The domain name is ${content.domainName}")
            }
    }
}
```

- API 세부 정보는 AWS SDK for Kotlin API 참조의 다음 주제를 참조하십시오.
  - CheckDomainAvailability
  - CheckDomainTransferability
  - GetDomainDetail
  - GetDomainSuggestions
  - GetOperationDetail
  - ListDomains
  - ListOperations
  - ListPrices
  - RegisterDomain
  - ViewBilling

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDKs를 사용한 Route 53 도메인 등록 작업

다음 코드 예제에서는 AWS SDKs를 사용하여 개별 Route 53 도메인 등록 작업을 수행하는 방법을 보여줍니다. 각 예제에는 GitHub에 대한 링크가 포함되어 있습니다. 여기에서 코드 설정 및 실행에 대한 지침을 찾을 수 있습니다.

다음 예제에는 가장 일반적으로 사용되는 작업만 포함되어 있습니다. 전체 목록은 Amazon Route 53 domain registration API 참조를 참조하세요.

예시

- AWS SDK 또는 CLI와 CheckDomainAvailability 함께 사용
- AWS SDK 또는 CLI와 CheckDomainTransferability 함께 사용
- AWS SDK 또는 CLI와 GetDomainDetail 함께 사용
- AWS SDK 또는 CLI와 GetDomainSuggestions 함께 사용
- AWS SDK 또는 CLI와 GetOperationDetail 함께 사용
- AWS SDK 또는 CLI와 ListDomains 함께 사용
- AWS SDK 또는 CLI와 ListOperations 함께 사용
- AWS SDK와 ListPrices 함께 사용
- AWS SDK 또는 CLI와 RegisterDomain 함께 사용
- AWS SDK 또는 CLI와 ViewBilling 함께 사용

AWS SDK 또는 CLI와 **`CheckDomainAvailability`** 함께 사용

다음 코드 예제는 `CheckDomainAvailability`의 사용 방법을 보여 줍니다.

작업 예제는 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 다음 코드 예제에서는 컨텍스트 내에서 이 작업을 확인할 수 있습니다.

- 기본 사항 알아보기

.NET

AWS SDK for .NET

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
/// <summary>
/// Check the availability of a domain name.
/// </summary>
/// <param name="domain">The domain to check for availability.</param>
/// <returns>An availability result string.</returns>
public async Task<string> CheckDomainAvailability(string domain)
{
    var result = await _amazonRoute53Domains.CheckDomainAvailabilityAsync(
        new CheckDomainAvailabilityRequest
        {
            DomainName = domain
        }
    );
    return result.Availability.Value;
}
```

- API 세부 정보는 AWS SDK for .NET API 참조에서 CheckDomainAvailability를 참조하십시오.

CLI

AWS CLI

Route 53에 도메인 이름 등록 가능 여부를 확인하려면

다음 `check-domain-availability` 명령은 Route 53를 사용하여 도메인 이름 `example.com`을 등록할 수 있는지 여부에 대한 정보를 반환합니다.

이 명령은 us-east-1 리전에서만 실행됩니다. 기본 리전이 us-east-1로 설정된 경우, region 파라미터를 생략할 수 있습니다.

```
aws route53domains check-domain-availability \
    --region us-east-1 \
    --domain-name example.com
```

출력:

```
{
    "Availability": "UNAVAILABLE"
}
```

Route 53은 .com 및 .jp와 같은 최상위 도메인(TLD)을 광범위하게 지원하지만, 사용 가능한 모든 TLD를 지원하지는 않습니다. 도메인의 가용성을 확인하고 Route 53이 TLD를 지원하지 않는 경우, check-domain-availability는 다음 메시지를 반환합니다.

```
An error occurred (UnsupportedTLD) when calling the CheckDomainAvailability
 operation: <top-level domain> tld is not supported.
```

Route 53에 도메인을 등록하는 데 사용할 수 있는 TLD 목록은 Amazon Route 53 개발자 안내서의 Amazon Route 53에 등록할 수 있는 도메인을 참조하세요. Amazon Route 53에 도메인을 등록하는 방법에 대한 자세한 내용은 Amazon Route 53 개발자 안내서의 새 도메인 등록을 참조하세요.

- API 세부 정보는 AWS CLI 명령 참조의 CheckDomainAvailability를 참조하세요.

Java

SDK for Java 2.x

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    public static void checkDomainAvailability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
```

```
        try {
            CheckDomainAvailabilityRequest availabilityRequest =
 CheckDomainAvailabilityRequest.builder()
                    .domainName(domainSuggestion)
                    .build();

            CheckDomainAvailabilityResponse response = route53DomainsClient
                    .checkDomainAvailability(availabilityRequest);
            System.out.println(domainSuggestion + " is " +
 response.availability().toString());

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- API 세부 정보는 AWS SDK for Java 2.x API 참조에서 CheckDomainAvailability를 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
suspend fun checkDomainAvailability(domainSuggestion: String) {
    val availabilityRequest =
        CheckDomainAvailabilityRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response =
 route53DomainsClient.checkDomainAvailability(availabilityRequest)
        println("$domainSuggestion is ${response.availability}")
    }
```

```
}
```

- API 세부 정보는 AWS SDK for Kotlin API 참조의 CheckDomainAvailability를 참조하십시오.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **CheckDomainTransferability** 함께 사용

다음 코드 예제는 CheckDomainTransferability의 사용 방법을 보여 줍니다.

작업 예제는 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 다음 코드 예제에서는 컨텍스트 내에서 이 작업을 확인할 수 있습니다.

- 기본 사항 알아보기

.NET

AWS SDK for .NET

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
/// <summary>
/// Check the transferability of a domain name.
/// </summary>
/// <param name="domain">The domain to check for transferability.</param>
/// <returns>A transferability result string.</returns>
public async Task<string> CheckDomainTransferability(string domain)
{
    var result = await _amazonRoute53Domains.CheckDomainTransferabilityAsync(
        new CheckDomainTransferabilityRequest
        {
            DomainName = domain
        }
```

```
        );
        return result.Transferability.Transferable.Value;
    }
```

- API 세부 정보는 AWS SDK for .NET API 참조의 CheckDomainTransferability를 참조하십시오.

CLI

AWS CLI

도메인을 Route 53으로 전송할 수 있는지 확인하려면

다음 `check-domain-transferability` 명령은 도메인 이름 `example.com`을 Route 53으로 이전할 수 있는지 여부에 대한 정보를 반환합니다.

이 명령은 `us-east-1` 리전에서만 실행됩니다. 기본 리전이 `us-east-1`로 설정된 경우, `region` 파라미터를 생략할 수 있습니다.

```
aws route53domains check-domain-transferability \
    --region us-east-1 \
    --domain-name example.com
```

출력:

```
{
    "Transferability": {
        "Transferable": "UNTRANSFERABLE"
    }
}
```

자세한 내용은 Amazon Route 53 개발자 안내서의 도메인 등록을 Amazon Route 53으로 이전을 참조하세요.

- API 세부 정보는 AWS CLI 명령 참조의 CheckDomainTransferability를 참조하세요.

Java

SDK for Java 2.x

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
   public static void checkDomainTransferability(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
           CheckDomainTransferabilityRequest transferabilityRequest =
CheckDomainTransferabilityRequest.builder()
                   .domainName(domainSuggestion)
                   .build();

           CheckDomainTransferabilityResponse response = route53DomainsClient
                   .checkDomainTransferability(transferabilityRequest);
           System.out.println("Transferability: " +
response.transferability().transferable().toString());

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- API 세부 정보는 AWS SDK for Java 2.x API 참조의 CheckDomainTransferability를 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
suspend fun checkDomainTransferability(domainSuggestion: String?) {
    val transferabilityRequest =
        CheckDomainTransferabilityRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response =
 route53DomainsClient.checkDomainTransferability(transferabilityRequest)
        println("Transferability: ${response.transferability?.transferable}")
    }
}
```

- API 세부 정보는 AWS SDK for Kotlin API 참조의 CheckDomainTransferability를 참조하십시오.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **`GetDomainDetail`** 함께 사용

다음 코드 예제는 `GetDomainDetail`의 사용 방법을 보여 줍니다.

작업 예제는 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 다음 코드 예제에서는 컨텍스트 내에서 이 작업을 확인할 수 있습니다.

- 기본 사항 알아보기

.NET

AWS SDK for .NET

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    /// <summary>
    /// Get details for a domain.
    /// </summary>
    /// <returns>A string with detail information about the domain.</returns>
    public async Task<string> GetDomainDetail(string domainName)
    {
        try
        {
            var result = await _amazonRoute53Domains.GetDomainDetailAsync(
                new GetDomainDetailRequest()
                {
                    DomainName = domainName
                });
            var details = $"\tDomain {domainName}:\n" +
                          $"\tCreated on
{result.CreationDate.ToShortDateString()}.\n" +
                          $"\tAdmin contact is {result.AdminContact.Email}.\n" +
                          $"\tAuto-renew is {result.AutoRenew}.\n";

            return details;
        }
        catch (InvalidInputException)
        {
            return $"Domain {domainName} was not found in your account.";
        }
    }
```

- API 세부 정보는 AWS SDK for .NET API 참조의 GetDomainDetail을 참조하십시오.

CLI

AWS CLI

지정된 도메인에 대한 자세한 정보를 가져오려면

다음 get-domain-detail 명령은 지정된 도메인의 자세한 정보를 표시합니다.

이 명령은 us-east-1 리전에서만 실행됩니다. 기본 리전이 us-east-1로 설정된 경우, region 파라미터를 생략할 수 있습니다.

```
aws route53domains get-domain-detail \
    --region us-east-1 \
    --domain-name example.com
```

출력:

```
{
    "DomainName": "example.com",
    "Nameservers": [
        {
            "Name": "ns-2048.awsdns-64.com",
            "GlueIps": []
        },
        {
            "Name": "ns-2049.awsdns-65.net",
            "GlueIps": []
        },
        {
            "Name": "ns-2050.awsdns-66.org",
            "GlueIps": []
        },
        {
            "Name": "ns-2051.awsdns-67.co.uk",
            "GlueIps": []
        }
    ],
    "AutoRenew": true,
    "AdminContact": {
        "FirstName": "Saanvi",
        "LastName": "Sarkar",
        "ContactType": "COMPANY",
        "OrganizationName": "Example",
```

```
        "AddressLine1": "123 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "ssarkar@example.com",
        "ExtraParams": []
    },
    "RegistrantContact": {
        "FirstName": "Alejandro",
        "LastName": "Rosalez",
        "ContactType": "COMPANY",
        "OrganizationName": "Example",
        "AddressLine1": "123 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "arosalez@example.com",
        "ExtraParams": []
    },
    "TechContact": {
        "FirstName": "Wang",
        "LastName": "Xiulan",
        "ContactType": "COMPANY",
        "OrganizationName": "Example",
        "AddressLine1": "123 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "wxiulan@example.com",
        "ExtraParams": []
    },
    "AdminPrivacy": true,
    "RegistrantPrivacy": true,
    "TechPrivacy": true,
    "RegistrarName": "Amazon Registrar, Inc.",
    "WhoIsServer": "whois.registrar.amazon.com",
    "RegistrarUrl": "http://registrar.amazon.com",
    "AbuseContactEmail": "abuse@registrar.amazon.com",
```

```
    "AbuseContactPhone": "+1.2062661000",
    "CreationDate": 1444934889.601,
    "ExpirationDate": 1602787689.0,
    "StatusList": [
        "clientTransferProhibited"
    ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 GetDomainDetail을 참조하세요.

Java

SDK for Java 2.x

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
   public static void getDomainDetails(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
       try {
           GetDomainDetailRequest detailRequest =
GetDomainDetailRequest.builder()
                   .domainName(domainSuggestion)
                   .build();

           GetDomainDetailResponse response =
route53DomainsClient.getDomainDetail(detailRequest);
           System.out.println("The contact first name is " +
response.registrantContact().firstName());
           System.out.println("The contact last name is " +
response.registrantContact().lastName());
           System.out.println("The contact org name is " +
response.registrantContact().organizationName());

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- API 세부 정보는 AWS SDK for Java 2.x API 참조의 GetDomainDetail을 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
suspend fun getDomainDetails(domainSuggestion: String?) {
    val detailRequest =
        GetDomainDetailRequest {
            domainName = domainSuggestion
        }
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response = route53DomainsClient.getDomainDetail(detailRequest)
        println("The contact first name is
 ${response.registrantContact?.firstName}")
        println("The contact last name is
 ${response.registrantContact?.lastName}")
        println("The contact org name is
 ${response.registrantContact?.organizationName}")
    }
}
```

- API 세부 정보는 AWS SDK for Kotlin API 참조의 GetDomainDetail을 참조하십시오.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **`GetDomainSuggestions`** 함께 사용

다음 코드 예제는 `GetDomainSuggestions`의 사용 방법을 보여 줍니다.

작업 예제는 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 다음 코드 예제에서는 컨텍스트 내에서 이 작업을 확인할 수 있습니다.

- 기본 사항 알아보기

.NET

AWS SDK for .NET

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    /// <summary>
    /// Get a list of suggestions for a given domain.
    /// </summary>
    /// <param name="domain">The domain to check for suggestions.</param>
    /// <param name="onlyAvailable">If true, only returns available domains.</
param>
    /// <param name="suggestionCount">The number of suggestions to return.
 Defaults to the max of 50.</param>
    /// <returns>A collection of domain suggestions.</returns>
    public async Task<List<DomainSuggestion>> GetDomainSuggestions(string domain,
 bool onlyAvailable, int suggestionCount = 50)
    {
        var result = await _amazonRoute53Domains.GetDomainSuggestionsAsync(
            new GetDomainSuggestionsRequest
            {
                DomainName = domain,
                OnlyAvailable = onlyAvailable,
                SuggestionCount = suggestionCount
            }
        );
        return result.SuggestionsList;
    }
```

- API 세부 정보는 AWS SDK for .NET API 참조의 GetDomainSuggestions를 참조하십시오.

CLI

AWS CLI

제안된 도메인 이름 목록을 가져오려면

다음 get-domain-suggestions 명령은 도메인 이름 example.com에 따라 제안된 도메인 이름 목록을 표시합니다. 응답에는 사용 가능한 도메인 이름만 포함됩니다. 이 명령은 us-east-1 리전에서만 실행됩니다. 기본 리전이 us-east-1로 설정된 경우, region 파라미터를 생략할 수 있습니다.

```
aws route53domains get-domain-suggestions \
    --region us-east-1 \
    --domain-name example.com \
    --suggestion-count 10 \
    --only-available
```

출력:

```
{
    "SuggestionsList": [
        {
            "DomainName": "egzaampal.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "examplelaw.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "examplehouse.net",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "homeexample.net",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "examplelist.com",
            "Availability": "AVAILABLE"
       },
        {
```

```
            "DomainName": "examplenews.net",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "officeexample.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "exampleworld.com",
            "Availability": "AVAILABLE"
        },
        {
            "DomainName": "exampleart.com",
            "Availability": "AVAILABLE"
        }
    ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 GetDomainSuggestions를 참조하세요.

Java

SDK for Java 2.x

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
   public static void listDomainSuggestions(Route53DomainsClient
route53DomainsClient, String domainSuggestion) {
        try {
            GetDomainSuggestionsRequest suggestionsRequest =
GetDomainSuggestionsRequest.builder()
                    .domainName(domainSuggestion)
                    .suggestionCount(5)
                    .onlyAvailable(true)
                    .build();

            GetDomainSuggestionsResponse response =
route53DomainsClient.getDomainSuggestions(suggestionsRequest);
```

```
            List<DomainSuggestion> suggestions = response.suggestionsList();
            for (DomainSuggestion suggestion : suggestions) {
                System.out.println("Suggestion Name: " +
 suggestion.domainName());
                System.out.println("Availability: " + suggestion.availability());
                System.out.println(" ");
            }

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- API 세부 정보는 AWS SDK for Java 2.x API 참조의 GetDomainSuggestions를 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
suspend fun listDomainSuggestions(domainSuggestion: String?) {
    val suggestionsRequest =
        GetDomainSuggestionsRequest {
            domainName = domainSuggestion
            suggestionCount = 5
            onlyAvailable = true
        }
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response =
 route53DomainsClient.getDomainSuggestions(suggestionsRequest)
        response.suggestionsList?.forEach { suggestion ->
            println("Suggestion Name: ${suggestion.domainName}")
            println("Availability: ${suggestion.availability}")
```

```
            println(" ")
        }
    }
}
```

- API 세부 정보는 AWS SDK for Kotlin API 참조의 GetDomainSuggestions를 참조하십시오.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **GetOperationDetail** 함께 사용

다음 코드 예제는 GetOperationDetail의 사용 방법을 보여 줍니다.

작업 예제는 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 다음 코드 예제에서는 컨텍스트 내에서 이 작업을 확인할 수 있습니다.

- 기본 사항 알아보기

.NET

AWS SDK for .NET

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
/// <summary>
/// Get details for a domain action operation.
/// </summary>
/// <param name="operationId">The operational Id.</param>
/// <returns>A string describing the operational details.</returns>
public async Task<string> GetOperationDetail(string? operationId)
{
    if (operationId == null)
        return "Unable to get operational details because ID is null.";
```

```
        try
        {
            var operationDetails =
                await _amazonRoute53Domains.GetOperationDetailAsync(
                    new GetOperationDetailRequest
                    {
                        OperationId = operationId
                    }
                );

            var details = $"\tOperation {operationId}:\n" +
                          $"\tFor domain {operationDetails.DomainName} on
{operationDetails.SubmittedDate.ToShortDateString()}.\n" +
                          $"\tMessage is {operationDetails.Message}.\n" +
                          $"\tStatus is {operationDetails.Status}.\n";

            return details;
        }
        catch (AmazonRoute53DomainsException ex)
        {
            return $"Unable to get operation details. Here's why: {ex.Message}.";
        }
    }
```

- API 세부 정보는 AWS SDK for .NET API 참조의 GetOperationDetail을 참조하십시오.

CLI

AWS CLI

작업의 현재 상태를 가져오려면

일부 도메인 등록 작업은 비동기적으로 작동하고 완료되기 전에 응답을 반환합니다. 이러한 작업은 현재 상태를 가져오는 데 사용할 수 있는 작업 ID를 반환합니다. 다음 `get-operation-detail` 명령은 지정된 작업의 상태를 반환합니다.

이 명령은 `us-east-1` 리전에서만 실행됩니다. 기본 리전이 `us-east-1`로 설정된 경우, `region` 파라미터를 생략할 수 있습니다.

```
aws route53domains get-operation-detail \
    --region us-east-1 \
```

```
    --operation-id edbd8d63-7fe7-4343-9bc5-54033example
```

출력:

```
{
    "OperationId": "edbd8d63-7fe7-4343-9bc5-54033example",
    "Status": "SUCCESSFUL",
    "DomainName": "example.com",
    "Type": "DOMAIN_LOCK",
    "SubmittedDate": 1573749367.864
}
```

- API 세부 정보는 AWS CLI 명령 참조의 GetOperationDetail을 참조하세요.

Java

SDK for Java 2.x

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
   public static void getOperationalDetail(Route53DomainsClient
route53DomainsClient, String operationId) {
       try {
           GetOperationDetailRequest detailRequest =
GetOperationDetailRequest.builder()
                   .operationId(operationId)
                   .build();

           GetOperationDetailResponse response =
route53DomainsClient.getOperationDetail(detailRequest);
           System.out.println("Operation detail message is " +
response.message());

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
```

```
    }
```

- API 세부 정보는 AWS SDK for Java 2.x API 참조의 GetOperationDetail을 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
suspend fun getOperationalDetail(opId: String?) {
    val detailRequest =
        GetOperationDetailRequest {
            operationId = opId
        }
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response = route53DomainsClient.getOperationDetail(detailRequest)
        println("Operation detail message is ${response.message}")
    }
}
```

- API 세부 정보는 AWS SDK for Kotlin API 참조의 GetOperationDetail을 참조하십시오.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **`ListDomains`** 함께 사용

다음 코드 예제는 `ListDomains`의 사용 방법을 보여 줍니다.

작업 예제는 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 다음 코드 예제에서는 컨텍스트 내에서 이 작업을 확인할 수 있습니다.

- 기본 사항 알아보기

.NET

AWS SDK for .NET

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
/// <summary>
/// List the domains for the account.
/// </summary>
/// <returns>A collection of domain summary records.</returns>
public async Task<List<DomainSummary>> ListDomains()
{
    var results = new List<DomainSummary>();
    var paginateDomains = _amazonRoute53Domains.Paginators.ListDomains(
        new ListDomainsRequest());

    // Get the entire list using the paginator.
    await foreach (var domain in paginateDomains.Domains)
    {
        results.Add(domain);
    }
    return results;
}
```

- API 세부 정보는 AWS SDK for .NET API 참조의 ListDomains를 참조하십시오.

CLI

AWS CLI

현재 AWS 계정에 등록된 도메인을 나열하려면

다음 `list-domains` 명령은 현재 AWS 계정에 등록된 도메인에 대한 요약 정보를 나열합니다.

이 명령은 `us-east-1` 리전에서만 실행됩니다. 기본 리전이 `us-east-1`로 설정된 경우, `region` 파라미터를 생략할 수 있습니다.

```
aws route53domains list-domains
    --region us-east-1
```

출력:

```
{
    "Domains": [
        {
            "DomainName": "example.com",
            "AutoRenew": true,
            "TransferLock": true,
            "Expiry": 1602712345.0
        },
        {
            "DomainName": "example.net",
            "AutoRenew": true,
            "TransferLock": true,
            "Expiry": 1602723456.0
        },
        {
            "DomainName": "example.org",
            "AutoRenew": true,
            "TransferLock": true,
            "Expiry": 1602734567.0
        }
    ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 ListDomains를 참조하세요.

Java

SDK for Java 2.x

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    public static void listDomains(Route53DomainsClient route53DomainsClient) {
```

```
        try {
            ListDomainsIterable listRes =
 route53DomainsClient.listDomainsPaginator();
            listRes.stream()
                    .flatMap(r -> r.domains().stream())
                    .forEach(content -> System.out.println("The domain name is "
 + content.domainName()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- API 세부 정보는 AWS SDK for Java 2.x API 참조의 ListDomains를 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
suspend fun listDomains() {
    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        route53DomainsClient
            .listDomainsPaginated(ListDomainsRequest {})
            .transform { it.domains?.forEach { obj -> emit(obj) } }
            .collect { content ->
                println("The domain name is ${content.domainName}")
            }
    }
}
```

- API 세부 정보는 AWS SDK for Kotlin API 참조의 ListDomains를 참조하십시오.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **ListOperations** 함께 사용

다음 코드 예제는 ListOperations의 사용 방법을 보여 줍니다.

작업 예제는 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 다음 코드 예제에서는 컨텍스트 내에서 이 작업을 확인할 수 있습니다.

- 기본 사항 알아보기

.NET

AWS SDK for .NET

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    /// <summary>
    /// List operations for the account that are submitted after a specified
date.
    /// </summary>
    /// <returns>A collection of operation summary records.</returns>
    public async Task<List<OperationSummary>> ListOperations(DateTime
submittedSince)
    {
        var results = new List<OperationSummary>();
        var paginateOperations = _amazonRoute53Domains.Paginators.ListOperations(
            new ListOperationsRequest()
            {
                SubmittedSince = submittedSince
            });

        // Get the entire list using the paginator.
        await foreach (var operations in paginateOperations.Operations)
        {
            results.Add(operations);
```

```
        }
        return results;
    }
```

- API 세부 정보는 AWS SDK for .NET API 참조의 ListOperations를 참조하십시오.

CLI

AWS CLI

작업 ID를 반환하는 작업의 상태를 나열하려면

일부 도메인 등록 작업은 비동기적으로 실행되고 완료되기 전에 응답을 반환합니다. 이러한 작업은 현재 상태를 가져오는 데 사용할 수 있는 작업 ID를 반환합니다. 다음 `list-operations` 명령은 상태를 포함한 현재 도메인 등록 작업에 대한 요약 정보를 나열합니다.

이 명령은 `us-east-1` 리전에서만 실행됩니다. 기본 리전이 `us-east-1`로 설정된 경우, `region` 파라미터를 생략할 수 있습니다.

```
aws route53domains list-operations
    --region us-east-1
```

출력:

```
{
    "Operations": [
        {
            "OperationId": "aab9822f-1da0-4bf3-8a15-fd4e0example",
            "Status": "SUCCESSFUL",
            "Type": "DOMAIN_LOCK",
            "SubmittedDate": 1455321739.986
        },
        {
            "OperationId": "c24379ed-76be-42f8-bdad-9379bexample",
            "Status": "SUCCESSFUL",
            "Type": "UPDATE_NAMESERVER",
            "SubmittedDate": 1468960475.109
        },
        {
            "OperationId": "f47e1297-ef9e-4c2b-ae1e-a5fcbexample",
            "Status": "SUCCESSFUL",
```

```
            "Type": "RENEW_DOMAIN",
            "SubmittedDate": 1473561835.943
        },
        {
            "OperationId": "75584f23-b15f-459e-aed7-dc6f5example",
            "Status": "SUCCESSFUL",
            "Type": "UPDATE_DOMAIN_CONTACT",
            "SubmittedDate": 1547501003.41
        }
    ]
}
```

출력에는 작업 ID를 반환하고 현재 AWS 계정을 사용하여 등록한 적이 있는 모든 도메인에서 수행한 모든 작업이 포함됩니다. 지정된 날짜 이후에 제출한 작업만 가져오려면 `submitted-since` 파라미터를 포함하고 날짜를 Unix 형식과 UTC(협정 세계시)로 지정할 수 있습니다. 다음 명령은 2020년 1월 1일 오전 12:00 UTC 이후에 제출된 모든 작업의 상태를 가져옵니다.

```
aws route53domains list-operations \
    --submitted-since 1577836800
```

- API 세부 정보는 AWS CLI 명령 참조의 ListOperations를 참조하세요.

Java

SDK for Java 2.x

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    public static void listOperations(Route53DomainsClient route53DomainsClient)
{
        try {
            Date currentDate = new Date();
            LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
            ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
            localDateTime = localDateTime.minusYears(1);
```

```
            Instant myTime = localDateTime.toInstant(zoneOffset);

            ListOperationsRequest operationsRequest =
 ListOperationsRequest.builder()
                    .submittedSince(myTime)
                    .build();

            ListOperationsIterable listRes =
 route53DomainsClient.listOperationsPaginator(operationsRequest);
            listRes.stream()
                    .flatMap(r -> r.operations().stream())
                    .forEach(content -> System.out.println(" Operation Id: " +
 content.operationId() +
                            " Status: " + content.statusAsString() +
                            " Date: " + content.submittedDate()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- API 세부 정보는 AWS SDK for Java 2.x API 참조의 ListOperations를 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
suspend fun listOperations() {
    val currentDate = Date()
    var localDateTime =
 currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    localDateTime = localDateTime.minusYears(1)
    val myTime: java.time.Instant? = localDateTime.toInstant(zoneOffset)
```

```
    val time2: Instant? = myTime?.let { Instant(it) }
    val operationsRequest =
        ListOperationsRequest {
            submittedSince = time2
        }

    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        route53DomainsClient
            .listOperationsPaginated(operationsRequest)
            .transform { it.operations?.forEach { obj -> emit(obj) } }
            .collect { content ->
                println("Operation Id: ${content.operationId}")
                println("Status: ${content.status}")
                println("Date: ${content.submittedDate}")
            }
    }
}
```

- API 세부 정보는 AWS SDK for Kotlin API 참조의 ListOperations를 참조하십시오.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK와 **ListPrices** 함께 사용

다음 코드 예제는 ListPrices의 사용 방법을 보여 줍니다.

작업 예제는 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 다음 코드 예제에서는 컨텍스트 내에서 이 작업을 확인할 수 있습니다.

- 기본 사항 알아보기

.NET

AWS SDK for .NET

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    /// <summary>
    /// List prices for domain type operations.
    /// </summary>
    /// <param name="domainTypes">Domain types to include in the results.</param>
    /// <returns>The list of domain prices.</returns>
    public async Task<List<DomainPrice>> ListPrices(List<string> domainTypes)
    {
        var results = new List<DomainPrice>();
        var paginatePrices = _amazonRoute53Domains.Paginators.ListPrices(new
ListPricesRequest());
        // Get the entire list using the paginator.
        await foreach (var prices in paginatePrices.Prices)
        {
            results.Add(prices);
        }
        return results.Where(p => domainTypes.Contains(p.Name)).ToList();
    }
```

- API 세부 정보는 AWS SDK for .NET API 참조의 ListPrices를 참조하십시오.

Java

SDK for Java 2.x

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    public static void listPrices(Route53DomainsClient route53DomainsClient,
String domainType) {
        try {
            ListPricesRequest pricesRequest = ListPricesRequest.builder()
                    .tld(domainType)
                    .build();

            ListPricesIterable listRes =
route53DomainsClient.listPricesPaginator(pricesRequest);
```

```
            listRes.stream()
                    .flatMap(r -> r.prices().stream())
                    .forEach(content -> System.out.println(" Name: " +
 content.name() +
                            " Registration: " +
 content.registrationPrice().price() + " "
                            + content.registrationPrice().currency() +
                            " Renewal: " + content.renewalPrice().price() + " " +
 content.renewalPrice().currency()));

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- API 세부 정보는 AWS SDK for Java 2.x API 참조의 ListPrices를 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
suspend fun listAllPrices(domainType: String?) {
    val pricesRequest =
        ListPricesRequest {
            tld = domainType
        }

    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        route53DomainsClient
            .listPricesPaginated(pricesRequest)
            .transform { it.prices?.forEach { obj -> emit(obj) } }
            .collect { pr ->
                println("Registration: ${pr.registrationPrice}
 ${pr.registrationPrice?.currency}")
```

```
                println("Renewal: ${pr.renewalPrice?.price}
 ${pr.renewalPrice?.currency}")
                println("Transfer: ${pr.transferPrice?.price}
 ${pr.transferPrice?.currency}")
                println("Restoration: ${pr.restorationPrice?.price}
 ${pr.restorationPrice?.currency}")
            }
    }
}
```

- API 세부 정보는AWS SDK for Kotlin API 참조의 ListPrices를 참조하십시오.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **RegisterDomain** 함께 사용

다음 코드 예제는 RegisterDomain의 사용 방법을 보여 줍니다.

작업 예제는 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 다음 코드 예제에서는 컨텍스트 내에서 이 작업을 확인할 수 있습니다.

- 기본 사항 알아보기

.NET

AWS SDK for .NET

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    /// <summary>
    /// Initiate a domain registration request.
    /// </summary>
    /// <param name="contact">Contact details.</param>
```

```
    /// <param name="domainName">The domain name to register.</param>
    /// <param name="autoRenew">True if the domain should automatically renew.</
param>
    /// <param name="duration">The duration in years for the domain
 registration.</param>
    /// <returns>The operation Id.</returns>
    public async Task<string?> RegisterDomain(string domainName, bool autoRenew,
 int duration, ContactDetail contact)
    {
        // This example uses the same contact information for admin, registrant,
 and tech contacts.
        try
        {
            var result = await _amazonRoute53Domains.RegisterDomainAsync(
                new RegisterDomainRequest()
                {
                    AdminContact = contact,
                    RegistrantContact = contact,
                    TechContact = contact,
                    DomainName = domainName,
                    AutoRenew = autoRenew,
                    DurationInYears = duration,
                    PrivacyProtectAdminContact = false,
                    PrivacyProtectRegistrantContact = false,
                    PrivacyProtectTechContact = false
                }
            );
            return result.OperationId;
        }
        catch (InvalidInputException)
        {
            _logger.LogInformation($"Unable to request registration for domain
 {domainName}");
            return null;
        }
    }
```

- API 세부 정보는 AWS SDK for .NET API 참조의 RegisterDomain을 참조하십시오.

CLI

AWS CLI

도메인을 등록하려면

다음 `register-domain` 명령은 도메인을 등록하여 JSON 형식 파일에서 모든 파라미터 값을 가져옵니다.

이 명령은 `us-east-1` 리전에서만 실행됩니다. 기본 리전이 `us-east-1`로 설정된 경우, `region` 파라미터를 생략할 수 있습니다.

```
aws route53domains register-domain \
    --region us-east-1 \
    --cli-input-json file://register-domain.json
```

`register-domain.json`의 콘텐츠:

```
{
    "DomainName": "example.com",
    "DurationInYears": 1,
    "AutoRenew": true,
    "AdminContact": {
        "FirstName": "Martha",
        "LastName": "Rivera",
        "ContactType": "PERSON",
        "OrganizationName": "Example",
        "AddressLine1": "1 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "mrivera@example.com"
    },
    "RegistrantContact": {
        "FirstName": "Li",
        "LastName": "Juan",
        "ContactType": "PERSON",
        "OrganizationName": "Example",
        "AddressLine1": "1 Main Street",
        "City": "Anytown",
```

```
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "ljuan@example.com"
    },
    "TechContact": {
        "FirstName": "Mateo",
        "LastName": "Jackson",
        "ContactType": "PERSON",
        "OrganizationName": "Example",
        "AddressLine1": "1 Main Street",
        "City": "Anytown",
        "State": "WA",
        "CountryCode": "US",
        "ZipCode": "98101",
        "PhoneNumber": "+1.8005551212",
        "Email": "mjackson@example.com"
    },
    "PrivacyProtectAdminContact": true,
    "PrivacyProtectRegistrantContact": true,
    "PrivacyProtectTechContact": true
}
```

출력:

```
{
    "OperationId": "b114c44a-9330-47d1-a6e8-a0b11example"
}
```

작업이 성공했는지 확인하기 위해 를 실행할 수 있습니다`get-operation-detail`. 자세한 내용은 get-domain-detail을 참조하세요.

자세한 내용은 Amazon Route 53 개발자 안내서의 새 도메인 등록을 참조하세요.

`ExtraParams`의 값이 필요한 최상위 도메인(TLD)과 유효한 값에 대한 자세한 내용은 Amazon Route 53 API 참조의 ExtraParam을 참조하세요.

- API 세부 정보는 AWS CLI 명령 참조의 RegisterDomain을 참조하세요.

Java

SDK for Java 2.x

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
   public static String requestDomainRegistration(Route53DomainsClient
route53DomainsClient,
           String domainSuggestion,
           String phoneNumber,
           String email,
           String firstName,
           String lastName,
           String city) {

       try {
           ContactDetail contactDetail = ContactDetail.builder()
                   .contactType(ContactType.COMPANY)
                   .state("LA")
                   .countryCode(CountryCode.IN)
                   .email(email)
                   .firstName(firstName)
                   .lastName(lastName)
                   .city(city)
                   .phoneNumber(phoneNumber)
                   .organizationName("My Org")
                   .addressLine1("My Address")
                   .zipCode("123 123")
                   .build();

           RegisterDomainRequest domainRequest = RegisterDomainRequest.builder()
                   .adminContact(contactDetail)
                   .registrantContact(contactDetail)
                   .techContact(contactDetail)
                   .domainName(domainSuggestion)
                   .autoRenew(true)
                   .durationInYears(1)
                   .build();
```

```
            RegisterDomainResponse response =
 route53DomainsClient.registerDomain(domainRequest);
            System.out.println("Registration requested. Operation Id: " +
 response.operationId());
            return response.operationId();

        } catch (Route53Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
        return "";
    }
```

- API 세부 정보는 AWS SDK for Java 2.x API 참조의 RegisterDomain을 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
suspend fun requestDomainRegistration(
    domainSuggestion: String?,
    phoneNumberVal: String?,
    emailVal: String?,
    firstNameVal: String?,
    lastNameVal: String?,
    cityVal: String?,
): String? {
    val contactDetail =
        ContactDetail {
            contactType = ContactType.Company
            state = "LA"
            countryCode = CountryCode.In
            email = emailVal
            firstName = firstNameVal
```

```
            lastName = lastNameVal
            city = cityVal
            phoneNumber = phoneNumberVal
            organizationName = "My Org"
            addressLine1 = "My Address"
            zipCode = "123 123"
        }

    val domainRequest =
        RegisterDomainRequest {
            adminContact = contactDetail
            registrantContact = contactDetail
            techContact = contactDetail
            domainName = domainSuggestion
            autoRenew = true
            durationInYears = 1
        }

    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        val response = route53DomainsClient.registerDomain(domainRequest)
        println("Registration requested. Operation Id: ${response.operationId}")
        return response.operationId
    }
}
```

- API 세부 정보는 AWS SDK for Kotlin API 참조의 RegisterDomain을 참조하십시오.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **`ViewBilling`** 함께 사용

다음 코드 예제는 `ViewBilling`의 사용 방법을 보여 줍니다.

작업 예제는 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 다음 코드 예제에서는 컨텍스트 내에서 이 작업을 확인할 수 있습니다.

- 기본 사항 알아보기

.NET

AWS SDK for .NET

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    /// <summary>
    /// View billing records for the account between a start and end date.
    /// </summary>
    /// <param name="startDate">The start date for billing results.</param>
    /// <param name="endDate">The end date for billing results.</param>
    /// <returns>A collection of billing records.</returns>
    public async Task<List<BillingRecord>> ViewBilling(DateTime startDate,
DateTime endDate)
    {
        var results = new List<BillingRecord>();
        var paginateBilling = _amazonRoute53Domains.Paginators.ViewBilling(
            new ViewBillingRequest()
            {
                Start = startDate,
                End = endDate
            });

        // Get the entire list using the paginator.
        await foreach (var billingRecords in paginateBilling.BillingRecords)
        {
            results.Add(billingRecords);
        }
        return results;
    }
```

- API 세부 정보는 AWS SDK for .NET API 참조의 ViewBilling을 참조하십시오.

CLI

AWS CLI

현재 AWS 계정의 도메인 등록 요금에 대한 결제 정보를 가져오려면

다음 `view-billing` 명령은 2018년 1월 1일(1514764800 Unix 시간)부터 2019년 12월 31일 자정(1577836800 Unix 시간)까지의 기간 동안 현재 계정의 모든 도메인 관련 결제 레코드를 반환합니다.

이 명령은 `us-east-1` 리전에서만 실행됩니다. 기본 리전이 `us-east-1`로 설정된 경우, `region` 파라미터를 생략할 수 있습니다.

```
aws route53domains view-billing \
    --region us-east-1 \
    --start-time 1514764800 \
    --end-time 1577836800
```

출력:

```
{
    "BillingRecords": [
        {
            "DomainName": "example.com",
            "Operation": "RENEW_DOMAIN",
            "InvoiceId": "149962827",
            "BillDate": 1536618063.181,
            "Price": 12.0
        },
        {
            "DomainName": "example.com",
            "Operation": "RENEW_DOMAIN",
            "InvoiceId": "290913289",
            "BillDate": 1568162630.884,
            "Price": 12.0
        }
    ]
}
```

자세한 내용은 Amazon Route 53 API 참조의 ViewBilling을 확인하세요.

- API 세부 정보는 AWS CLI 명령 참조의 ViewBilling을 참조하세요.

Java

SDK for Java 2.x

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
   public static void listBillingRecords(Route53DomainsClient
route53DomainsClient) {
       try {
           Date currentDate = new Date();
           LocalDateTime localDateTime =
currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime();
           ZoneOffset zoneOffset = ZoneOffset.of("+01:00");
           LocalDateTime localDateTime2 = localDateTime.minusYears(1);
           Instant myStartTime = localDateTime2.toInstant(zoneOffset);
           Instant myEndTime = localDateTime.toInstant(zoneOffset);

           ViewBillingRequest viewBillingRequest = ViewBillingRequest.builder()
                   .start(myStartTime)
                   .end(myEndTime)
                   .build();

           ViewBillingIterable listRes =
route53DomainsClient.viewBillingPaginator(viewBillingRequest);
           listRes.stream()
                   .flatMap(r -> r.billingRecords().stream())
                   .forEach(content -> System.out.println(" Bill Date:: " +
content.billDate() +
                           " Operation: " + content.operationAsString() +
                           " Price: " + content.price()));

       } catch (Route53Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- API 세부 정보는 AWS SDK for Java 2.x API 참조의 ViewBilling을 참조하십시오.

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예시 리포지토리에서 전체 예시를 찾고 설정 및 실행하는 방법을 배워보세요.

```
suspend fun listBillingRecords() {
    val currentDate = Date()
    val localDateTime =
 currentDate.toInstant().atZone(ZoneId.systemDefault()).toLocalDateTime()
    val zoneOffset = ZoneOffset.of("+01:00")
    val localDateTime2 = localDateTime.minusYears(1)
    val myStartTime = localDateTime2.toInstant(zoneOffset)
    val myEndTime = localDateTime.toInstant(zoneOffset)
    val timeStart: Instant? = myStartTime?.let { Instant(it) }
    val timeEnd: Instant? = myEndTime?.let { Instant(it) }

    val viewBillingRequest =
        ViewBillingRequest {
            start = timeStart
            end = timeEnd
        }

    Route53DomainsClient { region = "us-east-1" }.use { route53DomainsClient ->
        route53DomainsClient
            .viewBillingPaginated(viewBillingRequest)
            .transform { it.billingRecords?.forEach { obj -> emit(obj) } }
            .collect { billing ->
                println("Bill Date: ${billing.billDate}")
                println("Operation: ${billing.operation}")
                println("Price: ${billing.price}")
            }
    }
}
```

- API 세부 정보는 AWS SDK for Kotlin API 참조의 ViewBilling을 참조하십시오.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK에서 Route 53 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

Amazon Route 53의 보안

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드 내 보안 및 클라우드의 보안으로 설명합니다.

- 클라우드 보안 - AWS 는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사원은 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. Amazon Route 53에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 제공 범위 내AWS 서비스를 참조하십시오.
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 데이터의 민감도, 회사 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Route 53 사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제들에서는 보안 및 규정 준수 목표를 충족하도록 Route 53를 구성하는 방법을 보여줍니다. 또한 Route 53 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

- Route 53의 데이터 보호
- Amazon Route 53의 Identity and Access Management
- Amazon Route 53의 로깅 및 모니터링
- Amazon Route 53의 규정 준수 확인
- Amazon Route 53의 복원성
- Amazon Route 53의 인프라 보안

Route 53의 데이터 보호

AWS 공동 책임 모델 Amazon Route 53의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세

요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM)를 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- AWS 암호화 솔루션과 내부의 모든 기본 보안 제어를 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 AWS 통해에 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 Route 53 또는 기타 AWS 서비스 에서 콘솔, API AWS CLI또는 AWS SDKs를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명을 URL에 포함해서는 안 됩니다.

Route 53에서 누락된 위임 레코드 보호

Route 53를 사용하면 고객은 `example.com`과 같은 호스팅 영역을 생성하여 DNS 레코드를 호스팅할 수 있습니다. 각 호스팅 영역에는 고객이 상위 도메인에서 NS 레코드를 구성하는 데 사용할 수 있는 4개의 이름 서버 집합인 '위임 세트'가 함께 제공됩니다. 이 NS 레코드를 '위임 NS 레코드' 또는 '위임 레코드'라고 할 수 있습니다.

`example.com` Route 53 호스팅 영역이 권한을 갖추려면 `example.com` 도메인의 올바른 소유자가 도메인 등록 기관을 통해 '.com' 상위 도메인에서 위임 레코드를 구성해야 합니다. 연결된 호스팅 영역이 삭제되어 고객이 상위 도메인에 구성된 4개의 이름 서버에 대한 액세스 권한을 잃는 경우 공격자가 악용할 위험이 발생할 수 있습니다. 이를 '매달린 위임 레코드' 위험이라고 합니다.

Route 53는 호스팅 영역이 삭제되는 경우 매달린 위임 레코드 위험으로부터 보호합니다. 삭제 후 도메인 이름이 동일한 새 호스팅 영역을 생성하는 경우 Route 53는 삭제된 호스팅 영역을 가리키는 위임 레코드가 상위 도메인에 여전히 존재하는지 확인합니다. 이 경우 Route 53는 중복 이름 서버가 할당되지 않게 합니다. 방법은 다음 예제의 시나리오 1과 같습니다.

그러나 다음 예제의 시나리오 2 및 3에 자세히 설명된 것처럼 Route 53가 보호할 수 없는 다른 매달린 위임 레코드 위험이 있습니다. 이러한 광범위한 위험으로부터 보호하려면 상위 NS 레코드가 Route 53 호스팅 영역의 위임 세트와 일치하는지 확인하세요. Route 53 콘솔 또는를 통해 호스팅 영역의 위임 세트를 찾을 수 있습니다 AWS CLI. 자세한 내용은 레코드 나열 또는 get-hosted-zone을 참조하세요.

또한 Route 53 호스팅 영역에 대해 DNSSEC 서명을 활성화하면 위에 언급된 모범 사례를 넘어서는 또 다른 보호 계층의 역할을 할 수 있습니다. DNSSEC는 DNS 응답이 신뢰할 수 있는 출처에서 온 것임을 인증하여 이 위험으로부터 효과적으로 보호합니다. 자세한 정보는 Amazon Route 53에서 DNSSEC 서명 구성 섹션을 참조하세요.

예시

다음 예제에서는 도메인 `example.com`, 하위 도메인 `child.example.com`이 있다고 가정합니다. 다양한 시나리오에서 매달린 위임 레코드를 생성하는 방법, Route 53가 도메인을 남용으로부터 보호하는 방법, 매달린 위임 레코드와 관련된 위험을 효과적으로 완화하는 방법을 설명합니다.

시나리오 1:

> 4개의 이름 서버 <ns1>, <ns2>, <ns3>, <ns4>로 호스팅 영역 `child.example.com`를 생성할 수 있습니다. 호스팅 영역 `example.com`에서 위임을 올바르게 설정하여 4개의 이름 서버 <ns1>, <ns2>, <ns3>, <ns4>를 사용하여 `child.example.com`에 대한 위임 NS 레코드를 생성합니다. `example.com`에서 위임 NS 레코드를 제거하지 않고 `child.example.com` 호스팅 영역이 삭제되면 Route 53는 <ns1>, <ns2>, <ns3>, <ns4>가 도메인 이름이 동일한 새로 생성된 호스팅 영역에 할당되는 것을 방지하여 매달린 위임 레코드 위험으로부터 `child.example.com`을 보호합니다.

시나리오 2:

> 시나리오 1과 비슷하지만 이번에는 하위 호스팅 영역과 호스팅 영역 `example.com`의 위임 NS 레코드를 삭제합니다. 그러나 하위 호스팅 영역을 생성하지 않고 위임 NS 레코드 <ns1>, <ns2>, <ns3>, <ns4>를 다시 추가합니다. 여기서는 <ns1>, <ns2>, <ns3>, <ns4>가 매달린 위임 레코드입니다. Route 53가 <ns1>, <ns2>, <ns3>, <ns4>가 할당되는 것을 막고 있던 보류를 제거하고 이제 새로 생성된 호스팅 영역이 위의 이름 서버를 사용하도록 허용하기 때문입니다. 위험을 완화하려면 위임 레코드에서 <ns1>, <ns2>, <ns3>, <ns4>를 제거하고 하위 호스팅 영역이 생성된 후에만 다시 추가합니다.

시나리오 3:

이 시나리오에서는 이름 서버 <ns1>, <ns2>, <ns3>, <ns4>를 사용하여 Route 53 재사용 가능 위임 세트를 생성합니다. 그런 다음 상위 도메인 `.com`의 이러한 이름 서버에 도메인 `example.com`을 위임합니다. 하지만 재사용 가능한 위임 세트에 아직 `example.com`에 대한 호스팅 영역을 생성하지 않았습니다. 따라서 <ns1>, <ns2>, <ns3>, <ns4>는 매달린 위임 레코드입니다. 위험을 완화하려면 이름 서버 <ns1>, <ns2>, <ns3>, <ns4>가 있는 재사용 가능한 위임 세트를 사용하여 호스팅 영역을 생성합니다.

Amazon Route 53의 Identity and Access Management

도메인을 등록하거나 레코드를 업데이트하는 등 Amazon Route 53 리소스에서 작업을 수행하려면 AWS Identity and Access Management (IAM) 승인된 AWS 사용자임을 인증해야 합니다. Route 53 콘솔을 사용하는 경우 AWS 사용자 이름과 암호를 제공하여 자격 증명을 인증합니다.

자격 증명을 인증한 후 IAM은 작업을 수행하고 리소스에 액세스할 수 있는 권한이 있는지 AWS 확인하여에 대한 액세스를 제어합니다. 계정 관리자인 경우 IAM을 사용하여 계정과 관련된 리소스에 대한 다른 사용자의 액세스를 제어할 수 있습니다.

이 장에서는 IAM 및 Route 53를 사용하여 리소스를 보호하는 방법을 설명합니다.

주제

- ID를 통한 인증
- 액세스 제어
- Amazon Route 53 리소스에 대한 액세스 권한 관리 개요
- Amazon Route 53에 대한 자격 증명 기반 정책(IAM 정책) 사용
- Amazon Route 53 Resolver에 서비스 연결 역할 사용
- AWS Amazon Route 53에 대한 관리형 정책
- IAM 정책 조건을 사용하여 세분화된 액세스 제어 구현
- Amazon Route 53 API 권한: 작업, 리소스 및 조건 참조

ID를 통한 인증

인증은 자격 증명 AWS 으로에 로그인하는 방법입니다. IAM 사용자 또는 AWS 계정 루트 사용자 IAM 역할을 수임하여 로 인증(로그인 AWS)되어야 합니다.

자격 증명 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 자격 증명 AWS 으로에 로그인할 수 있습니다 AWS IAM Identity Center (IAM Identity Center) 사용자, 회사의 Single Sign-On 인증 및 Google 또는 Facebook 자격 증명은 페더레이션 자격 증명의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 AWS 에 액세스하면 간접적으로 역할을 수임하게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 에 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의에 로그인하는 방법을 AWS참조하세요. AWS 계정

AWS 프로그래밍 방식으로에 액세스하는 경우는 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트(SDK)와 명령줄 인터페이스(CLI)를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 직접 요청에 서명해야 합니다. 권장 방법을 사용하여 요청에 직접 서명하는 자세한 방법은 IAM 사용 설명서에서 API 요청용AWS Signature Version 4를 참조하세요.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어는 다중 인증(MFA)을 사용하여 계정의 보안을 강화할 것을 AWS 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 다중 인증 및 IAM 사용 설명서에서 IAM의AWS 다중 인증을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 테 AWS 계정 루트 사용자라고 하며 계정을 생성하는 데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명을 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 포함한 인간 사용자에게 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 AWS 서비스 에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, AWS Directory Service, Identity Center 디렉터리 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스 에 액세스하는 모든 사용자의 사용자입니다. 페더레이션 자격 증명에 액세스할 때 역할을 AWS 계정수임하고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을(를) 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 모든 및 애플리케이션에서 사용할 수 있도록 자체 ID 소스의

사용자 AWS 계정 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇인가요?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한이 AWS 계정 있는 내 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 증명이 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명이 필요한 특정 사용 사례가 있는 경우, 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우, 정기적으로 액세스 키 교체를 참조하세요.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 자격 증명을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서에서 IAM 사용자 사용 사례를 참조하세요.

IAM 역할

IAM 역할은 특정 권한이 AWS 계정 있는 내 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 에서 IAM 역할을 일시적으로 수임하려면 사용자에서 IAM 역할(콘솔)로 전환할 AWS Management Console수 있습니다. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 AWS CLI 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 관련 역할에 대한 자세한 내용은 IAM 사용 설명서의 Create a role for a third-party identity provider (federation)를 참조하세요. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 집합을 IAM의 역할과 연관짓습니다. 권한 집합에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 집합을 참조하세요.

- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 에서는 (역할을 프록시로 사용하는 대신) 정책을 리소스에 직접 연결할 AWS 서비스 수 있습니다. 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하세요.
- 교차 서비스 액세스 - 일부는 다른에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어, 서비스에서 호출하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 위탁자의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 다른 AWS 서비스 또는 리소스와의 상호 작용을 완료해야 하는 요청을 수신할 때만 수행됩니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.
  - 서비스 연결 역할 - 서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.
- Amazon EC2에서 실행되는 애플리케이션 - IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로필에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

액세스 제어

Amazon Route 53 리소스를 생성, 업데이트, 삭제 또는 나열하려면 작업을 수행할 수 있는 권한이 필요하며 해당 리소스에 액세스할 수 있는 권한이 필요합니다.

다음 섹션에서는 Route 53에 대한 권한을 관리하는 방법을 설명합니다. 먼저 개요를 읽어 보면 도움이 됩니다.

Amazon Route 53 리소스에 대한 액세스 권한 관리 개요

모든 AWS 리소스는 AWS 계정이 소유하며, 리소스를 생성하거나 액세스할 수 있는 권한은 권한 정책에 의해 관리됩니다.

> **Note**
>
> 계정 관리자 또는 관리자 사용자는 관리자 권한이 있는 사용자입니다. 관리자에 대한 자세한 내용은 IAM 사용 설명서의 IAM 모범 사례를 참조하세요.

권한을 부여할 때는 권한을 받는 사용자, 해당 권한의 대상 리소스, 그리고 해당 권한으로 수행할 수 있는 작업을 결정합니다.

사용자는 AWS 외부에서와 상호 작용하려는 경우 프로그래밍 방식 액세스가 필요합니다 AWS Management Console. 프로그래밍 방식 액세스를 부여하는 방법은 액세스 중인 사용자 유형에 따라 다릅니다 AWS.

사용자에게 프로그래밍 방식 액세스 권한을 부여하려면 다음 옵션 중 하나를 선택합니다.

프로그래밍 방식 액세스가 필요한 사용자는 누구인가요?	To	액세스 권한을 부여하는 사용자
작업 인력 ID (IAM Identity Center가 관리하는 사용자)	임시 자격 증명을 사용하여 AWS CLI, AWS SDKs 또는 AWS APIs.	사용하고자 하는 인터페이스에 대한 지침을 따릅니다. • 의 경우 AWS Command Line Interface 사용 설명서의 AWS CLI 를 사용하도록 구성을 AWS IAM Identity Center AWS CLI참조하세요.

프로그래밍 방식 액세스가 필요한 사용자는 누구인가요?	To	액세스 권한을 부여하는 사용자
		• AWS SDKs, 도구 및 AWS APIs의 경우 SDK 및 도구 참조 안내서의 IAM Identity Center 인증을 참조하세요. AWS SDKs
IAM	임시 자격 증명을 사용하여 AWS CLI, AWS SDKs 또는 AWS APIs.	IAM 사용 설명서의 AWS 리소스와 함께 임시 자격 증명 사용의 지침을 따릅니다.
IAM	(권장되지 않음) 장기 자격 증명을 사용하여 AWS CLI, AWS SDKs 또는 AWS APIs.	사용하고자 하는 인터페이스에 대한 지침을 따릅니다. • 자세한 AWS CLI내용은 AWS Command Line Interface 사용 설명서의 IAM 사용자 자격 증명을 사용하여 인증을 참조하세요. • AWS SDKs 및 도구의 경우 SDK 및 도구 참조 안내서의 장기 자격 증명을 사용하여 인증을 참조하세요. AWS SDKs • AWS APIs 경우 IAM 사용 설명서의 IAM 사용자의 액세스 키 관리를 참조하세요.

주제

- Amazon Route 53 리소스의 ARN
- 리소스 소유권 이해
- 리소스 액세스 관리
- 정책 요소 지정: 리소스, 작업, 효과 및 보안 주체
- 정책에서 조건 지정

Amazon Route 53 리소스의 ARN

Amazon Route 53는 DNS, 상태 확인, 도메인 등록을 위해 다양한 리소스 유형을 지원합니다. 정책에서 ARN에 대해 *를 사용하여 다음 리소스에 대한 액세스 권한을 부여하거나 거부할 수 있습니다.

- 상태 확인
- 호스팅 영역
- 재사용 가능한 위임 세트
- 리소스 레코드 세트 변경 배치의 상태(API에 한함)
- 트래픽 정책(트래픽 흐름)
- 트래픽 정책 인스턴스(트래픽 흐름)

권한을 지원하지 않는 Route 53 리소스도 있습니다. 다음 리소스의 경우, 액세스 권한을 부여하거나 거부할 수 없습니다.

- 도메인
- 개별 레코드
- 도메인 태그
- 상태 확인 태그
- 호스팅 영역 태그

Route 53는 이러한 각 유형의 리소스로 작업하기 위한 API 작업을 제공합니다. 자세한 내용은 Amazon Route 53 API Reference를 확인하십시오. 작업과 각 작업을 사용할 권한을 부여하거나 거부하기 위해 지정하는 ARN의 목록은 Amazon Route 53 API 권한: 작업, 리소스 및 조건 참조 단원을 참조하십시오.

리소스 소유권 이해

AWS 계정은 누가 리소스를 생성했는지에 관계없이 계정에 생성된 리소스를 소유합니다. 특히 리소스 소유자는 리소스 생성 요청을 인증하는 AWS 보안 주체 엔터티(즉, 루트 계정 또는 IAM 역할)의 계정입니다.

다음의 예제에서는 이러한 작동 방법을 설명합니다.

- AWS 계정의 루트 계정 자격 증명을 사용하여 호스팅 영역을 생성하는 경우 AWS 계정은 리소스의 소유자입니다.

- AWS 계정에서 사용자를 생성하고 해당 사용자에게 호스팅 영역을 생성할 수 있는 권한을 부여하는 경우 사용자는 호스팅 영역을 생성할 수 있습니다. 하지만 호스팅 영역 리소스는 해당 사용자가 속한 AWS 계정이 소유합니다.
- AWS 계정에서 호스팅 영역을 생성할 수 있는 권한이 있는 IAM 역할을 생성하는 경우 해당 역할을 수임할 수 있는 사람은 누구나 호스팅 영역을 생성할 수 있습니다. 역할이 속한 AWS 계정이 호스팅 영역 리소스를 소유합니다.

리소스 액세스 관리

권한 정책은 누가 무엇에 액세스 할 수 있는지를 지정합니다. 이 섹션에서는 Amazon Route 53에 대한 권한 정책을 생성하기 위한 옵션을 설명합니다. IAM 정책 구문과 설명에 대한 일반적인 내용은 IAM 사용 설명서의 AWS IAM 정책 참조를 참조하세요.

IAM 자격 증명에 연결된 정책을 자격 증명 기반(identity-based) 정책(IAM 정책)이라 하고 리소스에 연결된 정책을 리소스 기반(resource-based) 정책이라고 합니다. Route 53는 자격 증명 기반 정책(IAM 정책)만 지원합니다.

주제

- 자격 증명 기반 정책(IAM 정책)
- 리소스 기반 정책

자격 증명 기반 정책(IAM 정책)

정책을 IAM 보안 인증에 연결할 수 있습니다. 예를 들면, 다음을 수행할 수 있습니다:

- 계정 내 사용자 또는 그룹에 권한 정책 연결 - 계정 관리자는 특정 사용자에 연결된 권한 정책을 사용하여 해당 사용자에게 Amazon Route 53 리소스 생성 권한을 부여할 수 있습니다.
- 역할에 권한 정책 연결(교차 계정 권한 부여) - 다른 AWS 계정에서 생성한 사용자에게 Route 53 작업을 수행할 수 있는 권한을 부여할 수 있습니다. 이렇게 하려면 권한 정책을 IAM 역할에 연결한 다음 다른 계정의 사용자가 역할을 담당할 수 있도록 허용합니다. 다음 예제에서는 계정 A와 계정 B라는 두 개의 AWS 계정에 대해 이 작업을 적용하는 방법을 설명합니다.
  1. 계정 A 관리자는 IAM 역할을 생성하고 계정 A가 소유한 리소스를 생성하거나 액세스할 권한을 부여하는 권한 정책을 역할에 연결합니다.
  2. 계정 A 관리자는 신뢰 정책을 역할에 연결합니다. 신뢰 정책은 역할을 담당할 수 있는 보안 주체로 계정 B를 식별합니다.

3. 그런 다음 계정 B 관리자는 역할을 담당할 권한을 계정 B의 사용자 또는 그룹에게 위임할 수 있습니다. 이렇게 하면 계정 B의 사용자가 계정 A에서 리소스를 생성하거나 액세스할 수 있습니다.

다른 AWS 계정의 사용자에게 권한을 위임하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 액세스 관리를 참조하세요.

다음 예제 정책은 사용자가 `CreateHostedZone` 작업을 수행하여 AWS 계정에 대한 퍼블릭 호스팅 영역을 생성할 수 있도록 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone"
            ],
            "Resource":"*"
        }
    ]
}
```

정책을 프라이빗 호스팅 영역에도 적용하려면 아래 예제와 같이 Route 53 `AssociateVPCWithHostedZone` 작업 및 두 가지 Amazon EC2 작업, 즉 `DescribeVpcs` 및 `DescribeRegion`을 사용할 수 있는 권한을 부여해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource":"*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
```

```
                "ec2:DescribeRegion"
            ],
            "Resource":"*"
        },
    ]
}
```

Route 53 자격 증명에 정책을 연결하는 방법에 대한 자세한 내용은 Amazon Route 53에 대한 자격 증명 기반 정책(IAM 정책) 사용 섹션을 참조하세요. 사용자, 그룹, 역할 및 권한에 대한 자세한 내용은 IAM User Guide의 Identities (users, groups, and roles)를 참조하세요.

리소스 기반 정책

Amazon S3 등 다른 서비스에서도 권한 정책을 리소스에 연결할 수 있습니다. 예를 들어, 정책을 S3 버킷에 연결하여 해당 버킷에 대한 액세스 권한을 관리할 수 있습니다. Amazon Route 53는 리소스에 정책을 연결하는 것을 지원하지 않습니다.

정책 요소 지정: 리소스, 작업, 효과 및 보안 주체

Amazon Route 53에는 각 Route 53 리소스(Amazon Route 53 리소스의 ARN 참조)에서 사용할 수 있는 API 작업(Amazon Route 53 API 참조)이 포함되어 있습니다. 사용자 또는 연동 사용자에게 이러한 작업 중 하나 또는 전부를 수행할 권한을 부여할 수 있습니다. 도메인 등록과 같은 일부 API 작업을 수행하려면 둘 이상의 작업에 대한 권한이 필요할 수 있습니다.

다음은 기본 정책 요소입니다.

- 리소스 – Amazon 리소스 이름(ARN)을 사용하여 정책을 적용할 리소스를 식별합니다. 자세한 설명은 Amazon Route 53 리소스의 ARN 섹션을 참조하십시오.
- 조치 – 조치 키워드를 사용하여 허용 또는 거부할 리소스 작업을 식별합니다. 예를 들어, 지정된 `Effect`에 따라 사용자는 `route53:CreateHostedZone` 권한으로 Route 53 `CreateHostedZone` 작업을 수행할 수 있거나 수행할 수 없습니다.
- 효과 – 사용자가 지정된 리소스에서 작업을 수행하려고 할 때 효과를 허용 또는 거부로 지정합니다. 작업에 대한 액세스 권한을 명시적으로 부여하지 않으면 액세스는 묵시적으로 거부됩니다. 다른 정책에서 액세스 권한을 부여하는 경우라도 사용자가 해당 리소스에 액세스할 수 없도록 하기 위해 리소스에 대한 권한을 명시적으로 거부할 수도 있습니다.
- 보안 주체 – ID 기반 정책(IAM 정책)에서 정책이 연결되는 사용자는 암시적인 보안 주체입니다. 리소스 기반 정책의 경우, 사용자, 계정, 서비스 또는 권한의 수신자인 기타 개체를 지정합니다(리소스 기반 정책에만 해당). Route 53에서는 리소스 기반 정책을 지원하지 않습니다.

IAM 정책 구문과 설명에 대한 자세한 내용은 IAM 사용 설명서의 AWS IAM 정책 참조를 참조하세요.

모든 Route 53 API 작업과 해당 작업이 적용되는 리소스를 보여주는 목록(list)은 Amazon Route 53 API 권한: 작업, 리소스 및 조건 참조 섹션을 참조하세요.

정책에서 조건 지정

권한을 부여할 때 IAM 정책 언어를 사용하여 정책이 언제 적용되는지를 지정할 수 있습니다. 예를 들어, 특정 날짜 이후에만 정책을 적용할 수 있습니다. 정책 언어의 조건 지정에 대한 자세한 내용은 IAM 사용 안내서의 IAM JSON 정책 요소: 조건을 참조하세요.

조건을 표시하려면 미리 정의된 조건 키를 사용합니다. Route 53에만 해당되는 특정한 조건 키는 없습니다. 그러나 필요에 따라 사용할 수 있는 AWS 광범위한 조건 키가 있습니다. 전체 AWS 와이드 키 목록은 IAM 사용 설명서의 조건에 사용 가능한 키를 참조하세요.

Amazon Route 53에 대한 자격 증명 기반 정책(IAM 정책) 사용

이 주제에서는 자격 증명 기반 정책의 예를 통해 계정 관리자가 IAM 자격 증명에 권한 정책을 연결함으로써 Amazon Route 53 리소스에 대한 작업 수행 권한을 부여하는 방법을 보여 줍니다.

> **Important**
>
> Route 53 리소스 액세스를 관리하기 위한 기본 개념과 옵션을 설명하는 소개 주제를 먼저 읽어 보는 것이 좋습니다. 자세한 내용은 Amazon Route 53 리소스에 대한 액세스 권한 관리 개요 단원을 참조하십시오.

> **Note**
>
> 액세스 권한을 부여할 때 호스팅 영역과 Amazon VPC가 동일한 파티션에 속해 있어야 합니다. 파티션은의 그룹입니다 AWS 리전. 각 파티션 AWS 계정 은 하나의 파티션으로 범위가 지정됩니다.
> 지원되는 파티션은 다음과 같습니다.
>
> - `aws` - AWS 리전
> - `aws-cn` - 중국 리전
> - `aws-us-gov` - AWS GovCloud (US) Region

자세한 내용은 AWS 일반 참조의 액세스 관리 및 Amazon Route 53 엔드포인트 및 할당량을 참조하세요.

주제

- Amazon Route 53 콘솔 사용에 필요한 권한
- 도메인 레코드 소유자에 대한 사용 권한 예제
- DNSSEC 서명에 필요한 Route 53 고객 관리형 키 권한
- 고객 관리형 정책 예

다음 예는 권한 정책을 보여 줍니다. `Sid`(문 ID)는 선택 사항입니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid" : "AllowPublicHostedZonePermissions",
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53:UpdateHostedZoneComment",
                "route53:GetHostedZone",
                "route53:ListHostedZones",
                "route53:DeleteHostedZone",
                "route53:ChangeResourceRecordSets",
                "route53:ListResourceRecordSets",
                "route53:GetHostedZoneCount",
                "route53:ListHostedZonesByName"
            ],
            "Resource": "*"
        },
        {
         "Sid" : "AllowHealthCheckPermissions",
            "Effect": "Allow",
            "Action": [
                "route53:CreateHealthCheck",
                "route53:UpdateHealthCheck",
                "route53:GetHealthCheck",
                "route53:ListHealthChecks",
```

```
                "route53:DeleteHealthCheck",
                "route53:GetCheckerIpRanges",
                "route53:GetHealthCheckCount",
                "route53:GetHealthCheckStatus",
                "route53:GetHealthCheckLastFailureReason"
            ],
            "Resource": "*"
        }
    ]
}
```

이 정책에는 두 가지 문이 포함됩니다.

- 첫 번째 문은 퍼블릭 호스팅 영역과 그 레코드를 생성 및 관리하는 데 필요한 작업에 대한 권한을 부여합니다. Amazon 리소스 이름(ARN)의 와일드카드 문자(*)는 현재 AWS 계정이 소유한 모든 호스팅 영역에 대한 액세스 권한을 부여합니다.
- 두 번째 문은 상태 확인을 생성 및 관리하는 데 필요한 모든 작업 권한을 부여합니다.

작업과 각 작업을 사용할 권한을 부여하거나 거부하기 위해 지정하는 ARN의 목록은 Amazon Route 53 API 권한: 작업, 리소스 및 조건 참조 단원을 참조하세요.

Amazon Route 53 콘솔 사용에 필요한 권한

Amazon Route 53 콘솔에 대한 전체 액세스 권한을 부여하려면 다음 권한 정책에서 권한을 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "route53:*",
                "route53domains:*",
                "tag:*",
                "ssm:GetParametersByPath",
                "cloudfront:ListDistributions",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticbeanstalk:DescribeEnvironments",
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
```

```
                "s3:GetBucketWebsite",
                "ec2:DescribeRegions",
                "ec2:DescribeVpcs",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:ModifyNetworkInterfaceAttribute",
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic",
                "sns:CreateTopic",
                "kms:ListAliases",
                "kms:DescribeKey",
                "kms:CreateKey",
                "kms:CreateAlias",
                "kms:Sign",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:PutMetricAlarm",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:GetMetricStatistics"
            ],
            "Resource":"*"
        },
        {
            "Effect": "Allow",
            "Action": "apigateway:GET",
            "Resource": "arn:aws:apigateway:*::/domainnames"
        }
    ]
}
```

다음은 권한이 필요한 이유입니다.

`route53:*`

다음을 제외한 모든 Route 53 작업을 수행할 수 있습니다.

- 별칭 대상(Alias Target) 값이 CloudFront 배포, Elastic Load Balancing 로드 밸런서, Elastic Beanstalk 환경 또는 Amazon S3 버킷인 별칭 레코드를 생성 및 업데이트합니다. (이 권한으로 [Alias Target] 값이 동일한 호스팅 영역의 다른 레코드가 되는 별칭 레코드를 생성할 수 있습니다.)

- 프라이빗 호스팅 영역 작업
- 도메인 작업
- CloudWatch 경보를 생성하고, 삭제하고, 볼 수 있게 해줍니다.
- Route 53 콘솔에서 CloudWatch 지표을 렌더링합니다.

`route53domains:*`

도메인에 대한 작업을 할 수 있게 해줍니다.

> **Important**
>
> `route53` 작업을 개별적으로 나열하는 경우, 도메인을 작업할 `route53:CreateHostedZone`을 포함해야 합니다. 도메인을 등록하는 동시에 호스팅 영역이 생성되므로, 도메인 등록 권한이 포함된 정책에는 호스팅 영역을 생성할 권한도 필요합니다.

도메인 등록과 관련해 Route 53는 개별 리소스에 대한 권한 부여 또는 거부를 지원하지 않습니다.

`route53resolver:*`

Route 53 Resolver로 작업할 수 있게 해줍니다.

`ssm:GetParametersByPath`

새 별칭 레코드, 프라이빗 호스팅 영역 및 상태 확인을 생성할 때 공개적으로 사용 가능한 리전을 가져올 수 있습니다.

`cloudfront:ListDistributions`

별칭 대상(Alias Target)의 값이 CloudFront 배포인 별칭 레코드를 생성 및 업데이트할 수 있게 해줍니다.

Route 53 콘솔을 사용하지 않는 경우에는 이러한 권한이 필요하지 않습니다. Route 53는 콘솔에 표시할 배포 목록을 가져오는 데만 이 권한을 사용합니다.

`elasticloadbalancing:DescribeLoadBalancers`

[Alias Target]의 값이 ELB 로드 밸런서인 별칭 레코드를 생성 및 업데이트할 수 있게 해줍니다.

Route 53 콘솔을 사용하지 않는 경우에는 이러한 권한이 필요하지 않습니다. Route 53는 콘솔에 표시할 로드 밸런서 목록을 가져오는 데만 이 권한을 사용합니다.

elasticbeanstalk:DescribeEnvironments

별칭 대상(Alias Target)의 값이 Elastic Beanstalk 환경인 별칭 레코드를 생성 및 업데이트할 수 있게 해줍니다.

Route 53 콘솔을 사용하지 않는 경우에는 이러한 권한이 필요하지 않습니다. Route 53는 콘솔에 표시할 환경 목록을 가져오는 데만 이 권한을 사용합니다.

s3:ListAllMyBuckets, **s3:GetBucketLocation** 및 **s3:GetBucketWebsite**

별칭 대상(Alias Target)의 값이 Amazon S3 버킷인 별칭 레코드를 생성 및 업데이트할 수 있게 해줍니다. (버킷이 웹 사이트 엔드포인트로 구성되어 있는 경우에만 Amazon S3 버킷의 별칭을 생성할 수 있습니다. `s3:GetBucketWebsite`는 필요한 구성 정보를 가져옵니다.)

Route 53 콘솔을 사용하지 않는 경우에는 이러한 권한이 필요하지 않습니다. Route 53는 콘솔에 표시할 버킷 목록을 가져오는 데만 이 권한을 사용합니다.

ec2:DescribeVpcs 및 **ec2:DescribeRegions**

프라이빗 호스팅 영역에 대한 작업을 할 수 있게 해줍니다.

나열된 모든 **ec2** 권한

Route 53 Resolver로 작업할 수 있게 해줍니다.

sns:ListTopics, **sns:ListSubscriptionsByTopic**, **sns:CreateTopic**, **cloudwatch:DescribeAlarms**, **cloudwatch:PutMetricAlarm**, **cloudwatch:DeleteAlarms**

CloudWatch 경보를 생성하고, 삭제하고, 볼 수 있게 해줍니다.

cloudwatch:GetMetricStatistics

CloudWatch 지표 상태 확인을 생성할 수 있게 해줍니다.

Route 53 콘솔을 사용하지 않는 경우에는 이러한 권한이 필요하지 않습니다. Route 53는 콘솔에 표시할 통계를 가져오는 데만 이 권한을 사용합니다.

apigateway:GET

별칭 대상(Alias Target)의 값이 Amazon API Gateway API인 별칭 레코드를 생성 및 업데이트할 수 있게 해줍니다.

Route 53 콘솔을 사용하지 않는 경우에는 이 권한이 필요하지 않습니다. Route 53는 콘솔에 표시할 API 목록을 가져오는 데만 이 권한을 사용합니다.

`kms:*`

를 사용하여 DNSSEC 서명을 활성화 AWS KMS 할 수 있습니다.

도메인 레코드 소유자에 대한 사용 권한 예제

리소스 레코드 세트 권한을 사용하면 AWS 사용자가 업데이트하거나 수정할 수 있는 항목을 제한하는 세분화된 권한을 설정할 수 있습니다. 자세한 내용은 IAM 정책 조건을 사용하여 세분화된 액세스 제어 구현 단원을 참조하십시오.

일부 시나리오에서는 호스팅 영역 소유자가 호스팅 영역의 전반적인 관리를 담당하고 조직의 다른 사람이 이러한 태스크의 하위 집합을 담당합니다. 예를 들어 DNSSEC 서명을 활성화한 호스팅 영역 소유자는 다른 사용자가 다른 태스크 중에 호스팅 영역의 리소스 세트 레코드(RR)를 추가하고 삭제할 수 있는 권한을 포함하는 IAM 정책을 생성하려고 할 수 있습니다. 호스팅 영역 소유자가 레코드 소유자 또는 다른 사용자에 대해 사용하도록 선택하는 특정 권한은 조직의 정책에 따라 달라집니다.

다음은 레코드 소유자가 RR, 트래픽 정책 및 상태 확인을 수정할 수 있도록 허용하는 IAM 정책의 예입니다. 이 정책을 사용하는 레코드 소유자는 영역 만들기 또는 삭제, 쿼리 로깅 활성화 또는 비활성화, 재사용 가능한 위임 집합 만들기 또는 삭제, DNSSEC 설정 변경과 같은 영역 수준 작업을 수행할 수 없습니다.

```
{
      "Sid": "Do not allow zone-level modification ",
      "Effect": "Allow",
      "Action": [
        "route53:ChangeResourceRecordSets",
        "route53:CreateTrafficPolicy",
        "route53:DeleteTrafficPolicy",
        "route53:CreateTrafficPolicyInstance",
        "route53:CreateTrafficPolicyVersion",
        "route53:UpdateTrafficPolicyInstance",
        "route53:UpdateTrafficPolicyComment",
        "route53:DeleteTrafficPolicyInstance",
        "route53:CreateHealthCheck",
        "route53:UpdateHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:List*",
        "route53:Get*"
      ],
      "Resource": [
        "*"
```

```
      ]
}
```

DNSSEC 서명에 필요한 Route 53 고객 관리형 키 권한

Route 53에 대해 DNSSEC 서명을 활성화하면 Route 53은 AWS Key Management Service ()의 고객 관리형 키를 기반으로 키 서명 키(KSK)를 생성합니다AWS KMS. DNSSEC 서명을 지원하는 기존 고객 관리형 키를 사용하거나 새 고객 관리형 키를 생성할 수 있습니다. Route 53는 고객 관리형 키에 액세스할 수 있는 권한이 있어야 KSK를 생성할 수 있습니다.

Route 53가 고객 관리형 키에 액세스할 수 있도록 하려면 고객 관리형 키 정책에 다음 설명이 포함되어 있는지 확인해야 합니다.

```
{
            "Sid": "Allow Route 53 DNSSEC Service",
            "Effect": "Allow",
            "Principal": {
                "Service": "dnssec-route53.amazonaws.com"
            },
            "Action": ["kms:DescribeKey",
                       "kms:GetPublicKey",
                       "kms:Sign"],
            "Resource": "*"
        },
        {
            "Sid": "Allow Route 53 DNSSEC to CreateGrant",
            "Effect": "Allow",
            "Principal": {
                "Service": "dnssec-route53.amazonaws.com"
            },
            "Action": ["kms:CreateGrant"],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
```

혼동된 대리자 문제는 작업 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. AWS KMS 를 보호하기 위해 `aws:SourceAccount` 및 `aws:SourceArn` 조건(둘 다 또는 하나)의 조합을 제공하여 리소스 기반 정책의 리소스에 대한 서비스

권한을 선택적으로 제한할 수 있습니다. aws:SourceAccount는 호스팅 영역 소유자의 AWS 계정 ID입니다. aws:SourceArn는 호스팅 영역의 ARN입니다.

다음은 추가할 수 있는 권한의 두 가지 예입니다.

```
{
    "Sid": "Allow Route 53 DNSSEC Service",
    …
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
        },
        "ArnEquals": {
            "aws:SourceArn": "arn:aws:route53:::hostedzone/HOSTED_ZONE_ID"
        }
    }
},
```

– 또는 -

```
{
    "Sid": "Allow Route 53 DNSSEC Service",
    …
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": ["1111-2222-3333","4444-5555-6666"]
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:route53:::hostedzone/*"
        }
    }
},
```

자세한 내용은 IAM 사용 설명서의 혼동된 대리자 문제를 참조하세요.

고객 관리형 정책 예

Route 53 작업에 대한 권한을 허용하는 고유의 사용자 지정 IAM 정책을 생성할 수 있습니다. 지정된 권한이 필요한 IAM 그룹에 이러한 사용자 지정 정책을 연결할 수 있습니다. 이러한 정책은 Route 53

API, AWS SDKs 또는 AWS CLI를 사용할 때 작동합니다. 다음 예제에서는 몇 가지 일반적인 사용 사례의 권한을 보여 줍니다. 사용자에게 Route 53에 대한 전체 액세스 권한을 부여하는 정책에 대해서는 Amazon Route 53 콘솔 사용에 필요한 권한 섹션을 참조하세요.

예시

- 예 1: 모든 호스팅 영역에 대한 읽기 액세스 허용
- 예 2: 호스팅 영역 생성 및 삭제 허용
- 예 3: 모든 도메인에 대한 전체 액세스 허용(퍼블릭 호스팅 영역만 해당)
- 예 4: 인바운드 및 아웃바운드 Route 53 엔드포인트 생성 허용

예 1: 모든 호스팅 영역에 대한 읽기 액세스 허용

다음 권한 정책은 모든 호스팅 영역을 나열하고 호스팅 영역의 모든 레코드를 볼 수 있는 권한을 사용자에게 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "route53:GetHostedZone",
                "route53:ListResourceRecordSets"
            ],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:ListHostedZones"],
            "Resource":"*"
        }
    ]
}
```

예 2: 호스팅 영역 생성 및 삭제 허용

다음 권한 정책은 사용자가 호스팅 영역을 생성 및 업데이트하고, 변경 진행 상황을 추적할 수 있도록 합니다.

```
{
```

```
    "Version": "2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":["route53:CreateHostedZone"],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:DeleteHostedZone"],
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":["route53:GetChange"],
            "Resource":"*"
        }
    ]
}
```

예 3: 모든 도메인에 대한 전체 액세스 허용(퍼블릭 호스팅 영역만 해당)

다음 권한 정책은 도메인 등록 권한과 호스팅 영역 생성 권한을 비롯하여 사용자가 도메인 등록에 관한 모든 작업을 수행할 수 있도록 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "route53domains:*",
                "route53:CreateHostedZone"
            ],
            "Resource":"*"
        }
    ]
}
```

도메인을 등록하는 동시에 호스팅 영역이 생성되므로, 도메인 등록 권한이 포함된 정책에는 호스팅 영역을 생성할 권한도 필요합니다. (도메인 등록과 관련해 Route 53는 개별 리소스에 대한 권한 부여를 지원하지 않습니다.)

프라이빗 호스팅 영역 작업에 필요한 권한은 Amazon Route 53 콘솔 사용에 필요한 권한 단원을 참조하십시오.

예 4: 인바운드 및 아웃바운드 Route 53 엔드포인트 생성 허용

다음 권한 정책은 사용자가 Route 53 콘솔을 사용하여 Resolver 인바운드 및 아웃바운드 엔드포인트를 생성할 수 있도록 허용합니다.

이러한 권한 중 일부는 콘솔에서 엔드포인트를 생성하는 데에만 필요합니다. 프로그래밍 방식으로 인바운드 및 아웃바운드 엔드포인트를 생성할 수 있는 권한만 부여하려는 경우 이러한 권한을 생략할 수 있습니다.

- `route53resolver:ListResolverEndpoints`를 사용하면 엔드포인트가 생성되었는지 확인할 수 있도록 인바운드 또는 아웃바운드 엔드포인트 목록을 볼 수 있습니다.
- 가용 영역 목록을 표시하려면`DescribeAvailabilityZones`이 필요합니다.
- `DescribeVpcs`는 VPC 목록을 표시해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "route53resolver:CreateResolverEndpoint",
                "route53resolver:ListResolverEndpoints",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon Route 53 Resolver에 서비스 연결 역할 사용

Route 53 Resolver는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Resolver에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 Resolver에서 사전 정의하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 Resolver를 더 쉽게 설정할 수 있습니다. Resolver에서 서비스 연결 역할의 권한을 정의하므로 다르게 정의되지 않은 한, Resolver만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며, 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 링크 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 부주의로 삭제할 수 없기 때문에 Resolver 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하고 서비스 연결 역할(Service-Linked Role) 열에 예(Yes)가 있는 서비스를 찾으십시오. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 링크가 있는 예를 선택합니다.

주제

Resolver에 대한 서비스 연결 역할 권한

Resolver는 **AWSServiceRoleForRoute53Resolver** 서비스 연결 역할을 사용하여 사용자를 대신해 쿼리 로그를 제공합니다.

역할 권한 정책은 Resolver가 리소스에서 다음 작업을 완료하도록 허용합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
```

```
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "s3:GetBucketPolicy"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한 단원을 참조하세요.

Resolver에 대한 서비스 연결 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. Amazon Route 53 콘솔, AWS CLI또는 AWS API에서 해석기 쿼리 로그 구성 연결을 생성하면 Resolver가 서비스 연결 역할을 생성합니다.

> **Important**
>
> 이러한 서비스 연결 역할은 해당 역할이 지원하는 기능을 사용하는 다른 서비스에서 작업을 완료했을 경우 계정에 나타날 수 있습니다. 또한 Resolver 서비스가 서비스 연결 역할을 지원하기 시작한 2020년 8월 12일 이전에 이 서비스를 사용 중이었다면 Resolver에서 사용자 계정에 `AWSServiceRoleForRoute53Resolver` 역할을 이미 생성했습니다. 자세한 내용은 내 IAM 계정에 표시되는 새 역할을 참조하세요.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 새 Resolver 쿼리 로그 구성 연결을 생성하면 `AWSServiceRoleForRoute53Resolver` 서비스 연결 역할이 다시 생성됩니다.

Resolver에 대한 서비스 연결 역할 편집

Resolver에서는 `AWSServiceRoleForRoute53Resolver` 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 링크 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름

을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

Resolver에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 단, 서비스 링크 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

> **Note**
>
> 리소스를 삭제하려 할 때 Resolver 서비스가 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

`AWSServiceRoleForRoute53Resolver`에서 사용하는 Resolver 리소스를 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. Route 53 콘솔 메뉴를 확장합니다. 콘솔의 왼쪽 상단 모서리에서 세 개의 가로 막대 (☰) 아이콘을 선택합니다.
3. Resolver 메뉴에서 쿼리 로깅(Query logging)을 선택합니다.
4. 쿼리 로깅 구성 이름 옆의 확인란을 선택한 다음 삭제(Delete)를 선택합니다.
5. 쿼리 로깅 구성 삭제(Delete query logging configuration) 텍스트 상자에서 쿼리 로깅 중지(Stop logging queries)를 선택합니다.

   이렇게 하면 VPC 구성 연결이 해제됩니다. 쿼리 로깅 구성을 프로그래밍 방식으로 연결 해제할 수도 있습니다. 자세한 내용은 disassociate-resolver-query-log-config 섹션을 참조하세요.
6. 쿼리 로깅이 중지된 후 필드에 선택적으로 **`delete`**을 입력하고 삭제(Delete)를 선택하여 쿼리 로깅 구성을 삭제할 수 있습니다. 그러나 `AWSServiceRoleForRoute53Resolver`에서 사용하는 리소스를 삭제하는 데는 이 절차가 필요하지 않습니다.

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면 다음을 수행하세요.

IAM 콘솔, AWS CLI또는 AWS API를 사용하여 `AWSServiceRoleForRoute53Resolver` 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제 섹션을 참조하십시오.

Resolver 서비스 연결 역할을 지원하는 리전

Resolver에서는 서비스가 제공되는 모든 리전에서 서비스 연결 역할을 사용하도록 지원하지 않습니다. 다음 리전에서 `AWSServiceRoleForRoute53Resolver` 역할을 사용할 수 있습니다.

리전 이름	리전 자격 증명	Resolver의 지원
미국 동부(버지니아 북부)	us-east-1	예
미국 동부(오하이오)	us-east-2	예
미국 서부(캘리포니아 북부)	us-west-1	예
미국 서부(오리건)	us-west-2	예
아시아 태평양(뭄바이)	ap-south-1	예
아시아 태평양(오사카)	ap-northeast-3	예
아시아 태평양(서울)	ap-northeast-2	예
아시아 태평양(싱가포르)	ap-southeast-1	예
아시아 태평양(시드니)	ap-southeast-2	예
아시아 태평양(도쿄)	ap-northeast-1	예
캐나다(중부)	ca-central-1	예
유럽(프랑크푸르트)	eu-central-1	예
유럽(아일랜드)	eu-west-1	예
유럽(런던)	eu-west-2	예
유럽(파리)	eu-west-3	예
남아메리카(상파울루)	sa-east-1	예
중국(베이징)	cn-north-1	예
중국(닝샤)	cn-northwest-1	예

리전 이름	리전 자격 증명	Resolver의 지원
AWS GovCloud (US)	us-gov-east-1	예
AWS GovCloud (US)	us-gov-west-1	예

AWS Amazon Route 53에 대한 관리형 정책

AWS 관리형 정책은에서 생성하고 관리하는 독립 실행형 정책입니다 AWS. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반적인 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에 정의된 권한은 변경할 수 없습니다. 가 AWS 관리형 정책에 정의된 권한을 AWS 업데이트하면 정책이 연결된 모든 보안 주체 자격 증명(사용자, 그룹 및 역할)에 영향을 미칩니다. AWS 는 새 AWS 서비스 가 시작되거나 기존 서비스에 새 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AmazonRoute53FullAccess

`AmazonRoute53FullAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책을 통해 도메인 등록 및 상태 확인을 포함하여 Route 53 리소스에 대한 모든 액세스 권한을 부여하지만 Resolver는 제외합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `route53:*` - 다음을 제외한 모든 Route 53 작업을 수행할 수 있게 해줍니다.
  - 별칭 대상(Alias Target) 값이 CloudFront 배포, Elastic Load Balancing 로드 밸런서, Elastic Beanstalk 환경 또는 Amazon S3 버킷인 별칭 레코드를 생성 및 업데이트합니다. (이 권한으로 [Alias Target] 값이 동일한 호스팅 영역의 다른 레코드가 되는 별칭 레코드를 생성할 수 있습니다.)
  - 프라이빗 호스팅 영역 작업

  - 도메인 작업
  - CloudWatch 경보를 생성하고, 삭제하고, 볼 수 있게 해줍니다.
  - Route 53 콘솔에서 CloudWatch 지표을 렌더링합니다.
- `route53domains:*` - 도메인에 대한 작업을 할 수 있게 해줍니다.
- `cloudfront:ListDistributions` - 별칭 대상(Alias Target)의 값이 CloudFront 배포인 별칭 레코드를 생성 및 업데이트할 수 있게 해줍니다.

  Route 53 콘솔을 사용하지 않는 경우에는 이 권한이 필요하지 않습니다. Route 53는 콘솔에 표시할 배포 목록을 가져오는 데만 이 권한을 사용합니다.
- `elasticloadbalancing:DescribeLoadBalancers` - 별칭 대상(Alias Target)의 값이 Elastic Load Balancing 로드 밸런서인 별칭 레코드를 생성 및 업데이트할 수 있게 해줍니다.

  Route 53 콘솔을 사용하지 않는 경우에는 이러한 권한이 필요하지 않습니다. Route 53는 콘솔에 표시할 로드 밸런서 목록을 가져오는 데만 이 권한을 사용합니다.
- `elasticbeanstalk:DescribeEnvironments` - 별칭 대상(Alias Target)의 값이 Elastic Beanstalk 환경인 별칭 레코드를 생성 및 업데이트할 수 있게 해줍니다.

  Route 53 콘솔을 사용하지 않는 경우에는 이러한 권한이 필요하지 않습니다. Route 53는 콘솔에 표시할 환경 목록을 가져오는 데만 이 권한을 사용합니다.
- `s3:ListBucket`, `s3:GetBucketLocation` 및 `s3:GetBucketWebsite` - 별칭 대상(Alias Target)의 값이 Amazon S3 버킷인 별칭 레코드를 생성 및 업데이트할 수 있게 해줍니다. (버킷이 웹 사이트 엔드포인트로 구성되어 있는 경우에만 Amazon S3 버킷의 별칭을 생성할 수 있습니다. `s3:GetBucketWebsite`는 필요한 구성 정보를 가져옵니다.)

  Route 53 콘솔을 사용하지 않는 경우에는 이러한 권한이 필요하지 않습니다. Route 53는 콘솔에 표시할 버킷 목록을 가져오는 데만 이 권한을 사용합니다.
- `ec2:DescribeVpcs` - VPC 목록을 표시할 수 있게 해줍니다.
- `ec2:DescribeVpcEndpoints` – VPC 엔드포인트 목록을 표시할 수 있게 해줍니다.
- `ec2:DescribeRegions` - 가용 영역 목록을 표시할 수 있게 해줍니다.
- `sns:ListTopics`, `sns:ListSubscriptionsByTopic`, `cloudwatch:DescribeAlarms` – CloudWatch 경보를 생성하고, 삭제하고, 볼 수 있게 해줍니다.
- `cloudwatch:GetMetricStatistics` - CloudWatch 지표 상태 확인을 생성할 수 있게 해줍니다.

  Route 53 콘솔을 사용하지 않는 경우에는 이러한 권한이 필요하지 않습니다. Route 53는 콘솔에 표시할 통계를 가져오는 데만 이 권한을 사용합니다.

- `apigateway:GET` - 별칭 대상(Alias Target)의 값이 Amazon API Gateway API인 별칭 레코드를 생성 및 업데이트할 수 있게 해줍니다.

  Route 53 콘솔을 사용하지 않는 경우에는 이 권한이 필요하지 않습니다. Route 53는 콘솔에 표시할 API 목록을 가져오는 데만 이 권한을 사용합니다.

권한에 대한 자세한 내용은 Amazon Route 53 API 권한: 작업, 리소스 및 조건 참조 섹션을 참조하세요.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:*",
                "route53domains:*",
                "cloudfront:ListDistributions",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticbeanstalk:DescribeEnvironments",
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:GetBucketWebsite",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeRegions",
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:GetMetricStatistics"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "apigateway:GET",
            "Resource": "arn:aws:apigateway:*::/domainnames"
        }
    ]
}
```

AWS 관리형 정책: AmazonRoute53ReadOnlyAccess

`AmazonRoute53ReadOnlyAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책을 통해 도메인 등록 및 상태 확인을 포함하여 Route 53 리소스에 대한 읽기 전용 액세스 권한을 부여하지만 Resolver는 제외합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `route53:Get*` - Route 53 리소스를 가져옵니다.
- `route53:List*` - Route 53 리소스를 나열합니다.
- `route53:TestDNSAnswer` - Route 53가 DNS 요청에 응답하여 반환하는 값을 가져옵니다.

권한에 대한 자세한 내용은 Amazon Route 53 API 권한: 작업, 리소스 및 조건 참조 섹션을 참조하세요.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:Get*",
                "route53:List*",
                "route53:TestDNSAnswer"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS 관리형 정책: AmazonRoute53DomainsFullAccess

`AmazonRoute53DomainsFullAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 Route 53 도메인 등록 리소스에 대한 모든 액세스 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `route53:CreateHostedZone` - Route 53 호스팅 영역을 생성할 수 있게 해줍니다.
- `route53domains:*` - 도메인 이름을 등록하고 관련 작업을 수행할 수 있게 해줍니다.

권한에 대한 자세한 내용은 Amazon Route 53 API 권한: 작업, 리소스 및 조건 참조 섹션을 참조하세요.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53domains:*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS 관리형 정책: AmazonRoute53DomainsReadOnlyAccess

`AmazonRoute53DomainsReadOnlyAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 Route 53 도메인 등록 리소스에 대한 읽기 전용 액세스 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `route53domains:Get*` - Route 53에서 도메인 목록을 검색할 수 있게 해줍니다.
- `route53domains:List*` - Route 53 도메인 목록을 표시할 수 있게 해줍니다.

권한에 대한 자세한 내용은 Amazon Route 53 API 권한: 작업, 리소스 및 조건 참조 섹션을 참조하세요.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53domains:Get*",
                "route53domains:List*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS 관리형 정책: AmazonRoute53ResolverFullAccess

`AmazonRoute53ResolverFullAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 Route 53 Resolver에 대한 모든 액세스 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `route53resolver:*` - Route 53 콘솔에서 확인자 리소스를 만들고 관리할 수 있게 해줍니다.
- `ec2:DescribeSubnets` - Amazon VPC 서브넷을 나열할 수 있게 해줍니다.
- `ec2:CreateNetworkInterface`, `ec2:DeleteNetworkInterface`, 및 `ec2:ModifyNetworkInterfaceAttribute` - 네트워크 인터페이스를 생성, 수정 및 삭제할 수 있게 해줍니다.
- `ec2:DescribeNetworkInterfaces` - 네트워크 인터페이스 목록을 표시할 수 있게 해줍니다.
- `ec2:DescribeSecurityGroups` - 모든 보안 그룹의 목록을 표시할 수 있게 해줍니다.
- `ec2:DescribeVpcs` - VPC 목록을 표시할 수 있게 해줍니다.
- `ec2:DescribeAvailabilityZones` - 사용 가능한 영역을 나열할 수 있게 해줍니다.

권한에 대한 자세한 내용은 Amazon Route 53 API 권한: 작업, 리소스 및 조건 참조 섹션을 참조하세요.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ResolverFullAccess",
            "Effect": "Allow",
            "Action": [
                "route53resolver:*",
                "ec2:DescribeSubnets",
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs",
                "ec2:DescribeAvailabilityZones"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS 관리형 정책: AmazonRoute53ResolverReadOnlyAccess

`AmazonRoute53ResolverReadOnlyAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 Route 53 Resolver 에 대한 읽기 전용 액세스 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `route53resolver:Get*` - Resolver 리소스를 가져옵니다.
- `route53resolver:List*` - Resolver 리소스 목록을 표시할 수 있게 해줍니다.
- `ec2:DescribeNetworkInterfaces` - 네트워크 인터페이스 목록을 표시할 수 있게 해줍니다.
- `ec2:DescribeSecurityGroups` - 모든 보안 그룹의 목록을 표시할 수 있게 해줍니다.

권한에 대한 자세한 내용은 Amazon Route 53 API 권한: 작업, 리소스 및 조건 참조 섹션을 참조하세요.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ResolverReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "route53resolver:Get*",
                "route53resolver:List*",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS 관리형 정책: Route53ResolverServiceRolePolicy

`Route53ResolverServiceRolePolicy`를 IAM 엔티티에 연결할 수 없습니다. 이 정책은 Resolver에서 사용하거나 관리하는 AWS 서비스 및 리소스에 Route 53 Resolver가 액세스할 수 있는 서비스 연결 역할에 적용됩니다. 자세한 내용은 Amazon Route 53 Resolver에 서비스 연결 역할 사용 단원을 참조하십시오.

AWS 관리형 정책: AmazonRoute53ProfilesFullAccess

`AmazonRoute53ProfilesReadOnlyAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 Amazon Route 53 Profile 리소스에 대한 전체 액세스 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `route53profiles` - Route 53 콘솔에서 Profile 리소스를 만들고 관리할 수 있게 해줍니다.
- `ec2` - 보안 주체가 VPC에 대한 정보를 가져오도록 허용합니다.

권한에 대한 자세한 내용은 Amazon Route 53 API 권한: 작업, 리소스 및 조건 참조 섹션을 참조하세요.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ProfilesFullAccess",
            "Effect": "Allow",
            "Action": [
                "route53profiles:AssociateProfile",
                "route53profiles:AssociateResourceToProfile",
                "route53profiles:CreateProfile",
                "route53profiles:DeleteProfile",
                "route53profiles:DisassociateProfile",
                "route53profiles:DisassociateResourceFromProfile",
                "route53profiles:UpdateProfileResourceAssociation",
                "route53profiles:GetProfile",
                "route53profiles:GetProfileAssociation",
                "route53profiles:GetProfileResourceAssociation",
                "route53profiles:GetProfilePolicy",
                "route53profiles:ListProfileAssociations",
                "route53profiles:ListProfileResourceAssociations",
                "route53profiles:ListProfiles",
                "route53profiles:PutProfilePolicy",
                "route53profiles:ListTagsForResource",
                "route53profiles:TagResource",
                "route53profiles:UntagResource",
                "route53resolver:GetFirewallConfig",
                "route53resolver:GetFirewallRuleGroup",
                "route53resolver:GetResolverConfig",
                "route53resolver:GetResolverDnssecConfig",
                "route53resolver:GetResolverQueryLogConfig",
                "route53resolver:GetResolverRule",
                "ec2:DescribeVpcs",
                "route53:GetHostedZone"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS 관리형 정책: AmazonRoute53ProfilesReadOnlyAccess

`AmazonRoute53ProfilesReadOnlyAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 Amazon Route 53 Profile 리소스에 대한 읽기 전용 액세스 권한을 부여합니다.

권한 세부 정보

권한에 대한 자세한 내용은 Amazon Route 53 API 권한: 작업, 리소스 및 조건 참조 섹션을 참조하세요.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonRoute53ProfilesReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "route53profiles:GetProfile",
                "route53profiles:GetProfileAssociation",
                "route53profiles:GetProfileResourceAssociation",
                "route53profiles:GetProfilePolicy",
                "route53profiles:ListProfileAssociations",
                "route53profiles:ListProfileResourceAssociations",
                "route53profiles:ListProfiles",
                "route53profiles:ListTagsForResource",
                "route53resolver:GetFirewallConfig",
                "route53resolver:GetResolverConfig",
                "route53resolver:GetResolverDnssecConfig",
                "route53resolver:GetResolverQueryLogConfig"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS 관리형 정책에 대한 Route 53 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 Route 53의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 Route 53 문서 기록 페이지(Document history page)에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
AmazonRoute53ProfilesFullAccess - 정책 업데이트	`GetProfilePolicy` 및 `PutProfilePolicy` 에 대한 권한을 추가합니다. 이는 권한 전용 IAM 작업입니다. IAM 보안 주체에게 이러한 권한이 부여되지 않은 경우 AWS RAM 서비스를 사용하여 프로필을 공유하려고 할 때 오류가 발생합니다.	2024년 8월 27일
AmazonRoute53ProfilesReadOnlyAccess - 정책 업데이트	`GetProfilePolicy` 에 대한 권한을 추가합니다. 권한 전용 IAM 작업입니다. IAM 보안 주체에게이 권한이 부여되지 않은 경우 AWS RAM 서비스를 사용하여 프로파일의 정책에 액세스하려고 시도하는 중 오류가 발생합니다.	2024년 8월 27일
AmazonRoute53ResolverFullAccess - 정책 업데이트	정책을 고유하게 식별하는 문 ID(Sid)가 추가되었습니다.	2024년 8월 5일
AmazonRoute53ResolverReadOnlyAccess - 정책 업데이트	정책을 고유하게 식별하는 문 ID(Sid)가 추가되었습니다.	2024년 8월 5일
AmazonRoute53ProfilesFullAccess - 새 정책	Amazon Route 53는 Amazon Route 53 Profile 리소스에 대한 전체 액세스를 허용하는 새 정책을 추가했습니다.	2024년 4월 22일
AmazonRoute53ProfilesReadOnlyAccess - 새 정책	Amazon Route 53는 Amazon Route 53 Profile 리소스에 대한 읽기 전용 액세스를 허용하는 새 정책을 추가했습니다.	2024년 4월 22일

변경 사항	설명	날짜
Route53ResolverServiceRolePolicy - 새 정책	Amazon Route 53는 Route 53 Resolver가 Resolver에서 사용하거나 관리하는 AWS 서비스 및 리소스에 액세스할 수 있도록 허용하는 서비스 연결 역할에 연결된 새 정책을 추가했습니다.	2021년 7월 14일
AmazonRoute53ResolverReadOnlyAccess - 새 정책	Amazon Route 53는 Route 53 Resolver 리소스에 대한 읽기 전용 액세스를 허용하는 새 정책을 추가했습니다.	2021년 7월 14일
AmazonRoute53ResolverFullAccess - 새 정책	Amazon Route 53는 Route 53 Resolver 리소스에 대한 전체 액세스를 허용하는 새 정책을 추가했습니다.	2021년 7월 14일
AmazonRoute53DomainsReadOnlyAccess - 새 정책	Amazon Route 53는 Route 53 도메인 리소스에 대한 읽기 전용 액세스를 허용하는 새 정책을 추가했습니다.	2021년 7월 14일
AmazonRoute53DomainsFullAccess - 새 정책	Amazon Route 53는 Route 53 도메인 리소스에 대한 전체 액세스를 허용하는 새 정책을 추가했습니다.	2021년 7월 14일
AmazonRoute53ReadOnlyAccess - 새 정책	Amazon Route 53는 Route 53 리소스에 대한 읽기 전용 액세스를 허용하는 새 정책을 추가했습니다.	2021년 7월 14일

변경 사항	설명	날짜
AmazonRoute53FullAccess - 새 정책	Amazon Route 53는 Route 53 리소스에 대한 전체 액세스를 허용하는 새 정책을 추가했습니다.	2021년 7월 14일
Route 53 변경 내용 추적 시작	Route 53는 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2021년 7월 14일

IAM 정책 조건을 사용하여 세분화된 액세스 제어 구현

Route 53에서는 IAM 정책을 사용해 권한을 부여할 때 조건을 지정할 수 있습니다(액세스 제어 참조). 예를 들어, 다음을 수행할 수 있습니다.

- 단일 리소스 레코드 세트에 대한 액세스를 허용하는 권한을 부여합니다.
- 사용자가 호스팅 영역에서 특정 DNS 레코드 유형(예: A 레코드 및 AAAA 레코드)의 모든 리소스 레코드 세트에 액세스할 수 있도록 권한을 부여합니다.
- 사용자가 이름에 특정 문자열이 포함된 리소스 레코드 세트에 액세스할 수 있도록 권한을 부여합니다.
- 사용자가 Route 53 콘솔을 이용하거나 ChangeResourceRecordSets API를 사용할 때 `CREATE | UPSERT | DELETE` 작업의 하위 집합만 수행할 수 있도록 권한을 부여합니다.
- 사용자가 특정 VPC에서 프라이빗 호스팅 영역을 연결하거나 분리할 수 있는 권한을 부여합니다.
- 사용자가 특정 VPC와 연결된 호스팅 영역을 나열할 수 있는 권한을 부여합니다.
- 사용자가 새 프라이빗 호스팅 영역을 생성하고 이를 특정 VPC에 연결할 수 있는 권한을 부여합니다.
- 사용자가 VPC 연결 권한을 생성하거나 삭제할 수 있는 권한을 부여합니다.

세분화된 권한을 무엇이든 조합하여 권한을 생성할 수도 있습니다.

Route 53 조건 키 값 정규화

정책 조건에 입력하는 값은 다음과 같이 형식을 지정하거나 정규화해야 합니다.

`route53:ChangeResourceRecordSetsNormalizedRecordNames`의 경우:

- 모든 문자는 소문자여야 합니다.
- DNS 이름 뒤에는 점이 없어야 합니다.
- a~z, 0~9, -(하이픈), _(밑줄), .(마침표, 레이블 구분 기호) 이외의 문자는 \three-digit 8진수 코드 형태로 이스케이프 코드를 사용해야 합니다. 예를 들어 `\052` 는 * 문자의 8진수 코드입니다.

`route53:ChangeResourceRecordSetsActions`의 경우, 값은 다음 중 하나일 수 있으며 대문자여야 합니다.

- CREATE
- UPSERT
- DELETE

`route53:ChangeResourceRecordSetsRecordTypes`의 경우

- 값은 대문자여야 하며 Route 53에서 지원하는 모든 DNS 레코드 유형일 수 있습니다. 자세한 내용은 지원되는 DNS 레코드 유형 단원을 참조하십시오.

`route53:VPCs`의 경우:

- 값의 형식은 `VPCId=<vpc-id>,VPCRegion=<region>`이어야 합니다.
- `<vpc-id>` 및 `<region>` 값은 소문자(예: `VPCId=vpc-123abc, VPCRegion=us-east-1`)여야합니다.
- 컨텍스트 키와 값은 대/소문자를 구분합니다.

> **Important**
>
> 원하는 대로 작업을 허용하거나 제한할 권한을 얻으려면 다음 규칙을 따라야 합니다. `VPCId` 및 `VPCRegion` 요소만이 조건 키에서 수락되며 AWS 계정,와 같은 다른 AWS 리소스는 지원되지 않습니다.

정책이 예상한 대로 권한을 부여하거나 제한하는지 확인하려면 IAM 사용 설명서의 Access Analyzer나 정책 시뮬레이터를 사용하면 됩니다. Route 53 작업을 수행하는 테스트 사용자 또는 역할에 IAM 정책을 적용하여 권한을 검증할 수도 있습니다.

조건 지정: 조건 키 사용

AWS 는 액세스 제어를 위해 IAM을 지원하는 모든 AWS 서비스에 대해 미리 정의된 조건 키(AWS전체 조건 키) 세트를 제공합니다. 예를 들어 `aws:SourceIp` 조건 키를 사용하여 요청자의 IP 주소를 확인한 후 작업을 수행하도록 허용할 수 있습니다. AWS차원 키에 대한 정보와 목록은 IAM 사용 설명서의 사용 가능한 조건 키를 참조하세요.

> **Note**
>
> Route 53는 태그 기반 조건 키를 지원하지 않습니다.

다음 표는 Route 53에 적용되는 Route 53 서비스별 조건 키를 보여줍니다.

Route 53 조건 키	API 작업	값 유형	설명
`route53:ChangeResourceRecordSetsNormalizedRecordNames`	ChangeResourceRecordSets	다중 값	ChangeResourceRecordSets 요청의 DNS 레코드 이름 목록을 나타냅니다. 예상되는 동작을 가져오려면 다음과 같이 IAM 정책의 DNS 이름을 정규화해야 합니다. • 모든 문자는 소문자여야 합니다. • DNS 이름 뒤에는 점이 없어야 합니다. • a~z, 0~9, -(하이픈), _(밑줄), .(마침표, 레이블 구분 기호) 이외의 문자는 \three-digit 8진수 코드 형태로 이스케이프 코드를 사용해야 합니다.
`route53:ChangeResourceRecordSetsRecordTypes`	ChangeResourceRecordSets	다중 값	`ChangeResourceRecordSets` 요청의 DNS 레코드 유형 목록을 나타냅니다. `ChangeResourceRecordSetsRecordTypes` 은 Route 53에서 지원되는 모든 DNS 레코드 유형이 될 수 있습니다. 자세한 내용은 지원되는 DNS 레코드 유형 단원을 참조하

Route 53 조건 키	API 작업	값 유형	설명
			십시오. 정책에는 모두 대문자로 입력해야 합니다.
route53:ChangeResourceRecordSetsActions	ChangeResourceRecordSets	다중 값	ChangeResourceRecordSets 요청에서 작업 목록을 나타냅니다. ChangeResourceRecordSetsActions 값은 다음 중 하나일 수 있습니다(대문자여야 함). • CREATE • UPSERT • DELETE

Route 53 조건 키	API 작업	값 유형	설명
route53:VPCs	AssociateVPCWithHostedZone DisassociateVPCFromHostedZone ListHostedZonesByVPC CreateHostedZone CreateVPCAssociationAuthorization DeleteVPCAssociationAuthorization	다중 값	AssociateVPCWithHostedZone , DisassociateVPCFromHostedZone , ListHostedZonesByVPC , CreateHostedZone , CreateVPCAssociationAuthorization , DeleteVPCAssociationAuthorization 요청에서 "VPCId=<vpc-id>,VPCRegion=<region> 형식의 VPC 목록을 나타냅니다.

정책 예: 조건을 사용하여 세분화된 액세스 구현

이 단원의 각 예제에서는 Effect 절을 Allow로 설정하고 허용할 작업, 리소스, 파라미터만 지정합니다. 액세스는 IAM 정책에 명시적으로 나열된 항목에만 허용됩니다.

경우에 따라, Effect 절을 Deny로 설정하고 정책의 모든 논리를 반전시켜 거부 기반 정책이 되도록 이러한 정책을 다시 작성할 수도 있습니다. 하지만 허용 기반 정책에 비해 올바르게 작성하기가 어려우므로 거부 기반 정책을 사용하지 않는 것이 좋습니다. 특히 Route 53의 경우 텍스트 정규화가 필요하기 때문에 사용하지 않는 것이 좋습니다.

특정 이름을 사용하는 DNS 레코드에 대한 액세스를 제한하는 권한 부여

다음 권한 정책은 example.com 및 marketing.example.com의 호스팅 영역 Z12345에서 ChangeResourceRecordSets 작업을 허용하는 권한을 부여합니다. route53:ChangeResourceRecordSetsNormalizedRecordNames 조건 키를 사용해 지정된 이름과 일치하는 레코드로만 사용자 작업을 제한합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "Condition": {
                "ForAllValues:StringEquals":{
                    "route53:ChangeResourceRecordSetsNormalizedRecordNames":
 ["example.com", "marketing.example.com"]
                }
            }
          }
        ]
}
```

ForAllValues:StringEquals는 다중 값 키에 적용되는 IAM 조건 연산자입니다. 위 정책의 조건은 ChangeResourceRecordSets의 모든 변경 사항에 example.com라는 DNS 이름이 있는 경우에만 작업을 허용합니다. 자세한 내용을 알아보려면 IAM 사용 설명서에서 IAM 조건 연산자 및 다수의 키 또는 값을 사용하는 IAM 조건 단원을 참조하세요.

특정 접미사가 있는 이름과 일치하는 권한을 구현하기 위해 StringLike 또는 StringNotLike 조건 연산자가 포함된 정책에 IAM 와일드카드(*)를 사용할 수 있습니다. 다음 정책은 ChangeResourceRecordSets 작업의 모든 변경 사항에 “-beta.example.com”으로 끝나는 DNS 이름이 있을 때 작업을 허용합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
```

```
            "Condition": {
                "ForAllValues:StringLike":{
                     "route53:ChangeResourceRecordSetsNormalizedRecordNames": ["*-
beta.example.com"]
                }
            }
          }
        ]
}
```

> **Note**
>
> IAM 와일드카드는 도메인 이름 와일드카드와 다릅니다. 와일드카드를 도메인 이름에 사용하는 방법은 다음 예를 참조하세요.

와일드카드가 포함된 도메인 이름과 일치하는 DNS 레코드에 대한 액세스를 제한하는 권한 부여

다음 권한 정책은 example.com의 호스팅 영역 Z12345에서 ChangeResourceRecordSets 작업을 허용하는 권한을 부여합니다. route53:ChangeResourceRecordSetsNormalizedRecordNames 조건 키를 사용해 *.example.com과 일치하는 레코드로만 사용자 작업을 제한합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "Condition": {
                "ForAllValues:StringEquals":{
                     "route53:ChangeResourceRecordSetsNormalizedRecordNames": ["\
\052.example.com"]
                }
            }
          }
        ]
}
```

\052 는 DNS 이름의 * 문자에 대한 8진수 코드이고, \052의 \는 JSON 구문을 따르기 위해 \\로 이스케이프되었습니다.

특정 DNS 레코드에 대한 액세스를 제한하는 권한 부여

다음 권한 정책은 example.com의 호스팅 영역 Z12345에서 ChangeResourceRecordSets 작업을 허용하는 권한을 부여합니다. 세 가지 조건 키의 조합을 사용해 사용자 작업을 제한하여 특정 DNS 이름 및 유형의 DNS 레코드만 생성하거나 편집할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "Condition": {
                "ForAllValues:StringEquals":{
                     "route53:ChangeResourceRecordSetsNormalizedRecordNames":
 ["example.com"],
                     "route53:ChangeResourceRecordSetsRecordTypes": ["MX"],
                     "route53:ChangeResourceRecordSetsActions": ["CREATE", "UPSERT"]
                }
            }
          }
        ]
}
```

지정된 유형의 DNS 레코드만 생성 및 편집하도록 액세스를 제한하는 권한 부여

다음 권한 정책은 example.com의 호스팅 영역 Z12345에서 ChangeResourceRecordSets 작업을 허용하는 권한을 부여합니다. route53:ChangeResourceRecordSetsRecordTypes 조건 키를 사용해 특정 유형(A 및 AAAA)과 일치하는 레코드로만 사용자 작업을 제한합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "route53:ChangeResourceRecordSets",
            "Resource": "arn:aws:route53:::hostedzone/Z11111112222222333333",
            "Condition": {
                "ForAllValues:StringEquals":{
                     "route53:ChangeResourceRecordSetsRecordTypes": ["A", "AAAA"]
                }
```

```
            }
          }
        ]
}
```

IAM 보안 주체가 작동할 수 있는 VPC를 지정하는 권한을 부여합니다.

다음 권한 정책은 vpc-id로 지정된 VPC에 `AssociateVPCWithHostedZone`, `DisassociateVPCFromHostedZone`, `ListHostedZonesByVPC`, `CreateHostedZone`, `CreateVPCAssociationAuthorization`, `DeleteVPCAssociationAuthorization` 작업을 허용하는 권한을 부여합니다.

> **Important**
>
> 조건 값의 형식은 `VPCId=<vpc-id>,VPCRegion=<region>`이어야 합니다. 조건 값에 VPC ARN을 지정하면 조건 키가 적용되지 않습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "route53:*"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "ForAllValues:StringLike": {
                    "route53:VPCs": [
                        "VPCId=<vpc-id>,VPCRegion=<region>"
                    ]
                }
            }
        },
        {
            "Sid": "Statement2",
            "Effect": "Allow",
            "Action": "ec2:DescribeVpcs",
```

```
            "Resource": "*"
        }
    ]
}
```

Amazon Route 53 API 권한: 작업, 리소스 및 조건 참조

액세스 제어을 설정하고 IAM 자격 증명에 연결할 수 있는 권한 정책(자격 증명 기반 정책)을 작성할 때 서비스 승인 참조에서 Route 53에 사용되는 작업, 리소스, 조건 키, Route 53 Domains에 사용되는 작업, 리소스, 조건 키, Route 53 Resolver에 사용되는 작업, 리소스, 조건 키, DNS 설정을 VPC와 공유할 수 있게 해주는 Amazon Route 53 Profiles에 사용되는 작업, 리소스, 조건 키 목록을 사용할 수 있습니다. 페이지에는 각 Amazon Route 53 API 작업, 액세스 권한을 부여해야 하는 작업, 액세스 권한을 부여해야 하는 AWS 리소스가 포함됩니다. 정책의 `Action`필드에서 작업을 지정하고, 정책의 `Resource`필드에서 리소스 값을 지정합니다.

Route 53 정책에서 AWS전체 조건 키를 사용하여 조건을 표시할 수 있습니다. AWS전체 키의 전체 목록은 IAM 사용 설명서의 사용 가능한 키를 참조하세요.

> **Note**
>
> 액세스 권한을 부여할 때 호스팅 영역과 Amazon VPC가 동일한 파티션에 속해 있어야 합니다. 파티션은의 그룹입니다 AWS 리전. 각 파티션 AWS 계정 은 하나의 파티션으로 범위가 지정됩니다.
> 지원되는 파티션은 다음과 같습니다.
>
> - `aws` - AWS 리전
> - `aws-cn` - 중국 리전
> - `aws-us-gov` - AWS GovCloud (US) Region
>
> 자세한 내용은 AWS 일반 참조에서 액세스 관리를 참조하세요.

> **Note**
>
> 작업을 지정하려면 적절한 접두사(`route53`, `route53domains` 또는 `route53resolver`) 다음에 API 작업 이름을 사용합니다. 예를 들면 다음과 같습니다.
>
> - `route53:CreateHostedZone`

- route53domains:RegisterDomain
- route53resolver:CreateResolverEndpoint

Amazon Route 53의 로깅 및 모니터링

Amazon Route 53에서는 DNS 쿼리 로깅을 제공하고 상태 확인을 사용하여 리소스를 모니터링하는 기능을 제공합니다. 또한 Route 53는 다른 AWS 서비스와 통합되어 추가 로깅 및 모니터링을 제공합니다.

DNS 쿼리 로깅

요청된 도메인이나 하위 도메인, 요청의 날짜와 시간, DNS 레코드 유형(A 또는 AAAA) 등 Route 53가 수신하는 쿼리에 대한 정보를 로깅하도록 Route 53를 구성할 수 있습니다.

자세한 내용은 퍼블릭 DNS 쿼리 로깅 단원을 참조하십시오.

AWS CloudTrail 를 사용하여 콘솔 및 프로그래밍 작업 로깅

CloudTrail은 사용자, 역할 또는 AWS 서비스가 수행한 Route 53 작업의 레코드를 제공합니다. CloudTrail에서 수집한 정보를 사용하여 수행된 요청, 요청이 시작된 IP 주소, 요청한 사람, 요청한 시간 및 추가 세부 정보를 추적할 수 있습니다. 자세한 내용은 를 사용하여 Amazon Route 53 API 호출 로깅 AWS CloudTrail 단원을 참조하십시오.

도메인 등록 모니터링

Route 53 대시보드는 도메인 이전 및 만료 날짜가 다가오는 도메인의 상태 등 도메인 등록 상태에 대한 세부 정보를 제공합니다.

자세한 내용은 도메인 등록 모니터링 단원을 참조하십시오.

Route 53 상태 확인 및 Amazon CloudWatch를 사용하여 리소스 모니터링

CloudWatch를 사용하여 원시 데이터를 수집하고 읽기 가능하고 실시간에 가까운 지표로 처리하는 Route 53 상태 확인을 만들어 리소스를 모니터링할 수 있습니다.

자세한 내용은 Amazon Route 53 상태 확인 및 Amazon CloudWatch를 사용하여 리소스 모니터링 단원을 참조하십시오.

Amazon CloudWatch를 사용하여 Route 53 Resolver 엔드포인트 모니터링

CloudWatch를 사용하여 Resolver 엔드포인트에 의해 전달되는 DNS 쿼리 수를 모니터링할 수 있습니다.

자세한 내용은 Amazon CloudWatch를 사용하여 Route 53 Resolver 엔드포인트 모니터링 단원을 참조하십시오.

사용 AWS Trusted Advisor

Trusted Advisor 는 AWS 고객 응대에서 학습한 모범 사례를 활용합니다.는 AWS 환경을 Trusted Advisor 검사한 다음 비용을 절감하거나, 시스템 가용성 및 성능을 개선하거나, 보안 격차를 좁힐 기회가 있을 때 권장 사항을 제시합니다. 모든 AWS 고객은 다섯 가지 Trusted Advisor 검사에 액세스할 수 있습니다. 비즈니스 또는 엔터프라이즈 지원 플랜을 보유한 고객은 모든 Trusted Advisor 검사를 볼 수 있습니다.

자세한 내용은 Trusted Advisor 단원을 참조하십시오.

Amazon Route 53의 규정 준수 확인

타사 감사자는 여러 규정 준수 프로그램의 일환으로 Amazon Route 53의 보안 및 AWS 규정 준수를 평가합니다. 여기에는 SOC, PCI, FedRAMP, HIPAA 등이 포함됩니다.

특정 규정 준수 프로그램 범위의 AWS 서비스 목록은 AWS 규정 준수 프로그램 제공 범위 내 서비스를 참조하세요. 일반 정보는 AWS 규정 준수 프로그램을 참조하세요.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 AWS 아티팩트에서 보고서 다운로드를 참조하세요.

Route 53 사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률 및 규정에 따라 결정됩니다. Route 53 사용 시 HIPAA, PCI 또는 FedRAMP와 같은 표준을 준수해야 하는 경우는 다음과 같은 도움이 되는 리소스를 AWS 제공합니다.

- 보안 및 규정 준수 빠른 시작 안내서 -이 배포 안내서에서는 아키텍처 고려 사항에 대해 설명하고 보안 및 규정 준수 중심 기준 환경을 배포하기 위한 단계를 제공합니다 AWS.
- HIPAA 보안 및 규정 준수 아키텍팅 백서 - 이 백서는 기업에서 AWS 를 사용하여 HIPAA를 준수하는 애플리케이션을 생성하는 방법을 설명합니다.
- AWS 규정 준수 리소스 -이 워크북 및 가이드 모음은 업계 및 위치에 적용될 수 있습니다.
- AWS Config -이 AWS 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub -이 AWS 서비스는 보안 업계 표준 및 모범 사례 준수를 확인하는 데 도움이 AWS 되는 내 보안 상태에 대한 포괄적인 보기를 제공합니다.

Amazon Route 53의 복원성

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 기반으로 구축됩니다. AWS 리전은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹과 연결된 물리적으로 분리되고 격리된 여러 가용 영역을 제공합니다. 가용 영역을 사용하면 중단 없이 가용 영역 간에 자동으로 장애 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 복수 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

Route 53는 기능을 제어 및 데이터 영역으로 나눕니다. Route 53 서비스는 대부분의 AWS 서비스와 같이 리소스 생성, 업데이트 및 삭제와 같은 관리 작업을 수행할 수 있는 컨트롤 플레인과 서비스의 핵심 기능을 제공하는 데이터 영역을 포함합니다. Route 53의 제어 및 데이터 영역에 관한 정보는 제어 및 데이터 영역 개념을 참조하세요.

Route 53는 주로 글로벌 서비스이지만 다음 기능은 AWS 리전을 지원합니다.

- Route 53 Resolver를 사용하여 하이브리드 구성을 설정하는 경우 선택한 AWS 리전에서 엔드포인트를 생성하고 여러 가용 영역에서 IP 주소를 지정합니다. 아웃바운드 엔드포인트의 경우 엔드포인트를 생성한 것과 동일한 리전에 규칙을 생성합니다. 자세한 내용은 Amazon Route 53 Resolver란 무엇인가요? 단원을 참조하십시오.
- Amazon EC2 인스턴스 및 Elastic Load Balancing 로드 밸런서와 같이 특정 리전에서 생성한 리소스의 상태를 확인하도록 Route 53 상태 확인을 구성할 수 있습니다.
- 엔드포인트를 모니터링하는 상태 확인을 생성할 때 필요에 따라 Route 53가 상태 확인을 수행할 리전을 지정할 수 있습니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

Amazon Route 53의 인프라 보안

관리형 서비스인 Amazon Route 53는 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스 및가 인프라를 AWS 보호하는 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하세요.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 Route 53에 액세스합니다. 고객은 다음을 지원해야 합니다.

- Transport Layer Security(TLS) TLS 1.2는 필수이며 TLS 1.3을 권장합니다.

- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군 Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 위탁자와 관련된 보안 암호 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 자격 증명을 생성하여 요청에 서명할 수 있습니다.

Route 53 Resolver DNS 방화벽에서 Security Hub로 조사 결과 전송

AWS Security Hub는에서 보안 상태를 포괄적으로 볼 수 있도록 AWS 하고 보안 업계 표준 및 모범 사례를 기준으로 환경을 확인하는 데 도움이 됩니다. Security Hub는 AWS 계정 AWS 서비스및 지원되는 타사 파트너 제품에서 보안 데이터를 수집하고 보안 추세를 분석하고 우선 순위가 가장 높은 보안 문제를 식별하는 데 도움이 됩니다.

Route 53 Resolver DNS 방화벽을 Security Hub와 통합하여 DNS 방화벽에서 Security Hub로 조사 결과를 보낼 수 있습니다. 그런 다음 Security Hub는 이러한 결과를 보안 태세 분석에 포함합니다.

목차

Security Hub에서 조사 결과가 작동하는 방식

Security Hub에서 조사 결과는 보안 검사 또는 보안 관련 탐지에 대한 관찰 가능한 레코드입니다. 일부 결과는 다른 AWS 서비스 또는 타사 파트너가 감지한 문제에서 비롯됩니다. 또한 Security Hub에는 보안 문제를 감지하고 결과를 생성하는 데 사용하는 자체 보안 제어 기능이 있습니다.

Security Hub는 이러한 모든 출처를 총망라하여 조사 결과를 관리할 도구를 제공합니다. 조사 결과 목록을 보고 필터링하며 조사 결과 세부 정보를 볼 수 있습니다. 자세한 내용은 AWS Security Hub 사용 설명서의 Security Hub에서 조사 결과 세부 정보 및 조사 결과 기록 검토를 참조하세요. 조사 결과를 자동으로 업데이트하거나 사용자 지정 작업으로 보낼 수도 있습니다. 자세한 내용은 AWS Security Hub 사용 설명서의 Security Hub 조사 결과 자동 수정 및 작업 수행을 참조하세요.

Security Hub의 모든 결과는 AWS Security Finding Format(ASFF)이라는 표준 JSON 형식을 사용합니다. ASFF에는 보안 문제의 소스, 영향을 받는 리소스 및 조사 결과의 현재 상태에 대한 세부 정보가 포

함됩니다. 자세한 내용은 AWS Security Hub 사용 설명서의 AWS 보안 조사 결과 형식(ASFF)을 참조하세요.

DNS 방화벽은 결과를 Security Hub로 AWS 서비스 보내는 중 하나입니다.

DNS 방화벽이 보내는 조사 결과 유형

DNS 방화벽에는 다음과 같은 통합이 있습니다.

- 관리형 도메인 목록: AWS 관리형 도메인 목록과 연결된 도메인에 대해에서 차단되거나 경고되는 쿼리와 관련된 보안 조사 결과입니다.
- 사용자 지정 도메인 목록: 고객의 도메인 목록과 연결된 도메인에 대해에서 차단되거나 경고되는 쿼리와 관련된 보안 조사 결과입니다.
- DNS Firewall Advanced: DNS Firewall Advanced에서 차단하거나 경고하는 쿼리와 관련된 보안 조사 결과입니다.

Security Hub는 DNS 방화벽의 결과를 AWS Security Finding Format(ASFF)으로 수집합니다. ASFF의 경우, `Types` 필드가 결과 유형을 제공합니다. DNS 방화벽의 결과는에 대해 다음 값을 가질 수 있습니다`Types`.

- `TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation`

Security Hub를 사용할 수 없는 경우 재시도

Security Hub를 사용할 수 없는 경우 DNS 방화벽은 조사 결과가 수신될 때까지 결과 전송을 다시 시도합니다.

Security Hub에서 기존 조사 결과 업데이트

DNS 방화벽은 동일한 결과가 다시 관찰되면 기존 결과를 업데이트합니다.

DNS 방화벽의 일반적인 결과

Security Hub는 AWS Security Finding Format(ASFF)에서 DNS 방화벽 결과를 수집합니다.

다음은 ASFF의 DNS 방화벽에서 얻은 일반적인 결과의 예입니다.

```
{
            "SchemaVersion": "2018-10-08",
```

```
            "Id": "00000000-0000-0000-0000-example1",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/amazon/route-53-
resolver-dns-firewall-aws-list",
            "ProductName": "Route 53 Resolver DNS Firewall - AWS List",
            "CompanyName": "Amazon",
            "Region": "us-east-1",
            "GeneratorId": "arn:aws:route53resolver:us-east-1:000000000000:firewall-
rule-group/rslvr-frg-example1",
            "AwsAccountId": "000000000000",
            "Types": [
                "TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation"
            ],
            "FirstObservedAt": "2024-12-06T19:58:49.000Z",
            "LastObservedAt": "2024-12-06T19:58:49.000Z",
            "CreatedAt": "2024-12-06T19:58:49.000Z",
            "UpdatedAt": "2024-12-06T19:58:49.000Z",
            "Severity": {
                "Label": "HIGH",
                "Normalized": 70
            },
            "Title": "DNS Firewall ALERT generated for domain example1.com. from VPC
 vpc-example1",
            "Description": "DNS Firewall ALERT",
            "ProductFields": {
                "aws/route53resolver/dnsfirewall/queryName": "example1.com.",
                "aws/route53resolver/dnsfirewall/firewallRuleGroupId": "rslvr-frg-
example1",
                "aws/route53resolver/dnsfirewall/queryType": "A",
                "aws/route53resolver/dnsfirewall/queryClass": "IN",
                "aws/route53resolver/dnsfirewall/firewallDomainListId": "rslvr-fdl-
example1",
                "aws/route53resolver/dnsfirewall/transport": "UDP",
                "aws/route53resolver/dnsfirewall/firewallRuleAction": "ALERT",
                "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
amazon/route-53-resolver-dns-firewall-aws-list/00000000-0000-0000-0000-example1",
                "aws/securityhub/ProductName": "Route 53 Resolver DNS Firewall - AWS
 List",
                "aws/securityhub/CompanyName": "Amazon"
            },
            "Resources": [
                {
                    "Type": "Other",
                    "Id": "rslvr-in-example1",
                    "Partition": "aws",
```

```
                "Region": "us-east-1",
                "Details": {
                    "Other": {
                        "ResourceType": "ResolverEndpoint",
                        "EndpointId": "rslvr-in-example1"
                    }
                }
            },
            {
                "Type": "Other",
                "Id": "rni-example1",
                "Partition": "aws",
                "Region": "us-east-1",
                "Details": {
                    "Other": {
                        "NetworkInterfaceId": "rni-example1",
                        "ResourceType": "ResolverNetworkInterface"
                    }
                }
            }
        ],
        "WorkflowState": "NEW",
        "Workflow": {
            "Status": "NEW"
        },
        "RecordState": "ACTIVE",
        "FindingProviderFields": {
            "Severity": {
                "Label": "HIGH"
            },
            "Types": [
                "TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation"
            ]
        },
        "ProcessedAt": "2024-12-11T19:33:35.494Z"
    }
```


통합 활성화 및 구성

DNS 방화벽을 Security Hub와 통합하려면 먼저 Security Hub를 활성화해야 합니다. Security Hub 활성화에 대한 자세한 내용은 AWS Security Hub 사용 설명서의 Security Hub 활성화를 참조하세요.

Security Hub로 조사 결과 전송 중지

Security Hub로 DNS 방화벽 조사 결과 전송을 중지하려면 Security Hub 콘솔 또는 Security Hub API를 사용할 수 있습니다.

지침은 AWS Security Hub 사용 설명서의 통합에서 결과 흐름 비활성화를 참조하세요.

Amazon Route 53 모니터링

모니터링은 AWS 솔루션의 신뢰성, 가용성 및 성능을 유지하는 데 중요한 부분입니다. AWS 솔루션의 모든 부분에서 모니터링 데이터를 수집해야 다중 지점 장애가 발생할 경우 더 쉽게 디버깅할 수 있습니다. 하지만 모니터링을 시작하기 전에 다음 질문에 대한 답변을 포함하는 모니터링 계획을 작성해야 합니다.

- 모니터링의 목표
- 모니터링할 리소스
- 이러한 리소스를 모니터링하는 빈도
- 사용할 모니터링 도구
- 모니터링 작업을 수행할 사람
- 문제 발생 시 알려야 할 대상

주제

퍼블릭 DNS 쿼리 로깅

다음과 같이 Route 53가 수신하는 퍼블릭 DNS 쿼리에 대한 정보를 로깅하도록 Amazon Route 53를 구성할 수 있습니다.

- 요청된 도메인 또는 하위 도메인

- 요청의 날짜 및 시간
- DNS 레코드 유형(예: A 또는 AAAA)
- DNS 쿼리에 응답한 Route 53 엣지 로케이션
- DNS 응답 코드(예: `NoError` 또는 `ServFail`)

쿼리 로깅을 구성하면 Route 53는 CloudWatch Logs에 로그를 전송합니다. CloudWatch Logs 도구를 사용하여 쿼리 로그에 액세스합니다.

쿼리 로그에는 DNS 해석기가 Route 53으로 전달하는 쿼리만 포함되어 있습니다. DNS 해석기가 쿼리에 대한 응답(예: example.com의 로드 밸런서에 대한 IP 주소)을 이미 캐시한 경우 해석기는 해당 레코드에 대한 TTL이 만료될 때까지 쿼리를 Route 53에 전달하지 않고 캐시된 응답을 계속 반환합니다.

도메인 이름(example.com) 또는 하위 도메인 이름(www.example.com)에 대해 제출된 DNS 쿼리 수, 사용자가 사용하고 있는 해석기 및 레코드에 대한 TTL에 따라 쿼리 로그에는 DNS 해석기에 제출된 수천 개의 쿼리 중 한 개의 쿼리에 대한 정보만 포함될 수 있습니다. DNS 작업 방법에 대한 자세한 내용은 웹 사이트 또는 웹 애플리케이션으로 인터넷 트래픽을 라우팅하는 방식를 참조하세요.

자세한 로깅 정보가 필요하지 않은 경우에는 Amazon CloudWatch 지표를 사용해 호스팅 영역에서 Route 53가 응답하는 DNS 쿼리의 총 수를 확인할 수 있습니다. 자세한 내용은 퍼블릭 호스팅 영역에서 DNS 쿼리 지표 보기 섹션을 참조하세요.

주제

- DNS 쿼리 로깅 구성
- Amazon CloudWatch를 사용하여 DNS 쿼리 로그에 액세스
- 로그의 보존 기간 변경 및 Amazon S3에 로그 내보내기
- 쿼리 로깅 중지
- DNS 쿼리 로그에 나타나는 값
- 쿼리 로그 예

DNS 쿼리 로깅 구성

지정된 호스팅 영역에 대한 DNS 쿼리의 로깅을 시작하려면 Amazon Route 53 콘솔에서 다음 작업을 수행합니다.

- Route 53가 로그를 게시할 CloudWatch Logs 로그 그룹을 선택하거나 새 로그 그룹을 생성합니다.

> **Note**
>
> 로그 그룹은 미국 동부(버지니아 북부) 리전에 있어야 합니다.

- Create(생성)을 선택하여 완료합니다.

> **Note**
>
> 사용자가 도메인에 대한 DNS 쿼리를 제출하는 경우 쿼리 로깅 구성을 생성한 후 몇 분 내에 로그에서 쿼리를 볼 수 있어야 합니다.

DNS 쿼리 로깅을 구성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
3. 쿼리 로깅을 구성할 호스팅 영역을 선택합니다.
4. [Hosted zone details] 창에서 [Configure query logging]을 선택합니다.
5. 기존 로그 그룹을 선택하거나 새 로그 그룹을 생성합니다.
6. 권한에 대한 알림이 표시되면(이전에 새 콘솔로 쿼리 로깅을 구성하지 않은 경우 발생) 다음 중 하나를 수행합니다.
   - 이미 10개의 리소스 정책이 있는 경우 더 이상 만들 수 없습니다. 리소스 정책 중 하나를 선택하고 편집을 선택합니다. 편집을 통해, 로그 그룹에 로그를 쓸 수 있는 권한을 Route 53에 부여할 것입니다. 저장을 선택합니다. 알림이 사라지고 다음 단계로 계속 진행할 수 있습니다.
   - 이전에 쿼리 로깅을 구성한 적이 없거나 10개의 리소스 정책을 아직 생성하지 않은 경우 CloudWatch Logs 그룹에 로그를 쓸 수 있는 권한을 Route 53에 부여해야 합니다. 권한 부여를 선택합니다. 알림이 사라지고 다음 단계로 계속 진행할 수 있습니다.
7. 권한 - 선택 사항을 선택하여 리소스 정책이 CloudWatch 로그 그룹과 일치하는지 여부와 CloudWatch에 로그를 게시할 권한이 Route 53에 있는지 여부를 보여 주는 테이블을 확인합니다.
8. 생성을 선택합니다.

Amazon CloudWatch를 사용하여 DNS 쿼리 로그에 액세스

Amazon Route 53는 CloudWatch Logs에 직접 쿼리 로그를 전송하며, 로그는 Route 53를 통해 액세스할 수 없습니다. 대신 CloudWatch Logs를 사용하여 거의 실시간으로 로그를 보고 데이터를 검색 및 필터링하며 로그를 Amazon S3에 내보냅니다.

Route 53는 지정된 호스팅 영역에 대한 DNS 쿼리에 응답하는 각 Route 53 엣지 로케이션에 대해 하나의 CloudWatch Logs 로그 스트림을 생성하고 쿼리 로그를 해당 로그 스트림으로 전송합니다. 각 로그 스트림의 이름에 대한 형식은 *hosted-zone-id*/*edge-location-ID*(예: Z1D633PJN98FT9/DFW3)입니다.

각 엣지 로케이션은 3자 코드와 임의 배정된 번호로 식별됩니다(예: DFW3). 3자 코드는 일반적으로 엣지 로케이션 부근의 공항을 나타내는 국제 항공 운송 협회 공항 코드에 상응합니다. (이러한 약어는 향후에 변경될 수 있습니다.) 엣지 로케이션의 목록은 Route 53 제품 세부 정보 페이지의 'Route 53 글로벌 네트워크'를 참조하세요.

> **Note**
>
> 위의 규칙을 따르지 않는 접두사 또는 접미사가 있을 수 있습니다. 내부 전용 속성을 인코딩합니다.

자세한 설명은 다음과 같이 해당 문서를 참조하세요.

- Amazon CloudWatch Logs 사용 설명서
- Amazon CloudWatch Logs API 참조
- AWS CLI 명령 참조의 CloudWatch Logs 섹션
- DNS 쿼리 로그에 나타나는 값

로그의 보존 기간 변경 및 Amazon S3에 로그 내보내기

기본적으로 CloudWatch Logs는 쿼리 로그를 무기한 저장합니다. CloudWatch Logs가 보존 기간보다 오래된 로그를 삭제하도록 보존 기간을 선택적으로 지정할 수 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 CloudWatch Logs에서 로그 데이터 보존 기간 변경을 참조하세요.

로그 데이터를 보존하려고 하지만 데이터 조회 및 분석에 CloudWatch Logs 도구가 필요하지 않으면 로그를 Amazon S3에 내보낼 수 있으므로 스토리지 비용을 절감할 수 있습니다. 자세한 내용은 Amazon S3에 로그 데이터 내보내기를 참조하세요.

요금에 대한 자세한 내용은 해당하는 요금 페이지를 참조하세요.

- CloudWatch 요금 페이지의 "Amazon CloudWatch Logs"
- Amazon S3 요금

> **Note**
>
> Route 53에서 DNS 쿼리 로깅 구성 시 Route 53 요금은 발생하지 않습니다.

쿼리 로깅 중지

Amazon Route 53가 CloudWatch Logs로의 쿼리 로그 전송을 중지하도록 하려면 다음 절차를 수행하여 쿼리 로깅 구성을 삭제합니다.

쿼리 로깅 구성을 삭제하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
3. 쿼리 로깅 구성을 삭제할 호스팅 영역의 이름을 선택합니다.
4. 호스팅 영역 세부 사항 창에서 쿼리 로깅 구성 삭제를 선택합니다.
5. [삭제]를 선택하여 확인합니다.

DNS 쿼리 로그에 나타나는 값

각 로그 파일에는 Amazon Route 53가 해당 엣지 로케이션의 DNS 해석기로부터 수신한 각 DNS 쿼리당 하나의 로그 항목이 포함되어 있습니다. 각 로그 항목에는 다음 값이 포함되어 있습니다.

로그 형식 버전

이 쿼리 로그의 버전 번호입니다. 필드를 로그에 추가하거나 기존 필드의 형식을 변경하는 경우 이 값이 증가합니다.

쿼리 타임스탬프

ISO 8601 형식 및 협정 세계시(UTC)로 Route 53가 요청에 응답한 날짜 및 시간입니다(예: `2017-03-16T19:20:25.177Z`).

ISO 8601 형식에 대한 자세한 내용은 Wikipedia 도움말 ISO 8601을 참조하세요. UTC에 대한 자세한 내용은 Wikipedia 도움말 협정 세계시를 참조하세요.

호스팅 영역 ID

이 로그의 모든 DNS 쿼리와 연결된 호스팅 영역의 ID입니다.

쿼리 이름

요청에서 지정된 도메인 또는 하위 도메인입니다.

쿼리 유형

요청에서 지정된 DNS 레코드 유형 또는 ANY입니다. Route 53가 지원하는 유형에 대한 자세한 내용은 지원되는 DNS 레코드 유형를 참조하세요.

응답 코드

Route 53가 DNS 쿼리에 대한 응답으로 반환한 DNS 응답 코드입니다.

계층 4 프로토콜

쿼리를 제출하는 데 사용된 프로토콜로, TCP 또는 UDP입니다.

Route 53 엣지 로케이션

쿼리에 응답한 Route 53 엣지 로케이션입니다. 각 엣지 로케이션은 3자 코드와 임의의 숫자로 식별됩니다(예: DFW3). 3자 코드는 일반적으로 엣지 로케이션 부근의 공항을 나타내는 국제 항공 운송 협회 공항 코드에 상응합니다. (이러한 약어는 향후에 변경될 수 있습니다.)

엣지 로케이션의 목록은 Route 53 제품 세부 정보 페이지의 “Route 53 글로벌 네트워크”를 참조하세요.

해석기 IP 주소

요청을 Route 53에 제출한 DNS 해석기의 IP 주소입니다.

EDNS 클라이언트 서브넷

DNS 해석기에서 사용 가능한 경우 요청이 시작된 클라이언트의 부분 IP 주소입니다.

자세한 내용은 IETF 초안인 DNS 요청의 클라이언트 서브넷을 참조하세요.

쿼리 로그 예

다음은 쿼리 로그의 예입니다(Region은 자리 표시자).

```
1.0 2017-12-13T08:16:02.130Z Z123412341234 example.com A NOERROR UDP Region 192.168.1.1
 -
1.0 2017-12-13T08:15:50.235Z Z123412341234 example.com AAAA NOERROR TCP Region
 192.168.3.1 192.168.222.0/24
1.0 2017-12-13T08:16:03.983Z Z123412341234 example.com ANY NOERROR UDP Region
 2001:db8::1234 2001:db8:abcd::/48
1.0 2017-12-13T08:15:50.342Z Z123412341234 bad.example.com A NXDOMAIN UDP Region
 192.168.3.1 192.168.111.0/24
1.0 2017-12-13T08:16:05.744Z Z123412341234 txt.example.com TXT NOERROR UDP Region
 192.168.1.2 -
```

Resolver 쿼리 로깅

다음과 같은 DNS 쿼리를 로그할 수 있습니다.

- 지정한 Amazon Virtual Private Cloud(VPC)에서 시작되는 쿼리와 해당 DNS 쿼리에 대한 응답입니다.
- 인바운드 해석기 엔드포인트를 사용하는 온프레미스 리소스의 쿼리입니다.
- 재귀 DNS 해석을 위해 아웃바운드 해석기 엔드포인트를 사용하는 쿼리입니다.
- Route 53 Resolver DNS 방화벽 규칙을 사용하여 도메인 목록을 차단, 허용 또는 모니터링하는 쿼리입니다.

Resolver 쿼리 로그에는 다음과 같은 값이 포함됩니다.

- VPC가 생성된 AWS 리전
- 쿼리가 시작된 VPC의 ID
- 쿼리가 시작된 인스턴스의 IP 주소
- 쿼리가 시작된 리소스의 인스턴스 ID
- 쿼리가 처음 만들어진 날짜와 시간
- 요청된 DNS 이름(예: prod.example.com)
- DNS 레코드 유형(예: A 또는 AAAA)
- DNS 응답 코드(예: `NoError` 또는 `ServFail`)
- DNS 쿼리에 대한 응답으로 반환되는 DNS 응답 데이터(예: IP 주소)
- DNS 방화벽 규칙 작업에 대한 응답

로깅된 모든 값의 자세한 목록과 예제를 보려면 Resolver 쿼리 로그에 표시되는 값을 참조하세요.

> **Note**
>
> DNS 해석기의 표준과 마찬가지로 해석기는 해당 해석기의 유지 시간(TTL)에 따라 결정된 시간 동안 DNS 쿼리를 캐시합니다. Route 53 Resolver는 VPC에서 시작된 쿼리를 캐시하고, 가능한 경우 캐시에서 응답하여 응답 속도를 높입니다. Resolver 쿼리 로깅은 고유 쿼리만 로그하며 해석기가 캐시에서 응답할 수 있는 쿼리는 로그하지 않습니다.
> 예를 들어 쿼리 로깅 구성에서 쿼리를 로깅하는 VPC 중 하나에 있는 EC2 인스턴스가 accounting.example.com에 대한 요청을 제출한다고 가정합니다. 해석기는 해당 쿼리에 대한 응답을 캐시하고 쿼리를 로그합니다. 동일한 인스턴스의 탄력적 네트워크 인터페이스가 해석기 캐시의 TTL 내에서 accounting.example.com에 대한 쿼리를 만드는 경우 해석기가 캐시에서 쿼리에 응답합니다. 두 번째 쿼리는 로그되지 않습니다.

다음 AWS 리소스 중 하나로 로그를 보낼 수 있습니다.

- Amazon CloudWatch Logs(CloudWatch Logs) 로그 그룹
- Amazon S3(S3) 버킷
- Firehose 전송 스트림

자세한 내용은 AWS Resolver 쿼리 로그를 보낼 수 있는 리소스 단원을 참조하십시오.

주제

AWS Resolver 쿼리 로그를 보낼 수 있는 리소스

> **Note**
>
> 초당 쿼리 수(QPS)가 많은 워크로드에 대한 쿼리를 로그하려는 경우 Amazon S3를 사용하여 대상에 쿼리 로그가 기록될 때 쿼리 로그가 제한되지 않도록 해야 합니다. Amazon CloudWatch 를 사용하는 경우 `PutLogEvents` 운영에 대한 초당 요청 수 제한을 늘릴 수 있습니다. CloudWatch 제한을 늘리는 방법에 대해 자세히 알아보려면 Amazon CloudWatch 사용 설명서의 CloudWatch Logs 할당량을 참조하세요.

Resolver 쿼리 로그를 다음 AWS 리소스로 보낼 수 있습니다.

Amazon CloudWatch Logs(Amazon CloudWatch Logs) 로그 그룹

Logs Insights를 사용하여 로그를 분석하고 지표 및 경보를 생성할 수 있습니다.

자세한 내용은 Amazon CloudWatch Logs 사용 설명서를 참조하세요.

Amazon S3(S3) 버킷

S3 버킷은 장기 로그 아카이빙 시 경제적입니다. 일반적으로 지연 시간이 더 깁니다.

모든 S3 서버 측 암호화 옵션은 지원되지 않습니다. 자세한 내용은 Amazon S3 사용 설명서의 서버 측 암호화를 사용하여 데이터 보호를 참조하세요.

S3 버킷이 소유한 계정에 있는 경우 필요한 권한이 버킷 정책에 자동으로 추가됩니다. 소유하지 않은 계정의 S3 버킷에 로그를 보내려면 S3 버킷의 소유자가 계정에 대한 권한을 버킷 정책에 추가해야 합니다. 예:

```
{
    "Version": "2012-10-17",
    "Id": "CrossAccountAccess",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::your_bucket_name/AWSLogs/your_caller_account/
*"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::your_bucket_name"
        },
         {
            "Effect": "Allow",
            "Principal": {
                "AWS": "iam_user_arn_or_account_number_for_root"
```

```
            },
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::your_bucket_name"
        }
    ]
}
```

> **Note**
>
> 조직의 중앙 S3 버킷에 로그를 저장하려는 경우 중앙 계정에서 (중앙 버킷에 쓰는 데 필요한 권한을 사용하여) 쿼리 로깅 구성을 설정하고 RAM을 사용하여 계정 간에 구성을 공유하는 것이 좋습니다.

자세한 내용은 Amazon Simple Storage Service 사용 설명서를 참조하세요.

Firehose 전송 스트림

Amazon OpenSearch Service, Amazon Redshift 또는 기타 애플리케이션에 실시간으로 로그를 스트리밍할 수 있습니다.

자세한 내용은 Amazon Data Firehose 개발자 안내서를 참조하세요.

Resolver 쿼리 로깅 요금에 대한 자세한 내용은 Amazon CloudWatch 요금 섹션을 참조하세요.

CloudWatch Vended Logs 요금은 Resolver 로그를 사용하는 경우 적용되며, 로그가 Amazon S3에 직접 게시되는 경우에도 적용됩니다. 자세한 내용은 Amazon CloudWatch 요금의 로그 요금을 참조하세요.

Resolver 쿼리 로깅 구성 관리

구성(Resolver 쿼리 로깅)

VPC에서 시작된 DNS 쿼리의 로깅을 시작하려면 Amazon Route 53 콘솔에서 다음 작업을 수행합니다.

Resolver 쿼리 로깅을 구성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.

2. Route 53 콘솔 메뉴를 확장합니다. 콘솔의 왼쪽 상단 모서리에서 세 개의 가로 막대 (☰) 아이콘을 선택합니다.
3. Resolver 메뉴에서쿼리 로깅(Query logging)을 선택합니다.
4. 리전 선택기에서 쿼리 로깅 구성을 생성할 AWS 리전을 선택합니다. 이 리전은 DNS 쿼리를 로그하려는 VPC를 생성한 리전과 동일해야 합니다. 여러 리전에 VPC가 있는 경우 리전별로 쿼리 로깅 구성을 하나 이상 생성해야 합니다.
5. 쿼리 로깅 구성(Configure query logging)을 선택합니다.
6. 다음 값을 지정하세요.

   쿼리 로깅 구성 이름

   쿼리 로깅 구성의 이름을 입력합니다. 이 이름은 쿼리 로깅 구성 목록의 콘솔에 표시됩니다. 나중에 이 구성을 찾는 데 도움이 되는 이름을 입력합니다.

   쿼리 로그 대상

   Resolver가 쿼리 로그를 전송할 AWS 리소스 유형을 선택합니다. 옵션(CloudWatch Logs 로그 그룹, S3 버킷, Kinesis Data Firehose 전송 스트림) 중에서 선택하는 방법에 대한 자세한 내용은 AWS Resolver 쿼리 로그를 보낼 수 있는 리소스 섹션을 참조하세요.

   리소스 유형을 선택한 후 해당 유형의 다른 리소스를 생성하거나 현재 AWS 계정에서 생성한 기존 리소스를 선택할 수 있습니다.

   > **Note**
   >
   > 쿼리 로깅 구성을 생성하는 AWS 리전인 4단계에서 선택한 리전에서 생성된 리소스만 선택할 수 있습니다. 새 리소스를 생성하도록 선택하면 해당 리소스가 동일한 리전에서 생성됩니다.

   쿼리를 로그할 VPC

   이 쿼리 로깅 구성은 선택한 VPC에서 시작된 DNS 쿼리를 로그합니다. 해석기에서 쿼리를 로그할 현재 리전에서 각 VPC에 대한 확인란을 선택한 다음 선택을 선택합니다.

> **Note**
>
> VPC 로그 전송은 특정 대상 유형에 대해 한 번만 활성화할 수 있습니다. 로그는 동일한 유형의 여러 대상으로 전송할 수 없습니다. 예를 들어, VPC 로그는 2개의 Amazon S3 대상으로 전송될 수 없습니다.

7. 쿼리 로깅 구성을 선택합니다.

> **Note**
>
> 쿼리 로깅 구성을 생성한 후 몇 분 내에 VPC의 리소스가 만든 DNS 쿼리를 로그에서 확인할 수 있어야 합니다.

Resolver 쿼리 로그에 표시되는 값

각 로그 파일에는 Amazon Route 53가 해당 엣지 로케이션의 DNS 해석기로부터 수신한 각 DNS 쿼리에 대한 하나의 로그 항목이 포함되어 있습니다. 각 로그 항목에는 다음 값이 포함되어 있습니다.

버전

쿼리 로그 형식의 버전 번호입니다. 현재 버전은 `1.1`입니다.

버전 값은 **`major_version.minor_version`** 형식의 메이저 및 마이너 버전입니다. 예를 들어 `version` 값이 `1.7`일 수 있습니다. 여기서 `1` 은 메이저 버전이고 `7`은 마이너 버전입니다.

Route 53에서는 이전 버전과 호환되지 않는 로그 구조가 변경되면 메이저 버전이 증가합니다. 여기에는 이미 존재하는 JSON 필드를 제거하거나 필드 내용이 표시되는 방식(예: 날짜 형식)을 변경하는 작업이 포함됩니다.

변경 사항이 로그 파일에 새 필드를 추가하는 경우 Route 53는 마이너 버전을 증가시킵니다. VPC 내의 일부 또는 모든 기존 DNS 쿼리에 대해 새 정보를 사용할 수 있는 경우 이런 일이 일어날 수 있습니다.

account_id

VPC를 생성한 AWS 계정의 ID입니다.

리전

VPC를 생성한 AWS 리전입니다.

vpc_id

쿼리가 시작된 VPC의 ID입니다.

query_timestamp

쿼리가 ISO 8601 형식 및 협정 세계시(UTC)로 제출된 날짜 및 시간입니다(예: 2017-03-16T19:20:17Z).

ISO 8601 형식에 대한 자세한 내용은 Wikipedia 도움말 ISO 8601을 참조하세요. UTC에 대한 자세한 내용은 Wikipedia 도움말 협정 세계시를 참조하세요.

query_name

쿼리에 지정된 도메인 이름(예: example.com) 또는 하위 도메인 이름(예: www.example.com)입니다.

query_type

요청에서 지정된 DNS 레코드 유형 또는 ANY입니다. Route 53가 지원하는 유형에 대한 자세한 내용은 지원되는 DNS 레코드 유형를 참조하세요.

query_class

쿼리의 클래스입니다.

rcode

Resolver가 DNS 쿼리에 대한 응답으로 반환한 DNS 응답 코드입니다. 이 응답 코드는 쿼리가 유효한지 여부를 표시합니다. 가장 일반적인 응답 코드는 NOERROR이며, 이는 쿼리가 유효한 상태임을 의미합니다. 응답이 유효하지 않은 경우에는 Resolver가 이유를 설명하는 응답 코드를 반환합니다. 가능한 응답 코드의 목록을 보려면 IANA 웹 사이트에서 DNS RCODEs 섹션을 참조하세요.

answer_type

Resolver가 쿼리에 대한 응답으로 반환하는 값의 DNS 레코드 유형(예: A, MX 또는 CNAME)입니다. Route 53가 지원하는 유형에 대한 자세한 내용은 지원되는 DNS 레코드 유형를 참조하세요.

rdata

Resolver가 쿼리에 대한 응답으로 반환한 값입니다. 예를 들어 A 레코드의 경우 이 값은 IPv4 형식의 IP 주소입니다. CNAME 레코드의 경우 이 값은 CNAME 레코드의 도메인 이름입니다.

answer_class

쿼리에 대한 해석기 응답의 클래스입니다.

srcaddr

쿼리가 시작된 인스턴스의 IP 주소입니다.

srcport

쿼리가 시작된 인스턴스의 포트입니다.

운송

DNS 쿼리를 제출하는 데 사용되는 프로토콜입니다.

srcids

DNS 쿼리가 시작되거나 전달된 `instance`, `resolver_endpoint`, 및 `resolver_network_interface`의 ID입니다.

인스턴스

쿼리가 시작된 인스턴스의 ID입니다.

> **Note**
>
> 계정에 표시되지 않는 인스턴스 ID가 Amazon Route 53 Resolver 쿼리 로그에 표시되는 경우 DNS 쿼리가 사용자가 사용한 AWS CloudShell AWS Lambda Amazon EKS 또는 Fargate 콘솔에서 시작되었기 때문일 수 있습니다.

resolver_endpoint

DNS 쿼리를 온프레미스 DNS 서버로 전달하는 해석기 엔드포인트의 ID입니다.

firewall_rule_group_id

쿼리에 있는 도메인 이름과 일치하는 DNS Firewall 규칙 그룹의 ID입니다. 이는 DNS 방화벽이 알림 또는 차단으로 설정된 작업과 일치하는 규칙을 발견한 경우에만 채워집니다.

방화벽 규칙에 대한 자세한 내용은 DNS 방화벽 규칙 그룹 및 규칙를 참조하세요.

firewall_rule_action

쿼리에 있는 도메인 이름과 일치하는 규칙에 의해 지정된 작업입니다. 이는 DNS 방화벽이 알림 또는 차단으로 설정된 작업과 일치하는 규칙을 발견한 경우에만 채워집니다.

firewall_domain_list_id

쿼리에 있는 도메인 이름과 일치하는 규칙에 의해 사용되는 도메인 목록입니다. 이는 DNS 방화벽이 알림 또는 차단으로 설정된 작업과 일치하는 규칙을 발견한 경우에만 채워집니다.

additional_properties

로그 전송 이벤트에 대한 추가 정보입니다. is_delay: 로그 전송이 지연되는 경우입니다.

Route 53 Resolver 쿼리 로그 예제

다음은 Resolver 쿼리 로그 예제입니다.

```
    {
      "srcaddr": "4.5.64.102",
      "vpc_id": "vpc-7example",
      "answers": [
          {
              "Rdata": "203.0.113.9",
              "Type": "PTR",
              "Class": "IN"
          }
      ],
      "firewall_rule_group_id": "rslvr-frg-01234567890abcdef",
      "firewall_rule_action": "BLOCK",
      "query_name": "15.3.4.32.in-addr.arpa.",
      "firewall_domain_list_id": "rslvr-fdl-01234567890abcdef",
      "query_class": "IN",
      "srcids": {
          "instance": "i-0d15cd0d3example"
      },
      "rcode": "NOERROR",
      "query_type": "PTR",
      "transport": "UDP",
      "version": "1.100000",
      "account_id": "111122223333",
      "srcport": "56067",
      "query_timestamp": "2021-02-04T17:51:55Z",
      "region": "us-east-1"
  }
```

Resolver 쿼리 로깅 구성을 다른 AWS 계정과 공유

한 AWS 계정을 사용하여 생성한 쿼리 로깅 구성을 다른 계정과 공유할 수 AWS 있습니다. 구성을 공유하기 위해 Route 53 Resolver 콘솔은 AWS Resource Access Manager와 통합됩니다. Resource Access Manager에 대한 자세한 내용은 Resource Access Manager 사용 설명서 섹션을 참조하세요.

다음을 참조하세요.

공유된 쿼리 로깅 구성을 VPC와 연결

다른 AWS 계정이 하나 이상의 구성을 계정과 공유한 경우 VPCs를 생성한 구성과 연결하는 것과 동일한 방식으로 VPCs 구성과 연결할 수 있습니다.

구성 삭제 또는 공유 해제

구성을 다른 계정과 공유한 후 구성을 삭제하거나 공유를 중지할 경우, 그리고 하나 이상의 VPC가 구성에 연결된 경우 Route 53 Resolver가 해당 VPC에서 시작된 DNS 쿼리를 로깅하지 않습니다.

구성에 연결할 수 있는 쿼리 로깅 구성 및 VPC의 최대 수

계정이 구성을 생성하여 하나 이상의 다른 계정과 공유하는 경우 구성에 연결할 수 있는 최대 VPC 수가 계정에 적용됩니다. 예를 들어 조직에 10,000개의 계정이 있는 경우 중앙 계정에서 쿼리 로깅 구성을 생성하고를 통해 공유 AWS RAM 하여 조직 계정과 공유할 수 있습니다. 그러면 조직 계정은 해당 VPC와 구성을 연결하여 AWS 리전 한도인 100개당 해당 계정의 쿼리 로그 구성 VPC 연결에 대해 구성을 계산합니다. 그러나 모든 VPC가 단일 계정에 있는 경우 해당 계정의 서비스 한도를 늘려야 할 수 있습니다.

현재 Resolver 할당량은 Route 53 Resolver의 할당량 섹션을 참조하세요.

권한

규칙을 다른 AWS 계정과 공유하려면 PutResolverQueryLogConfigPolicy 작업을 사용할 권한이 있어야 합니다.

규칙이 공유되는 AWS 계정에 대한 제한 사항

규칙이 공유되는 계정은 규칙을 변경하거나 삭제할 수 없습니다.

태그 지정

규칙을 생성한 계정만 규칙의 태그를 추가하거나 삭제하거나 볼 수 있습니다.

규칙의 현재 공유 상태를 보고(규칙을 공유한 계정 또는 규칙이 공유되는 계정 포함) 규칙을 다른 계정과 공유하려면 다음 절차를 수행하세요.

공유 상태를 확인하고 쿼리 로깅 구성을 다른 AWS 계정과 공유하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 쿼리 로깅을 선택합니다.
3. 탐색 모음에서 규칙을 생성한 리전을 선택합니다.

   현재 계정이 생성하거나 현재 계정과 공유되는 규칙의 현재 공유 상태가 공유 상태 열에 표시됩니다.

   - 공유되지 않음: 현재 AWS 계정이 규칙을 생성했으며 규칙은 다른 계정과 공유되지 않습니다.
   - 나와 공유됨: 현재 계정이 규칙을 생성하고 하나 이상의 계정과 공유했습니다.
   - 나와 공유 상태: 다른 계정이 규칙을 생성하고 현재 계정과 공유했습니다.
4. 공유 정보를 표시하거나 다른 계정과 공유할 규칙의 이름을 선택합니다.

   규칙: ## ## 페이지에서 소유자 아래의 값은 규칙을 생성한 계정의 ID를 나타냅니다. Sharing status(공유 상태)의 값이 나와 공유 상태가 아닐 경우 현재 계정입니다. 이 경우 소유자는 규칙을 생성하고 현재 계정과 공유한 계정입니다.

   공유 상태도 표시됩니다.
5. 구성 공유를 선택하여 AWS RAM 콘솔을 엽니다.
6. 리소스 공유를 생성하려면 AWS RAM 사용 설명서의 AWS RAM에서 리소스 공유 생성 단계를 따릅니다.

> **Note**
>
> 공유 설정을 업데이트할 수 없습니다. 다음 설정 중 하나로도 변경하려면 규칙을 새로운 설정과 다시 공유한 후 이전 공유 설정을 제거해야 합니다.

도메인 등록 모니터링

Amazon Route 53 대시보드는 다음을 포함하여 도메인 등록 상태에 대한 세부 정보를 제공합니다.

- 새 도메인 등록 상태
- Route 53으로의 도메인 이전 상태
- 만료 날짜가 다가오고 있는 도메인 목록

특히 새 도메인을 등록하거나 도메인을 Route 53으로 이전한 후에는 Route 53 콘솔에서 대시보드를 주기적으로 확인하여 해결할 문제가 없음을 확인하는 것이 좋습니다.

또한 도메인의 연락처 정보가 최신인지 확인할 것을 권장합니다. 도메인 만료 날짜가 다가오면 도메인의 등록자 연락처에게 도메인이 만료되는 시기와 갱신 방법에 관한 정보가 포함된 이메일이 전송됩니다.

Amazon Route 53 상태 확인 및 Amazon CloudWatch를 사용하여 리소스 모니터링

CloudWatch를 사용하여 원시 데이터를 수집하여 읽기 가능하고 실시간에 가까운 지표로 처리하는 Amazon Route 53 상태 확인을 만들어 리소스를 모니터링할 수 있습니다. 이러한 통계는 2주간 기록되므로 기록 정보를 보고 리소스가 어떻게 실행되고 있는지 전체적으로 더 잘 파악할 수 있습니다. Route 53 상태 확인의 지표 데이터는 기본적으로 1분 간격으로 CloudWatch에 자동 전송됩니다.

Route 53 상태 확인에 대한 자세한 내용은 CloudWatch를 이용한 상태 확인 모니터링 섹션을 참조하세요. CloudWatch에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 Amazon CloudWatch란 무엇입니까?를 참조하세요.

Route 53 상태 확인 지표 및 차원

상태 확인이 생성되면 Amazon Route 53는 지정하는 리소스에 대한 지표와 차원을 1분에 한 번씩 CloudWatch에 전송하기 시작합니다. Route 53 콘솔에서 상태 확인의 상태를 확인할 수 있습니다. 또한 다음 절차를 사용하여 CloudWatch 콘솔에서 지표를 보거나 AWS Command Line Interface ()를 사용하여 지표를 볼 수 있습니다AWS CLI.

CloudWatch 콘솔을 사용하여 지표를 보려면

1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 지표(Metrics)를 선택합니다.
3. [All Metrics] 탭에서 [Route 53]을 선택합니다.
4. 상태 확인 지표(Health Check Metrics)를 선택합니다.

를 사용하여 지표를 보려면 AWS CLI

- 명령 프롬프트에서 다음 명령을 사용합니다.

```
aws cloudwatch list-metrics --namespace "AWS/Route53"
```

주제

Route 53 상태 확인을 위한 CloudWatch 지표

AWS/Route53 네임스페이스에는 Route 53 상태 확인을 위한 다음 지표가 포함되어 있습니다.

ChildHealthCheckHealthyCount

계산된 상태 확인의 경우, 상태가 정상인 상태 확인의 수입니다.

유효 통계: 평균(권장), 최소, 최대

단위: 개

ConnectionTime

Route 53 상태 확인 프로그램이 엔드포인트와의 TCP 연결을 설정하는 데 걸린 평균 시간(ms)입니다. 모든 리전이나 선택한 지리적 리전에 걸친 상태 확인의 ConnectionTime를 볼 수 있습니다.

유효 통계: 평균(권장), 최소, 최대

단위: 밀리초

HealthCheckPercentageHealthy

선택된 엔드포인트를 정상으로 여기는 Route 53 상태 확인 프로그램의 비율입니다.

유효 통계: 평균, 최소, 최대

단위: 백분율

HealthCheckStatus

CloudWatch에서 확인하고 있는 상태 확인 엔드포인트의 상태입니다. 1은 정상임을 나타내며 0은 정상이 아님을 나타냅니다.

유효한 통계: 최소, 평균, 최대

단위: 없음

SSLHandshakeTime

Route 53 상태 확인 프로그램이 SSL 핸드셰이크를 완료하는 데 걸린 평균 시간(ms)입니다. 모든 리전이나 선택한 지리적 리전에 걸친 상태 확인의 `SSLHandshakeTime`를 볼 수 있습니다.

유효 통계: 평균(권장), 최소, 최대

단위: 밀리초

TimeToFirstByte

Route 53 상태 확인 프로그램이 HTTP 또는 HTTPS 요청에 대한 응답의 첫 번째 바이트를 수신하는 데 걸린 평균 시간(ms)입니다. 모든 리전이나 선택한 지리적 리전에 걸친 상태 확인의 `TimeToFirstByte`를 볼 수 있습니다.

유효 통계: 평균(권장), 최소, 최대

단위: 밀리초

Route 53 상태 확인 지표를 위한 차원

Route 53 상태 확인 지표는 `AWS/Route53` 네임스페이스를 사용하며 `HealthCheckId`의 지표를 제공합니다. 지표를 검색하려면 `HealthCheckId` 차원을 제공해야 합니다.

또한 `ConnectionTime`, `SSLHandshakeTime` 및 `TimeToFirstByte`의 경우, `Region`을 지정할 수도 있습니다(선택 사항). `Region`을 생략하면 CloudWatch가 모든 리전에 걸친 지표를 반환합니다. `Region`을 포함하면 CloudWatch가 지정된 리전의 지표만 반환합니다.

자세한 내용은 CloudWatch를 이용한 상태 확인 모니터링 섹션을 참조하세요.

Amazon CloudWatch를 사용하여 호스팅 영역 모니터링

Amazon CloudWatch를 사용하여 퍼블릭 호스팅 영역을 모니터링하여 원시 데이터를 수집해 읽기 가능하고 실시간에 가까운 지표로 처리할 수 있습니다. 지표는 Route 53가 지표의 기반이 되는 DNS 쿼리를 수신하는 즉시 사용 가능한 상태가 됩니다. Route 53 호스팅 영역에 대한 CloudWatch 지표 데이터는 1분씩 세분화됩니다.

자세한 내용은 다음 설명서를 참조하세요.

- Amazon CloudWatch 콘솔에서 지표를 확인하는 방법과 AWS Command Line Interface (AWS CLI)를 사용해 지표를 검색하는 방법에 대한 개요 및 정보는 퍼블릭 호스팅 영역에서 DNS 쿼리 지표 보기 섹션을 참조하세요.
- 지표의 보존 기간에 대한 자세한 내용은 Amazon CloudWatch API 참조의 GetMetricStatistics를 참조하세요.
- CloudWatch에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 Amazon CloudWatch란 무엇입니까?를 참조하세요.
- CloudWatch 지표에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 Amazon CloudWatch 지표 사용을 참조하세요.

주제

Route 53 퍼블릭 호스팅 영역에 대한 CloudWatch 지표

AWS/Route53 네임스페이스에는 다음과 같은 Route 53 호스팅 영역의 지표가 포함되어 있습니다.

DNSQueries

호스팅 영역에서 지정된 기간 동안 Route 53가 응답하는 DNS 쿼리의 수입니다.

유효한 통계: Sum, SampleCount

단위: 개

리전: Route 53는 글로벌 서비스입니다. 호스팅 영역 지표를 가져오려면 해당 리전을 미국 동부(버지니아 북부)로 지정해야 합니다.

DNSSECInternalFailure

호스팅 영역의 객체가 INTERNAL_Failure 상태인 경우 값은 1입니다. 그렇지 않은 경우 값은 0입니다.

유효 통계: Sum

단위: 개

볼륨: 호스팅 영역당 4시간 마다 1개

리전: Route 53는 글로벌 서비스입니다. 호스팅 영역 지표를 가져오려면 해당 리전을 미국 동부(버지니아 북부)로 지정해야 합니다.

DNSSECKeySigningKeysNeedingAction

(KMS 오류로 인해) ACTION_NEEDED 상태인 키 서명 키(KSK)의 수입니다.

유효한 통계: Sum, SampleCount

단위: 개

볼륨: 호스팅 영역당 4시간 마다 1개

리전: Route 53는 글로벌 서비스입니다. 호스팅 영역 지표를 가져오려면 해당 리전을 미국 동부(버지니아 북부)로 지정해야 합니다.

DNSSECKeySigningKeyMaxNeedingActionAge

키 서명 키(KSK)가 ACTION_NEEDED 상태로 설정된 이후 경과된 시간입니다.

유효한 통계: Maximum

단위: 초

볼륨: 호스팅 영역당 4시간 마다 1개

리전: Route 53는 글로벌 서비스입니다. 호스팅 영역 지표를 가져오려면 해당 리전을 미국 동부(버지니아 북부)로 지정해야 합니다.

DNSSECKeySigningKeyAge

키 서명 키(KSK)가 생성된 이후(활성화된 이후가 아님) 경과된 시간입니다.

유효한 통계: Maximum

단위: 초

볼륨: 호스팅 영역당 4시간 마다 1개

리전: Route 53는 글로벌 서비스입니다. 호스팅 영역 지표를 가져오려면 해당 리전을 미국 동부(버지니아 북부)로 지정해야 합니다.

Route 53 퍼블릭 호스팅 영역 지표의 CloudWatch 차원

호스팅 영역의 Route 53 지표는 AWS/Route53 네임스페이스를 사용하며 HostedZoneId의 지표를 제공합니다. DNS 쿼리 수를 얻으려면 HostedZoneId 차원에 호스팅 영역의 ID를 지정해야 합니다.

Amazon CloudWatch를 사용하여 Route 53 Resolver 엔드포인트 모니터링

Amazon CloudWatch를 사용하여 Route 53 Resolver 엔드포인트에 의해 전달되는 DNS 쿼리 수를 모니터링할 수 있습니다. Amazon CloudWatch는 원시 데이터를 수집하여 실시간에 가까운 읽기 가능한 지표로 처리합니다. 이러한 통계는 2주간 기록되므로 기록 정보를 보고 리소스가 어떻게 실행되고 있는지 전체적으로 더 잘 파악할 수 있습니다. 기본적으로 Resolver 엔드포인트의 지표 데이터는 5분 간격으로 CloudWatch에 자동 전송됩니다. 5분 간격은 메트릭 데이터를 전송할 수 있는 가장 작은 시간 간격이기도 합니다.

Resolver에 대한 자세한 내용은 Amazon Route 53 Resolver란 무엇인가요? 섹션을 참조하세요. CloudWatch에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 Amazon CloudWatch란 무엇입니까?를 참조하세요.

Route 53 Resolver의 지표 및 차원

DNS 쿼리를 네트워크와 주고받도록 Resolver를 구성하면 Resolver는 전달되는 쿼리의 수에 대한 지표 및 차원을 5분마다 CloudWatch로 전송하기 시작합니다. 다음 절차를 사용하여 CloudWatch 콘솔에서 지표를 보거나 AWS Command Line Interface ()를 사용하여 지표를 볼 수 있습니다AWS CLI.

CloudWatch 콘솔을 사용하여 Resolver 지표를 확인하려면

1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 탐색 모음에서 엔드포인트를 생성한 리전을 선택합니다.
3. 탐색 창에서 지표(Metrics)를 선택합니다.
4. 모든 지표 탭에서 Route 53 Resolver를 선택합니다.
5. 지정된 엔드포인트의 쿼리 수를 보려면 By Endpoint(엔드포인트 기준)를 선택합니다. 그런 다음 쿼리 수를 보려는 엔드포인트를 선택합니다.

   모든 엔드포인트에서를 선택하여 현재 AWS 계정에서 생성한 모든 인바운드 엔드포인트 또는 모든 아웃바운드 엔드포인트의 쿼리 수를 확인합니다. 그런 다음 InboundQueryVolume 또는 OutboundQueryVolume을 선택해 원하는 수를 확인합니다.

를 사용하여 지표를 보려면 AWS CLI

- 명령 프롬프트에서 다음 명령을 사용합니다.

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

주제

Route 53 Resolver의 CloudWatch 지표

AWS/Route53Resolver 네임스페이스에는 Route 53 Resolver 엔드포인트 및 IP 주소에 대한 지표가 포함됩니다.

주제

Resolver 엔드포인트에 대한 지표

AWS/Route53Resolver 네임스페이스에는 다음과 같은 Route 53 Resolver 엔드포인트의 지표가 포함됩니다.

EndpointHealthyENICount

OPERATIONAL 상태의 탄력적 네트워크 인터페이스의 수입니다. 즉, (EndpointId에 의해 지정된) 엔드포인트의 Amazon VPC 네트워크 인터페이스가 올바르게 구성되어 있고 네트워크와 Resolver 사이의 인바운드 또는 아웃바운드 DNS 쿼리를 전달할 수 있습니다.

유효 통계: Minimum, Maximum, Average, Sum

단위: 개

EndpointUnhealthyENICount

AUTO_RECOVERING 상태의 탄력적 네트워크 인터페이스의 수입니다.

즉, 해석기가 (EndpointId에 의해 지정된) 엔드포인트에 연결된 Amazon VPC 네트워크 인터페이스 중 하나 이상을 복구하려고 합니다. 복구 프로세스 중 엔드포인트가 제한된 용량으로 작동하며 완전히 복구될 때까지 DNS 쿼리를 처리할 수 없습니다.

유효 통계: Minimum, Maximum, Average, Sum

단위: 개

InboundQueryVolume

인바운드 엔드포인트의 경우, EndpointId에 의해 지정된 엔드포인트를 통해 네트워크에서 VPC로 전달된 DNS 쿼리의 수입니다.

유효 통계: Sum

단위: 개

OutboundQueryVolume

아웃바운드 엔드포인트의 경우, EndpointId에 의해 지정된 엔드포인트를 통해 VPC에서 네트워크로 전달된 DNS 쿼리의 수입니다.

유효 통계: Sum

단위: 개

OutboundQueryAggregateVolume

아웃바운드 엔드포인트의 경우, 다음을 포함하여 Amazon VPC에서 네트워크로 전달된 총 DNS 쿼리 수입니다.

- EndpointId에 의해 지정된 엔드포인트를 통해 VPC에서 네트워크로 전달된 DNS 쿼리 수.
- 현재 계정이 Resolver 규칙을 다른 계정과 공유하는 경우, 다른 계정에서 생성되어 EndpointId에 의해 지정된 엔드포인트를 통해 네트워크로 전달되는 VPC의 쿼리입니다.

유효 통계: Sum

단위: 개

Resolver IP 주소에 대한 지표

AWS/Route53Resolver 네임스페이스에는 Resolver 인바운드 또는 아웃바운드 엔드포인트에 연결된 각 IP 주소에 대한 다음 지표가 포함됩니다. (엔드포인트를 지정하면 Resolver가 Amazon VPC 탄력적 네트워크 인터페이스를 생성합니다.)

InboundQueryVolume

인바운드 엔드포인트의 각 IP 주소에 대해 네트워크에서 지정된 IP 주소로 전달된 DNS 쿼리 수입니다. 각 IP 주소는 IP 주소 ID로 식별됩니다. Route 53 콘솔을 사용하여 이 값을 확인할 수 있습니다. 해당 엔드포인트 페이지의 IP 주소 섹션에서 IP address ID(IP 주소 ID) 열을 확인합니다. 또한 ListResolverEndpointIpAddresses를 사용하여 프로그래밍 방식으로 이 값을 확인할 수도 있습니다.

유효 통계: Sum

단위: 개

OutboundQueryAggregateVolume

아웃바운드 엔드포인트의 각 IP 주소에 대해 다음을 포함하여 Amazon VPC에서 네트워크로 전달된 총 DNS 쿼리 수입니다.

- 지정된 IP 주소를 사용하여 VPC에서 네트워크로 전달된 DNS 쿼리 수.
- 현재 계정이 Resolver 규칙을 다른 계정과 공유하는 경우, 다른 계정에서 생성되어 지정된 IP 주소를 사용하여 네트워크로 전달되는 VPC의 쿼리입니다.

각 IP 주소는 IP 주소 ID로 식별됩니다. Route 53 콘솔을 사용하여 이 값을 확인할 수 있습니다. 해당 엔드포인트 페이지의 IP 주소 섹션에서 IP address ID(IP 주소 ID) 열을 확인합니다. 또한 ListResolverEndpointIpAddresses를 사용하여 프로그래밍 방식으로 이 값을 확인할 수도 있습니다.

유효 통계: Sum

단위: 개

Route 53 Resolver 지표의 차원

인바운드 및 아웃바운드 엔드포인트의 Route 53 Resolver 지표는 `AWS/Route53Resolver` 네임스페이스를 사용하며 `EndpointId`의 지표를 제공합니다. `EndpointId` 차원의 값을 지정하면 CloudWatch는 지정된 엔드포인트의 DNS 쿼리 수를 반환합니다. 를 지정하지 않으면 `EndpointId` CloudWatch는 현재 AWS 계정에서 생성한 모든 엔드포인트에 대한 DNS 쿼리 수를 반환합니다.

`RniId` 차원은 `OutboundQueryAggregateVolume` 및 `InboundQueryVolume` 지표에 대해 지원됩니다.

Amazon CloudWatch 를 사용하여 Route 53 Resolver DNS 방화벽 규칙 그룹 모니터링

Amazon CloudWatch를 사용하여 Route 53 Resolver DNS 방화벽 규칙 그룹에 의해 필터링되는 DNS 쿼리 수를 모니터링할 수 있습니다. Amazon CloudWatch는 원시 데이터를 수집하여 실시간에 가까운 읽기 가능한 지표로 처리합니다. 이러한 통계는 2주간 기록되므로 기록 정보를 보고 리소스가 어떻게 실행되고 있는지 전체적으로 더 잘 파악할 수 있습니다. 기본적으로 DNS 방화벽 규칙 그룹의 지표 데이터는 5분 간격으로 CloudWatch에 자동 전송됩니다.

DNS 방화벽에 대한 자세한 내용은 DNS 방화벽을 사용하여 아웃바운드 DNS 트래픽 필터링 섹션을 참조하세요. CloudWatch에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 Amazon CloudWatch란 무엇입니까?를 참조하세요.

Route 53 Resolver DNS 방화벽의 지표 및 차원

Route 53 Resolver DNS 방화벽 규칙 그룹을 VPC에 연결하여 DNS 쿼리를 필터링하면 DNS 방화벽은 필터링하는 쿼리에 대한 지표 및 차원을 5분마다 CloudWatch에 전송하기 시작합니다. DNS 방화벽의 지표 및 차원에 대한 자세한 내용은 Route 53 Resolver DNS 방화벽의 CloudWatch 지표 섹션을 참조하세요.

다음 절차를 사용하여 CloudWatch 콘솔에서 지표를 보거나 AWS Command Line Interface ()를 사용하여 지표를 볼 수 있습니다AWS CLI.

CloudWatch 콘솔을 사용하여 DNS 방화벽 지표를 확인하려면

1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 탐색 모음에서 확인하려는 리전을 선택합니다.
3. 탐색 창에서 지표(Metrics)를 선택합니다.
4. 모든 지표 탭에서 Route 53 Resolver를 선택합니다.
5. 관심 있는 지표를 선택합니다.

를 사용하여 지표를 보려면 AWS CLI

- 명령 프롬프트에서 다음 명령을 사용합니다.

```
aws cloudwatch list-metrics --namespace "AWS/Route53Resolver"
```

주제

Route 53 Resolver DNS 방화벽의 CloudWatch 지표

AWS/Route53Resolver 네임스페이스에는 Route 53 Resolver DNS 방화벽 규칙 그룹에 대한 지표가 포함됩니다.

주제

Route 53 Resolver DNS 방화벽 규칙 그룹에 대한 지표

FirewallRuleGroupQueryVolume

(FirewallRuleGroupId에 의해 지정된) 방화벽 규칙 그룹과 일치하는 DNS 방화벽 쿼리 수입니다.

차원: FirewallRuleGroupId

유효 통계: Sum

단위: 개

VPC에 대한 지표

VpcFirewallQueryVolume

(VpcId에 의해 지정된) VPC의 DNS 방화벽 쿼리 수입니다.

차원: VpcId

유효 통계: Sum

단위: 개

방화벽 규칙 그룹 및 VPC 연결에 대한 지표

FirewallRuleGroupVpcQueryVolume

(FirewallRuleGroupId에 의해 지정된) 방화벽 규칙 그룹과 일치하는 (VpcId에 의해 지정된) VPC의 DNS 방화벽 쿼리 수입니다.

차원: FirewallRuleGroupId, VpcId

유효 통계: Sum

단위: 개

방화벽 규칙 그룹의 도메인 목록에 대한 지표

FirewallRuleQueryVolume

(FirewallRuleGroupId에 의해 지정된) 방화벽 규칙 그룹 내에서 (FirewallDomainListId에 의해 지정된) 방화벽 도메인 목록과 일치하는 DNS 방화벽 쿼리 수입니다.

차원: FirewallRuleGroupId, FirewallDomainListId

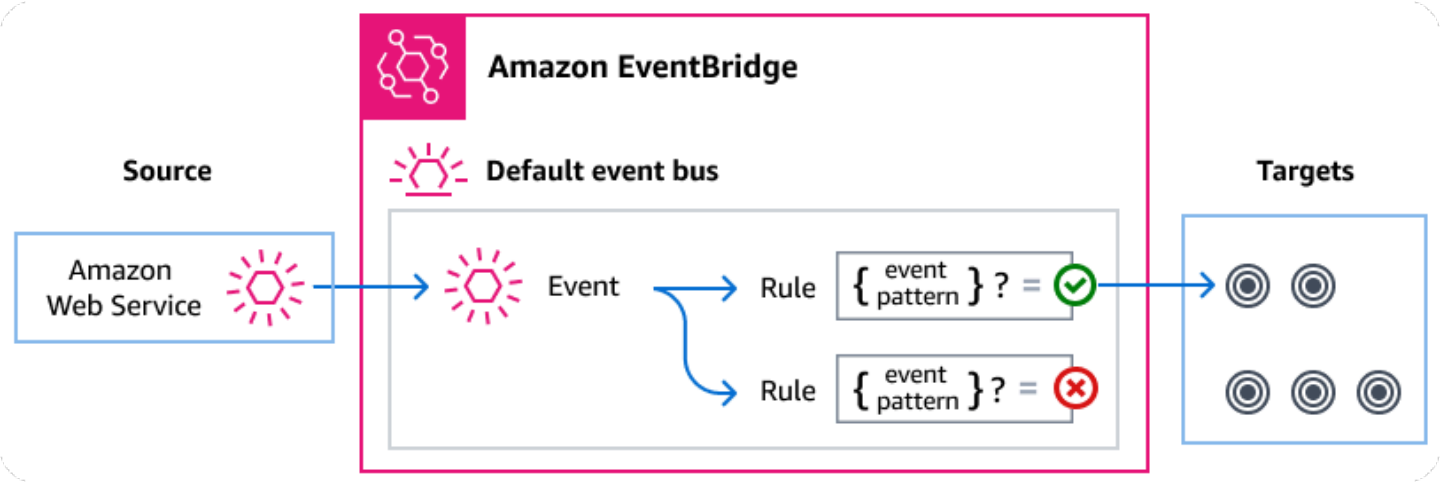
유효 통계: Sum

단위: 개

를 사용하여 Route 53 Resolver DNS 방화벽 이벤트 관리 Amazon EventBridge

Amazon EventBridge 는 이벤트를 사용하여 애플리케이션 구성 요소를 함께 연결하는 서버리스 서비스이므로 확장 가능한 이벤트 기반 애플리케이션을 더 쉽게 구축할 수 있습니다. 이벤트 기반 아키텍처는 이벤트를 내보내고 이에 응답하여 함께 작동하는 느슨하게 결합된 소프트웨어 시스템을 구축하는 스타일입니다. 이벤트는 리소스나 환경의 변화를 나타냅니다.

많은 AWS 서비스와 마찬가지로 DNS 방화벽은 이벤트를 생성하고 기본 이벤트 버스로 EventBridge 전송합니다. (모든 AWS 계정에서 기본 이벤트 버스는 자동으로 프로비저닝됩니다.) 이벤트 버스는 이벤트를 수신하여 0개 이상의 목적지 또는 대상에 전달하는 라우터입니다. 이벤트 버스에 대해 지정한 규칙은 이벤트가 도착할 때 이벤트를 평가합니다. 각 규칙은 이벤트가 규칙의 이벤트 패턴과 일치하는지 여부를 확인합니다. 이벤트가 일치하면 이벤트 버스는 이벤트를 지정된 대상에게 전송합니다.



주제

- Route 53 Resolver DNS 방화벽 이벤트
- EventBridge 규칙을 사용하여 Route 53 Resolver DNS 방화벽 이벤트 전송
- Amazon EventBridge 권한
- 추가 EventBridge 리소스
- Route 53 Resolver DNS 방화벽 이벤트 세부 정보 참조

Route 53 Resolver DNS 방화벽 이벤트

Route 53 Resolver는 DNS 방화벽 이벤트를 기본 EventBridge 이벤트 버스로 자동으로 전송합니다. 이벤트 버스에 규칙을 생성할 수 있습니다. 각 규칙에는 이벤트 패턴과 하나 이상의 대상이 포함됩니다. 규칙의 이벤트 패턴과 일치하는 이벤트는 최대한 지정된 대상으로 전달됩니다. 이벤트는 비순차적으로 전달될 수 있습니다.

다음 이벤트는 DNS 방화벽에서 생성됩니다. 자세한 내용은 Amazon EventBridge 사용 설명서의 EventBridge를 참조하세요.

이벤트 세부 정보 유형	설명
DNS 방화벽 블록	도메인에서 수행되는 모든 블록 작업입니다.
DNS 방화벽 알림	도메인에서 수행되는 모든 알림 작업입니다.

EventBridge 규칙을 사용하여 Route 53 Resolver DNS 방화벽 이벤트 전송

EventBridge 기본 이벤트 버스가 DNS 방화벽 이벤트를 대상으로 전송하도록 하려면 원하는 DNS 방화벽 이벤트의 데이터와 일치하는 이벤트 패턴이 포함된 규칙을 생성해야 합니다.

규칙의 생성은 다음과 같은 일반적인 단계로 구성됩니다.

1. 다음을 지정하는 규칙에 대한 이벤트 패턴 생성:
   - Route 53 Resolver는 규칙에 의해 평가되는 이벤트의 소스입니다.
   - (선택 사항): 일치하는지 확인할 기타 모든 이벤트 데이터.

   자세한 내용은 ??? 단원을 참조하세요.
2. (선택 사항):가 정보를 규칙의 대상으로 EventBridge 전달하기 전에 이벤트의 데이터를 사용자 지정하는 입력 변환기를 생성합니다.

   자세한 내용은 EventBridge 사용 설명서의 입력 변환을 참조하세요.
3. 이벤트 패턴과 일치하는 이벤트를 EventBridge 전달할 대상(들)을 지정합니다.

   대상은 다른 AWS 서비스, software-as-a-service(SaaS) 애플리케이션, API 대상 또는 기타 사용자 지정 엔드포인트일 수 있습니다. 자세한 내용은 EventBridge 사용 설명서의 대상을 참조하세요.

이벤트 버스 규칙 생성에 대해 자세히 알아보려면 EventBridge 사용 설명서의 이벤트에 대응하는 규칙 생성을 참조하세요.

Route 53 Resolver DNS 방화벽 이벤트에 대한 이벤트 패턴 생성

DNS Firewall이 이벤트를 기본 이벤트 버스로 전송하는 경우,는 각 규칙에 대해 정의된 이벤트 패턴을 EventBridge 사용하여 이벤트를 규칙의 대상(들)에 전달해야 하는지 여부를 결정합니다. 이벤트 패턴이 원하는 DNS 방화벽 이벤트의 데이터와 일치합니다. 각 이벤트 패턴은 다음을 포함하는 JSON 객체입니다.

- 이벤트를 전송하는 서비스를 식별하는 `source` 속성입니다. DNS 방화벽 이벤트의 경우 소스는 `aws.route53resolver`입니다.
- (선택 사항): 일치시킬 이벤트 유형의 배열을 포함하는 `detail-type` 속성입니다.
- (선택 사항): 일치시킬 다른 이벤트 데이터를 포함하는 `detail` 속성입니다.

예를 들어 다음 이벤트 패턴은 DNS 방화벽의 알림 및 차단 이벤트와 일치합니다.

```
{
  "source": ["aws.route53resolver"],
  "detail-type": ["DNS Firewall Block", "DNS Firewall Alert"]
}
```

다음 이벤트 패턴이 BLOCK 작업과 일치하는 동안:

```
{
  "source": ["aws.route53resolver"],
  "detail-type": ["DNS Firewall Block"]
}
```

DNS 방화벽은 6시간 내에 동일한 도메인에 대해 동일한 이벤트를 한 번만 전송합니다. 예시:

1. 인스턴스 i-123은 T1 시점에 DNS 쿼리 exampledomain.com을 전송했습니다. 처음 발생하므로 DNS 방화벽이 알림 또는 차단 이벤트를 보냅니다.
2. 인스턴스 i-123은 T1+30분 시점에 DNSquery exampledomain.com을 전송했습니다. 6시간 기간 내에 반복 발생하므로 DNS 방화벽이 경고 또는 차단 이벤트를 보내지 않습니다.
3. 인스턴스 i-123은 T1+7 시간에 DNS 쿼리 exampledomain.com을 전송했습니다. 6시간 기간 외에 발생하므로 DNS 방화벽이 알림 또는 차단 이벤트를 전송합니다.

자세한 내용은 EventBridge 사용 설명서의 이벤트 패턴을 참조하세요.

에서 DNS 방화벽 이벤트에 대한 이벤트 패턴 테스트 EventBridge

EventBridge 샌드박스를 사용하면 더 큰 규칙 생성 또는 편집 프로세스를 완료할 필요 없이 이벤트 패턴을 빠르게 정의하고 테스트할 수 있습니다. 샌드박스를 사용하여 이벤트 패턴을 정의하고 샘플 이벤트를 사용하여 패턴이 원하는 이벤트와 일치하는지 확인할 수 있습니다. 샌드박스에서 직접 해당 이벤트 패턴을 사용하여 새 규칙을 생성할 수 있는 옵션을 EventBridge 제공합니다.

자세한 내용은 EventBridge 사용 설명서의 EventBridge 샌드박스를 사용하여 이벤트 패턴 테스트를 참조하세요.

DNS 방화벽의 EventBridge 규칙 및 대상 생성

다음 절차에서는 EventBridge가 모든 DNS 방화벽 알림 및 차단 작업에 대한 이벤트를 전송하고 AWS Lambda 함수를 규칙의 대상으로 추가할 수 있는 규칙을 생성하는 방법을 보여줍니다.

1. AWS CLI 를 사용하여 EventBridge 규칙을 생성합니다.

```
aws events put-rule \
--event-pattern "{\"source\":
[\"aws.route53resolver\"],\"detail-type\":
[\"DNS Firewall Block\", \"DNS Firewall Alert\"]}" \
--name dns-firewall-rule
```

2. Lambda 함수를 규칙의 대상으로 연결:

   ```
   AWS events put-targets --rule dns-firewall-rule --targets
   Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
   ```

3. 대상을 호출하는 데 필요한 권한을 추가하려면 다음 Lambda AWS CLI 명령을 실행합니다.

   ```
   AWS lambda add-permission --function-name <your_function> --statement-
   id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
   ```

Amazon EventBridge 권한

DNS 방화벽에는 이벤트를 Amazon EventBridge로 전송하는 데 추가 권한이 필요하지 않습니다.

지정하는 대상에는 특정 권한이나 구성이 필요할 수 있습니다. 대상에 특정 서비스를 사용하는 방법에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 Amazon EventBridge 대상을 참조하세요.

추가 EventBridge 리소스

를 사용하여 이벤트를 처리하고 관리하는 방법에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 다음 주제를 참조 EventBridge 하세요.

- 이벤트 버스의 작동 방식에 대한 자세한 내용은 Amazon EventBridge 이벤트 버스를 참조하세요.
- 이벤트 구조에 대해 자세히 알아보려면 이벤트를 참조하세요.
- 이벤트를 규칙과 일치 EventBridge 시킬 때 사용할의 이벤트 패턴을 구성하는 방법에 대한 자세한 내용은 이벤트 패턴을 참조하세요.
- EventBridge 에서 처리하는 이벤트를 지정하는 규칙을 생성하는 방법에 대한 자세한 내용은 규칙을 참조하세요.
- 일치하는 이벤트를 EventBridge 보내는 서비스 또는 기타 대상을 지정하는 방법에 대한 자세한 내용은 대상을 참조하세요.

Route 53 Resolver DNS 방화벽 이벤트 세부 정보 참조

AWS 서비스의 모든 이벤트에는 이벤트의 소스인 AWS 서비스, 이벤트가 생성된 시간, 이벤트가 발생한 계정 및 리전 등 이벤트에 대한 메타데이터가 포함된 공통 필드 세트가 있습니다. 이러한 일반 필드에 대한 정의는 Amazon EventBridge 사용 설명서의 이벤트 구조 참조를 참조하세요.

또한 각 이벤트에는 해당 특정 이벤트와 관련된 데이터를 포함하는 `detail` 필드가 있습니다. 다음 참조는 다양한 DNS 방화벽 이벤트에 대한 세부 정보 필드를 정의합니다.

EventBridge 를 사용하여 DNS 방화벽 이벤트를 선택하고 관리할 때는 다음 사항에 유의하는 것이 좋습니다.

- DNS 방화벽의 모든 이벤트에 대한 `source` 필드는 `aws.route53resolver`로 설정됩니다.
- `detail-type` 필드는 이벤트 유형을 지정합니다.

  예: `DNS Firewall Block`또는 `DNS Firewall Alert`.
- `detail` 필드는 해당 특정 이벤트와 관련된 데이터를 포함합니다.

DNS 방화벽 이벤트와 일치하는 규칙을 활성화하는 이벤트 패턴을 구성하는 방법에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 이벤트 패턴을 참조하세요.

이벤트 및 이벤트 EventBridge 처리 방법에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 Amazon EventBridge 이벤트를 참조하세요.

주제

DNS 방화벽 알림 이벤트 세부 정보

다음은 Alert 상태 이벤트의 세부 정보 필드입니다.

`source` 및 `detail-type` 필드는 Route 53 이벤트에 대한 특정 값을 포함하므로 여기에 포함됩니다.

```
{...,
 "detail-type": "DNS Firewall Alert",
  "source": "aws.route53resolver",
 ...,
 "detail": {
```

```
      "account-id": "string",
      "last-observed-at": "string",
      "query-name": "string",
      "query-type": "string",
      "query-class": "string",
      "transport": "string",
      "firewall-rule-action": "string",
      "firewall-rule-group-id": "string",
      "firewall-domain-list-id": "string",
      "firewall-protection": "string",
      "resources": [{
         "resource-type": "string",
         "instance-details": {
             "id": "string",
       }
     },
     {
         "resource-type": "string",
         "resolver-endpoint-details": {
         "id": "string"
       }
     }
 ]
```

`detail-type`

이벤트의 유형을 식별합니다.

이 이벤트의 경우 이 값은 `DNS Firewall Alert`입니다.

`source`

이벤트를 생성한 서비스를 식별합니다. DNS 방화벽 이벤트의 경우 이 값은 `aws.route53resolver`입니다.

`detail`

이벤트에 대한 정보를 포함하는 JSON 객체입니다. 이벤트를 생성하는 서비스에 따라 이 필드의 내용이 결정됩니다.

이 이벤트의 경우 이 데이터에는 다음이 포함됩니다.

`account-id`

VPC를 AWS 계정 생성한의 ID입니다.

`last-observed-at`

VPC에서 Alert/Block 쿼리가 수행된 시점의 타임스탬프입니다.

`query-name`

쿼리에 지정된 도메인 이름(예: example.com) 또는 하위 도메인 이름(예: www.example.com)입니다.

`query-type`

요청에서 지정된 DNS 레코드 유형 또는 ANY입니다. Route 53가 지원하는 유형에 대한 자세한 내용은 지원되는 DNS 레코드 유형를 참조하세요.

`query-class`

쿼리의 클래스입니다.

`transport`

DNS 쿼리를 제출하는 데 사용되는 프로토콜입니다.

`firewall-rule-action`

쿼리에 있는 도메인 이름과 일치하는 규칙에 의해 지정된 작업입니다. `ALERT` 또는 `BLOCK`입니다.

`firewall-rule-group-id`

쿼리에 있는 도메인 이름과 일치하는 DNS Firewall 규칙 그룹의 ID입니다. 방화벽 규칙 그룹에 대한 자세한 내용은 DNS 방화벽 DNS 방화벽 규칙 그룹 및 규칙를 참조하세요.

`firewall-domain-list-id`

쿼리에 있는 도메인 이름과 일치하는 규칙에 의해 사용되는 도메인 목록입니다.

`firewall-protection`

DNS Firewall Advanced 보호, DGA 또는 DNS_TUNNELING. 자세한 내용은 DNS 방화벽 섹션을 참조하세요Route 53 Resolver DNS 방화벽 고급.

`resourcese`

리소스 유형과 이에 대한 추가 세부 정보를 포함합니다.

`resource-type`

Resolver 엔드포인트 또는 VPC 인스턴스와 같은 리소스 유형을 지정합니다.

resource-type-detail

요청에 대한 추가 세부 정보입니다.

Example DNS 방화벽 알림 이벤트

다음은 알림 이벤트 예제입니다.

```
{
 "version": "1.0",
 "id": "8e5622f9-d81c-4d81-612a-9319e7ee2506",
 "detail-type": "DNS Firewall Alert",
 "source": "aws.route53resolver",
 "account": "123456789012",
 "time": "2023-05-30T21:52:17Z",
 "region": "us-west-2",
 "resources": [],
 "detail": {
 "account-id": "123456789012",
 "last-observed-at": "2023-05-30T20:15:15.900Z",
 "query-name": "15.3.4.32.in-addr.arpa.",
 "query-type": "A",
 "query-class": "IN",
 "transport": "UDP",
 "firewall-rule-action": "ALERT",
 "firewall-rule-group-id": "rslvr-frg-01234567890abcdef",
 "firewall-domain-list-id": "rslvr-fdl-01234567890abcdef",
 "firewall-protection": "DGA",
 "resources": [{
      "resource-type": "instance",
      "instance-details": {
         "id": "i-05746eb48123455e0",
       }
     },
     {
      "resource-type": "resolver-endpoint",
      "resolver-endpoint-details": {
         "id": "i-05746eb48123455e0"
       }
     }
 ],
"src-addr": "4.5.64.102",
"src-port": "56067",
```

```
"vpc-id": "vpc-7example"
 }
}
```

DNS 방화벽 차단 이벤트 세부 정보

다음은 ### ##에 대한 세부 정보 필드입니다.

source 및 detail-type 필드는 Route 53 이벤트에 대한 특정 값을 포함하므로 여기에 포함됩니다.

```
{...,
 "detail-type": "DNS Firewall Block",
  "source": "aws.route53resolver",
 ...,
 "detail": {
      "account-id": "string",
      "last-observed-at": "string",
      "query-name": "string",
      "query-type": "string",
      "query-class": "string",
      "transport": "string",
      "firewall-rule-action": "string",
      "firewall-rule-group-id": "string",
      "firewall-domain-list-id": "string",
      "firewall-protection": "string",
      "resources": [{
         "resource-type": "string",
         "instance-details": {
             "id": "string",
       }
     },
     {
         "resource-type": "string",
         "resolver-endpoint-details": {
         "id": "string"
       }
     }
 ]
```

`detail-type`

이벤트의 유형을 식별합니다.

이 이벤트의 경우 이 값은 DNS Firewall Alert입니다.

source

이벤트를 생성한 서비스를 식별합니다. DNS 방화벽 이벤트의 경우 이 값은 aws.route53resolver입니다.

detail

이벤트에 대한 정보를 포함하는 JSON 객체입니다. 이벤트를 생성하는 서비스에 따라 이 필드의 내용이 결정됩니다.

이 이벤트의 경우 이 데이터에는 다음이 포함됩니다.

account-id

VPC를 AWS 계정 생성한의 ID입니다.

last-observed-at

VPC에서 Alert/Block 쿼리가 수행된 시점의 타임스탬프입니다.

query-name

쿼리에 지정된 도메인 이름(예: example.com) 또는 하위 도메인 이름(예: www.example.com)입니다.

query-type

요청에서 지정된 DNS 레코드 유형 또는 ANY입니다. Route 53가 지원하는 유형에 대한 자세한 내용은 지원되는 DNS 레코드 유형를 참조하세요.

query-class

쿼리의 클래스입니다.

transport

DNS 쿼리를 제출하는 데 사용되는 프로토콜입니다.

firewall-rule-action

쿼리에 있는 도메인 이름과 일치하는 규칙에 의해 지정된 작업입니다. ALERT 또는 BLOCK입니다.

firewall-rule-group-id

쿼리에 있는 도메인 이름과 일치하는 DNS Firewall 규칙 그룹의 ID입니다. 방화벽 규칙 그룹에 대한 자세한 내용은 DNS 방화벽 DNS 방화벽 규칙 그룹 및 규칙를 참조하세요.

`firewall-domain-list-id`

쿼리에 있는 도메인 이름과 일치하는 규칙에 의해 사용되는 도메인 목록입니다.

`firewall-protection`

DNS Firewall Advanced 보호, DGA 또는 DNS_TUNNELING. 자세한 내용은 DNS 방화벽 섹션을 참조하세요Route 53 Resolver DNS 방화벽 고급.

`resourcese`

리소스 유형과 이에 대한 추가 세부 정보를 포함합니다.

`resource-type`

Resolver 엔드포인트 또는 VPC 인스턴스와 같은 리소스 유형을 지정합니다.

`resource-type``-detail`

요청에 대한 추가 세부 정보입니다.

Example 예제 이벤트

다음은 차단 이벤트 예제입니다.

```
{
 "version": "1.0",
 "id": "8e5622f9-d81c-4d81-612a-9319e7ee2506",
 "detail-type": "DNS Firewall Block",
 "source": "aws.route53resolver",
 "account": "123456789012",
 "time": "2023-05-30T21:52:17Z",
 "region": "us-west-2",
 "resources": [],
 "detail": {
 "account-id": "123456789012",
 "last-observed-at": "2023-05-30T20:15:15.900Z",
 "query-name": "15.3.4.32.in-addr.arpa.",
 "query-type": "A",
 "query-class": "IN",
 "transport": "UDP",
 "firewall-rule-action": "BLOCK",
 "firewall-rule-group-id": "rslvr-frg-01234567890abcdef",
 "firewall-domain-list-id": "rslvr-fdl-01234567890abcdef",
 "firewall-protection": "DNS_TUNNELING",
 "resources": [{
```

```
      "resource-type": "instance",
      "instance-details": {
         "id": "i-05746eb48123455e0"
       }
     },
     {
      "resource-type": "resolver-endpoint",
      "resolver-endpoint-details": {
         "id": "i-05746eb48123455e0",
       }
     }
 ],
"src-addr": "4.5.64.102",
"src-port": "56067",
"vpc-id": "vpc-7example"
 }
}
```

를 사용하여 Amazon Route 53 API 호출 로깅 AWS CloudTrail

Route 53는 Route 53의 사용자, 역할 또는 AWS CloudTrail서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다. CloudTrail은 Route 53 콘솔의 호출 및 Route 53 API에 대한 코드 호출을 포함하여 Route 53에 대한 모든 API 호출을 이벤트로 캡처합니다. 추적을 생성하면 Route 53 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 전달할 수 있습니다. 트레일을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail이 수집한 정보를 사용하여 Route 53에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

주제

- CloudTrail의 Route 53 정보
- 이벤트 기록에서 Route 53 이벤트 확인하기
- Route 53 로그 파일 항목 이해

CloudTrail의 Route 53 정보

AWS 계정을 생성할 때 계정에서 CloudTrail이 활성화됩니다. Route 53에서 활동이 발생하면 해당 활동이 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최근 이벤트를 보고 검색하고 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하십시오.

Route 53에 대한 이벤트를 포함하여 AWS 계정의 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 트레일을 생성하면 기본적으로 모든 리전에 트레일이 적용됩니다. 추적은 AWS 파티션의 모든 리전에서 이벤트를 로깅하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하세요.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 수신 및 여러 계정에서 CloudTrail 로그 파일 수신

모든 Route 53 작업은 CloudTrail에서 로깅되며 Amazon Route 53 API 참조에 설명되어 있습니다. 예를 들어 `CreateHostedZone`, `CreateHealthCheck` 및 `RegisterDomain` 작업을 직접적으로 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 대한 정보가 포함됩니다. ID 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트로 했는지 아니면 IAM 사용자 보안 인증 정보로 했는지 여부.
- 역할 또는 페더레이션 사용자의 임시 보안 인증을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청을 했는지 여부입니다.

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

이벤트 기록에서 Route 53 이벤트 확인하기

CloudTrail에서는 이벤트 기록에서 최근 이벤트를 확인할 수 있습니다. Route 53 API 요청에 대한 이벤트를 확인하려면 콘솔 상단의 리전 선택기에서 미국 동부(버지니아 북부)를 선택해야 합니다. 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 이벤트 기록으로 이벤트 보기를 참조하세요.

Route 53 로그 파일 항목 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보를 포함하고 있습니다.

CloudTrail 로그 파일은 퍼블릭 API 직접 호출에 대한 순서 지정된 스택 추적이 아니기 때문에 특정 순서로 표시되지 않습니다.

eventName 요소는 발생한 작업을 식별합니다. (CloudTrail 로그에서 첫 번째 문자는 비록 작업 이름에는 대문자로 되어 있더라도 도메인 등록 작업의 경우 소문자입니다(예: UpdateDomainContact는 로그에서 updateDomainContact로 표시됩니다). CloudTrail에서는 모든 Route 53 API 작업을 지원합니다. 다음 예제는 다음 작업을 보여주는 CloudTrail 로그 항목입니다.

- AWS 계정과 연결된 호스팅 영역 나열
- 상태 확인 생성
- 레코드 2개 생성
- 호스팅 영역 삭제
- 등록된 도메인에 대한 정보 업데이트
- Route 53 Resolver 아웃바운드 엔드포인트 만들기


```
{
    "Records": [
        {
            "apiVersion": "2013-04-01",
            "awsRegion": "us-east-1",
            "eventID": "1cdbea14-e162-43bb-8853-f9f86d4739ca",
            "eventName": "ListHostedZones",
            "eventSource": "route53.amazonaws.com",
            "eventTime": "2015-01-16T00:41:48Z",
            "eventType": "AwsApiCall",
            "eventVersion": "1.02",
            "recipientAccountId": "444455556666",
            "requestID": "741e0df7-9d18-11e4-b752-f9c6311f3510",
            "requestParameters": null,
            "responseElements": null,
            "sourceIPAddress": "192.0.2.92",
            "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
            "userIdentity": {
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                "accountId": "111122223333",
                "arn": "arn:aws:iam::111122223333:user/smithj",
                "principalId": "A1B2C3D4E5F6G7EXAMPLE",
                "type": "IAMUser",
                "userName": "smithj"
            }
```

```
        },
        {
            "apiVersion": "2013-04-01",
            "awsRegion": "us-east-1",
            "eventID": "45ec906a-1325-4f61-b133-3ef1012b0cbc",
            "eventName": "CreateHealthCheck",
            "eventSource": "route53.amazonaws.com",
            "eventTime": "2018-01-16T00:41:57Z",
            "eventType": "AwsApiCall",
            "eventVersion": "1.02",
            "recipientAccountId": "444455556666",
            "requestID": "79915168-9d18-11e4-b752-f9c6311f3510",
            "requestParameters": {
                "callerReference": "2014-05-06 64832",
                "healthCheckConfig": {
                    "iPAddress": "192.0.2.249",
                    "port": 80,
                    "type": "TCP"
                }
            },
            "responseElements": {
                "healthCheck": {
                    "callerReference": "2014-05-06 64847",
                    "healthCheckConfig": {
                        "failureThreshold": 3,
                        "iPAddress": "192.0.2.249",
                        "port": 80,
                        "requestInterval": 30,
                        "type": "TCP"
                    },
                    "healthCheckVersion": 1,
                    "id": "b3c9cbc6-cd18-43bc-93f8-9e557example"
                },
                "location": "https://route53.amazonaws.com/2013-04-01/healthcheck/
b3c9cbc6-cd18-43bc-93f8-9e557example"
            },
            "sourceIPAddress": "192.0.2.92",
            "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
            "userIdentity": {
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                "accountId": "111122223333",
                "arn": "arn:aws:iam::111122223333:user/smithj",
                "principalId": "A1B2C3D4E5F6G7EXAMPLE",
                "type": "IAMUser",
```

```
                "userName": "smithj"
            }
        },
        {
            "additionalEventData": {
                "Note": "Do not use to reconstruct hosted zone"
            },
            "apiVersion": "2013-04-01",
            "awsRegion": "us-east-1",
            "eventID": "883b14d9-2f84-4005-8bc5-c7bf0cebc116",
            "eventName": "ChangeResourceRecordSets",
            "eventSource": "route53.amazonaws.com",
            "eventTime": "2018-01-16T00:41:43Z",
            "eventType": "AwsApiCall",
            "eventVersion": "1.02",
            "recipientAccountId": "444455556666",
            "requestID": "7081d4c6-9d18-11e4-b752-f9c6311f3510",
            "requestParameters": {
                "changeBatch": {
                    "changes": [
                        {
                            "action": "CREATE",
                            "resourceRecordSet": {
                                "name": "prod.example.com.",
                                "resourceRecords": [
                                    {
                                        "value": "192.0.1.1"
                                    },
                                    {
                                        "value": "192.0.1.2"
                                    },
                                    {
                                        "value": "192.0.1.3"
                                    },
                                    {
                                        "value": "192.0.1.4"
                                    }
                                ],
                                "tTL": 300,
                                "type": "A"
                            }
                        },
                        {
                            "action": "CREATE",
```

```
                        "resourceRecordSet": {
                            "name": "test.example.com.",
                            "resourceRecords": [
                                {
                                    "value": "192.0.1.1"
                                },
                                {
                                    "value": "192.0.1.2"
                                },
                                {
                                    "value": "192.0.1.3"
                                },
                                {
                                    "value": "192.0.1.4"
                                }
                            ],
                            "tTL": 300,
                            "type": "A"
                        }
                    }
                ],
                "comment": "Adding subdomains"
            },
            "hostedZoneId": "Z1PA6795UKMFR9"
        },
        "responseElements": {
            "changeInfo": {
                "comment": "Adding subdomains",
                "id": "/change/C156SRE0X2ZB10",
                "status": "PENDING",
                "submittedAt": "Jan 16, 2018 12:41:43 AM"
            }
        },
        "sourceIPAddress": "192.0.2.92",
        "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
        "userIdentity": {
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "accountId": "111122223333",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "type": "IAMUser",
            "userName": "smithj"
        }
    },
```

```
        {
            "apiVersion": "2013-04-01",
            "awsRegion": "us-east-1",
            "eventID": "0cb87544-ebee-40a9-9812-e9dda1962cb2",
            "eventName": "DeleteHostedZone",
            "eventSource": "route53.amazonaws.com",
            "eventTime": "2018-01-16T00:41:37Z",
            "eventType": "AwsApiCall",
            "eventVersion": "1.02",
            "recipientAccountId": "444455556666",
            "requestID": "6d5d149f-9d18-11e4-b752-f9c6311f3510",
            "requestParameters": {
                "id": "Z1PA6795UKMFR9"
            },
            "responseElements": {
                "changeInfo": {
                    "id": "/change/C1SIJYUYIKVJWP",
                    "status": "PENDING",
                    "submittedAt": "Jan 16, 2018 12:41:36 AM"
                }
            },
            "sourceIPAddress": "192.0.2.92",
            "userAgent": "Apache-HttpClient/4.3 (java 1.5)",
            "userIdentity": {
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                "accountId": "111122223333",
                "arn": "arn:aws:iam::111122223333:user/smithj",
                "principalId": "A1B2C3D4E5F6G7EXAMPLE",
                "type": "IAMUser",
                "userName": "smithj"
            }
        },
        {
            "eventVersion": "1.05",
            "userIdentity": {
                "type": "IAMUser",
                "principalId": "A1B2C3D4E5F6G7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:user/smithj",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                "userName": "smithj",
                "sessionContext": {
                    "attributes": {
                        "mfaAuthenticated": "false",
```

```
                    "creationDate": "2018-11-01T19:43:59Z"
                }
            },
            "invokedBy": "test"
        },
        "eventTime": "2018-11-01T19:49:36Z",
        "eventSource": "route53domains.amazonaws.com",
        "eventName": "updateDomainContact",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "192.0.2.92",
        "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:52.0)
Gecko/20100101 Firefox/52.0",
        "requestParameters": {
            "domainName": {
                "name": "example.com"
            }
        },
        "responseElements": {
            "requestId": "034e222b-a3d5-4bec-8ff9-35877ff02187"
        },
        "additionalEventData": "Personally-identifying contact information is not
logged in the request",
        "requestID": "015b7313-bf3d-11e7-af12-cf75409087f6",
        "eventID": "f34f3338-aaf4-446f-bf0e-f72323bac94d",
        "eventType": "AwsApiCall",
        "recipientAccountId": "444455556666"
    },
    {
        "eventVersion": "1.05",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "A1B2C3D4E5F6G7EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/smithj",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2018-11-01T14:33:09Z"
                },
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "AROAIUZEZLWWZOEXAMPLE",
                    "arn": "arn:aws:iam::123456789012:role/Admin",
```

```
                        "accountId": "123456789012",
                        "userName": "Admin"
                    }
                }
            },
            "eventTime": "2018-11-01T14:37:19Z",
            "eventSource": "route53resolver.amazonaws.com",
            "eventName": "CreateResolverEndpoint",
            "awsRegion": "us-west-2",
            "sourceIPAddress": "192.0.2.176",
            "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:52.0)
 Gecko/20100101 Firefox/52.0",
            "requestParameters": {
                "creatorRequestId": "123456789012",
                "name": "OutboundEndpointDemo",
                "securityGroupIds": [
                    "sg-05618b249example"
                ],
                "direction": "OUTBOUND",
                "ipAddresses": [
                    {
                        "subnetId": "subnet-01cb0c4676example"
                    },
                    {
                        "subnetId": "subnet-0534819b32example"
                    }
                ],
                "tags": []
            },
            "responseElements": {
                "resolverEndpoint": {
                    "id": "rslvr-out-1f4031f1f5example",
                    "creatorRequestId": "123456789012",
                    "arn": "arn:aws:route53resolver:us-west-2:123456789012:resolver-
endpoint/rslvr-out-1f4031f1f5example",
                    "name": "OutboundEndpointDemo",
                    "securityGroupIds": [
                        "sg-05618b249example"
                    ],
                    "direction": "OUTBOUND",
                    "ipAddressCount": 2,
                    "hostVPCId": "vpc-0de29124example",
                    "status": "CREATING",
```

```
                    "statusMessage": "[Trace id: 1-5bd1d51e-f2f3032eb75649f71example]
 Creating the Resolver Endpoint",
                    "creationTime": "2018-11-01T14:37:19.045Z",
                    "modificationTime": "2018-11-01T14:37:19.045Z"
                }
            },
            "requestID": "3f066d98-773f-4628-9cba-4ba6eexample",
            "eventID": "cb05b4f9-9411-4507-813b-33cb0example",
            "eventType": "AwsApiCall",
            "recipientAccountId": "123456789012"
        }
    ]
}
```

Amazon Route 53 문제 해결

이 페이지에서는 Amazon Route 53에 대한 다음 문제 해결 주제를 다룹니다.

1. 도메인 사용 불가:
   - 등록자 이메일, DNS 서비스 전송 문제, 잘못된 이름 서버 설정 또는 삭제된 호스팅 영역을 확인하지 않는 등 인터넷에서 도메인을 사용할 수 없는 일반적인 이유를 이해합니다.
2. 도메인 일시 중지:
   - 도메인 일시 중지의 원인(ClientHold 상태)과 만료된 도메인, 확인되지 않은 등록자 이메일 변경, 결제 처리 문제를 포함하여 도메인 일시 중지를 해제하는 방법을 알아봅니다.
3. 실패한 도메인 이전:
   - 전송 권한 부여 안 함, 잘못된 권한 부여 코드 또는 국제화된 도메인 이름 문제 등 Route 53으로의 도메인 이전이 실패한 일반적인 이유를 알아봅니다.
4. DNS 설정이 적용되지 않음:
   - DNS 확인자 캐싱, 잘못된 이름 서버 업데이트, 동일한 이름의 여러 호스팅 영역 등 DNS 설정 변경 사항이 아직 적용되지 않는 문제를 해결합니다.
5. '서버를 찾을 수 없음' 오류:
   - 브라우저에서 누락된 레코드, 잘못된 레코드 값 또는 사용할 수 없는 리소스와 같은 '서버를 찾을 수 없음' 오류에 대한 솔루션을 찾습니다.
6. S3 버킷으로 트래픽 라우팅:
   - 웹사이트 호스팅을 위해 구성된 Amazon S3 버킷으로 트래픽을 라우팅하려고 할 때 발생하는 문제를 해결합니다.
7. 청구 문제:
   - 가 닫히거나 영구적으로 닫힐 때 동일한 호스팅 영역에 대해 두 번 청구되는 것, 도메인에 대한 여러 인보 AWS 계정 이스, 도메인 등록 문제를 비롯한 일반적인 결제 시나리오를 이해합니다.

주제

- 웹사이트 호스팅에 구성된 Amazon S3 버킷에 트래픽을 라우팅할 수 없음
- 같은 호스팅 영역에 대해 요금이 두 번 청구됨
- 도메인에 대해 여러 개의 인보이스 청구
- 내 AWS 계정이 닫히거나 영구적으로 닫히고 내 도메인이 Route 53에 등록됨

내 도메인을 인터넷에서 사용할 수 없음

도메인을 인터넷에서 사용하지 못하는 가장 공통적인 이유는 아래와 같습니다.

주제

- 새 도메인을 등록했지만 확인 이메일에 포함된 링크를 클릭하지 않은 경우
- 도메인 등록만 Amazon Route 53으로 이전하고, DNS 서비스는 이전하지 않았음
- 도메인 등록을 이전한 후 도메인 설정에서 이름 서버를 잘못 지정하였음
- DNS 서비스를 먼저 이전하고 나서 도메인 등록을 이전할 때까지 충분히 기다리지 않았음
- Route 53가 도메인의 인터넷 트래픽 라우팅에 사용하는 호스팅 영역을 삭제했습니다.
- 도메인이 일시 중지된 경우

새 도메인을 등록했지만 확인 이메일에 포함된 링크를 클릭하지 않은 경우

새 도메인을 등록할 때 ICANN은 등록자 연락처의 이메일 주소가 유효하다는 확인을 받을 것을 요구합니다. 확인을 위해 링크가 포함된 이메일을 보내드립니다. (첫 번째 이메일에 응답하지 않을 경우 같은 이메일을 최대 두 번 더 보냅니다.) 최상위 도메인에 따라 다르지만 3~15일 사이에 링크를 클릭해야 합니다. 이 기간이 지나면 링크 작동이 정지됩니다.

할당된 기간 안에 이메일의 링크를 클릭하지 않으면 ICANN은 도메인 일시 중지를 요구합니다. 등록자 연락처로 확인 이메일을 다시 보내는 자세한 방법은 권한 부여 및 확인 이메일 재전송 단원을 참조하십시오.

도메인 등록만 Amazon Route 53으로 이전하고, DNS 서비스는 이전하지 않았음

이전 등록 기관이 도메인 등록 시 DNS 서비스를 무료로 제공한 경우에는 도메인 등록을 Route 53으로 이전하면서 등록 기관이 DNS 서비스 제공을 중단했을 수도 있습니다. 다음 절차에 따라 사실 여부를 확인한 후 그렇다면 문제까지 해결할 수 있습니다.

도메인 등록을 Route 53으로 이전하고 나서 전 등록 기관이 중단한 DNS 서비스를 복구하는 방법

1. 이전 등록 대행자에게 연락하여 도메인 DNS 서비스 중단 여부를 확인합니다. 중단하였다면 선호도에 따라 도메인 DNS 서비스를 가장 빠르게 복구할 수 있는 세 가지 방법이 있습니다.

   - 이전 등록 대행자가 유료 DNS 서비스를 제공하고 있다면 도메인에 대한 이전 DNS 레코드와 이름 서버를 사용해 DNS 서비스 복구를 요청하십시오.
   - 이전 등록 대행자가 도메인 등록 없이는 유료 DNS 서비스를 제공하지 않는다면 도메인 등록을 다시 등록 대행자에게 이전한 후 도메인에 대한 이전 DNS 레코드와 이름 서버를 사용해 DNS 서비스를 복구할 수 있는지 물으십시오.
   - 도메인 등록을 전 등록 대행자로 다시 이전할 수는 있지만 DNS 레코드가 삭제된 경우에는 도메인 등록을 다시 이전하여 이전에 도메인에 할당되었던 것과 동일한 이름 서버를 사용할 수 있는지 물으십시오. 가능하다면 이전 DNS 레코드는 직접 다시 생성해야 합니다. 이렇게 DNS 레코드만 생성하면 도메인을 다시 사용할 수 있게 됩니다.

   이전 등록 대행자가 위 옵션 중 어떤 것도 도울 수 없는 경우에는 2단계로 진행합니다.

   > **Important**
   >
   > Route 53으로 도메인을 이전하면서 지정했던 이름 서버를 사용해서 DNS 서비스를 복구하지 못한다면 인터넷에서 도메인을 다시 사용하기 위한 절차에서 나머지 단계를 완료한 후에도 최대 2일이 소요될 수 있습니다. DNS 해석기는 일반적으로 도메인 이름 서버의 이름을 24~48시간까지 캐싱하며, 모든 DNS 클라이언트가 새로운 이름 서버의 이름을 가져오는 데 최대 2일이 걸리는 이유도 여기에서 기인합니다.

2. 새로운 DNS 서비스(예: Route 53)를 선택합니다.
3. 새로운 DNS 서비스에서 제공하는 메서드를 사용하여 다음과 같이 호스팅 영역과 레코드를 생성합니다.

   a. 도메인과 동일한 이름으로 호스팅 영역을 생성합니다(예: example.com).

   b. 이전 등록 대행자에게서 가져온 영역 파일을 사용하여 레코드를 생성합니다.

   새로운 DNS 서비스로 Route 53를 선택하면 영역 파일을 가져와서 레코드를 생성할 수 있습니다. 자세한 내용은 영역 파일을 가져와 레코드 생성 단원을 참조하십시오.
4. 새로운 호스팅 영역의 이름 서버를 가져옵니다. DNS 서비스로 Route 53를 선택한 경우에는 퍼블릭 호스팅 영역에 대한 이름 서버 가져오기 섹션을 참조하세요.

5. 도메인 이름 서버를 4단계에서 가져온 이름 서버로 변경합니다. 자세한 내용은 도메인의 글루 레코드 및 이름 서버 추가 또는 변경 단원을 참조하십시오.

도메인 등록을 이전한 후 도메인 설정에서 이름 서버를 잘못 지정하였음

도메인 등록을 Amazon Route 53으로 이전하면서 지정하는 도메인 설정 중에 도메인의 DNS 쿼리에 응답하는 이름 서버들이 있습니다. 이 이름 서버들은 도메인과 동일한 이름의 호스팅 영역에서 제공됩니다. 호스팅 영역에는 www.example.com 웹 서버의 IP 주소 등을 포함하여 도메인 트래픽을 라우팅하는 방법에 대한 정보가 저장됩니다.

잘못된 호스팅 영역에 이름 서버를 지정하는 실수를 저지를 수도 있습니다. 특히 도메인과 동일한 이름의 호스팅 영역이 2개 이상일 때 이러한 실수를 범하기 쉽습니다. 도메인이 이름 서버를 올바른 호스팅 영역에 사용하고 있는지 확인하려면 먼저 필요할 경우 도메인 이름 서버를 업데이트한 후 다음 절차를 진행하십시오.

> **Important**
>
> 도메인을 Route 53으로 이전할 때 잘못된 이름 서버 레코드를 지정하면 도메인 이름 서버를 수정한 후에도 DNS 서비스를 완전히 복구할 때까지 최대 2일이 걸릴 수 있습니다. 이는 인터넷을 통하는 DNS 해석기가 일반적으로 2일 1회에 한하여 이름 서버를 요청하고 응답을 캐시하기 때문입니다.

호스팅 영역에 이름 서버를 지정하는 방법

1. 다른 도메인 DNS 서비스를 사용하는 경우에는 DNS 서비스에서 제공하는 메서드를 사용하여 호스팅 영역에 이름 서버를 지정합니다. 그러고 나서 다음 절차로 진행합니다.

   Route 53을 도메인의 DNS 서비스로 사용하는 경우에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
3. [Hosted Zones] 페이지에서 호스팅 영역의 (이름 대신) 라디오 버튼을 선택합니다.

   > **Important**
   >
   > 동일한 이름의 호스팅 영역이 2개 이상이라면 이름 서버를 올바른 호스팅 영역에 지정할 수 있도록 주의해야 합니다.

4. 오른쪽 창에서 [Name Servers]에 나열된 4개의 서버를 기록합니다.

도메인이 올바른 이름 서버를 사용하고 있는지 확인하는 방법

1. 도메인에 다른 DNS 서비스를 사용하는 경우에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.

   Route 53를 사용하는 경우에는 다음 단계로 넘어갑니다.
2. 탐색 창에서 [Registered Domains]를 선택합니다.
3. 설정을 편집하고자 하는 도메인의 이름을 선택합니다.
4. Add or Edit Name Servers를 선택합니다.
5. 이전 절차에서 지정한 이름 서버 목록과 Edit Name Servers for 도메인 이름 대화 상자에 나열된 이름 서버를 서로 비교합니다.
6. 대화 상자의 이름 서버와 이전 절차에서 지정한 이름 서버가 일치하지 않으면 대화 상자의 이름 서버를 변경한 후 Update를 선택합니다.

DNS 서비스를 먼저 이전하고 나서 도메인 등록을 이전할 때까지 충분히 기다리지 않았음

DNS 서비스를 Amazon Route 53으로 이전하였거나, 혹은 다른 DNS 서비스로 이전하면서 도메인 구성을 새로운 DNS 서비스의 이름 서버를 사용할 도메인 등록 기관으로 업데이트하였습니다.

도메인 요청에 응답하는 DNS 해석기는 일반적으로 이름 서버 이름을 24~48시간까지 캐싱합니다. 예를 들어 도메인 DNS 서비스를 변경하여 다른 DNS 서비스의 이름 서버로 바꾸면 DNS 해석기가 새로운 이름 서버와 DNS 서비스를 사용할 때까지 최대 48시간이 소요될 수 있습니다.

아래는 DNS 서비스를 이전하고 나서 도메인을 너무 빨리 이전하여 인터넷에서 도메인을 사용할 수 없게 되는 경우를 설명한 것입니다.

1. 도메인 DNS 서비스를 이전하였습니다.
2. DNS 해석기가 새로운 DNS 서비스의 이름 서버를 사용하기 전에 도메인을 Route 53으로 이전하였습니다.
3. 도메인이 Route 53으로 이전되자마자 이전 등록 기관이 도메인 DNS 서비스를 취소하였습니다.
4. DNS 해석기는 여전히 이전 DNS 서비스로 쿼리를 라우팅하려고 하지만 트래픽 라우팅 방법을 나타내는 레코드가 더 이상 존재하지 않습니다.

이전 DNS 서비스의 이름 서버 캐싱이 만료되면 DNS가 새로운 DNS 서비스를 사용하기 시작합니다. 그러나 안타깝지만 이 프로세스를 가속화할 방법이 없습니다.

Route 53가 도메인의 인터넷 트래픽 라우팅에 사용하는 호스팅 영역을 삭제했습니다.

Route 53가 도메인의 DNS 서비스인데 도메인의 인터넷 트래픽 라우팅에 사용하는 호스팅 영역을 삭제한 경우, 이 도메인을 인터넷에서 사용할 수 없게 됩니다. 이는 도메인이 Route 53에 등록되었는지 여부와 상관없이 해당됩니다.

> **Important**
>
> 도메인에 인터넷 서비스를 복원하는 과정은 최대 48시간이 소요됩니다.

Route 53가 도메인의 인터넷 트래픽 라우팅에 사용하는 호스팅 영역을 삭제한 경우 인터넷 서비스를 복원하려면

1. 도메인과 이름이 동일한 다른 호스팅 영역을 생성합니다. 자세한 내용은 퍼블릭 호스팅 영역 생성 단원을 참조하십시오.
2. 삭제한 호스팅 영역에 있던 레코드를 다시 생성합니다. 자세한 내용은 레코드 작업 단원을 참조하십시오.
3. Route 53가 새 호스팅 영역에 할당된 이름 서버의 이름을 가져옵니다. 자세한 내용은 퍼블릭 호스팅 영역에 대한 이름 서버 가져오기 단원을 참조하십시오.
4. 3단계에서 얻은 이름 서버를 사용하도록 도메인 등록을 업데이트

   - 도메인이 Route 53에 등록되어 있으면 도메인의 글루 레코드 및 이름 서버 추가 또는 변경 섹션을 참조하세요.
   - 도메인이 다른 도메인 등록 대행자에 등록되어 있는 경우 등록 대행자가 제공한 방법을 사용하여 도메인 등록이 새로운 이름 서버를 사용하도록 업데이트하십시오.
5. 삭제된 호스팅 영역에 이름 서버의 이름을 캐싱한 recursive resolver를 이름 서버용 TTL이 전달되기를 기다리십시오. TTL이 전달된 후 브라우저 또는 애플리케이션이 도메인 또는 하위 도메인 중 하나에 DNS 쿼리를 제출하면 재귀 해석기가 이 쿼리를 새 호스팅 영역에 대한 Route 53 이름 서버로 전달합니다. 자세한 내용은 Amazon Route 53가 도메인의 트래픽을 라우팅하는 방법 단원을 참조하십시오.

   이름 서버용 TTL은 도메인의 TLD에 따라 최대 48시간입니다.

도메인이 일시 중지된 경우

도메인을 일시 중지했기 때문에 인터넷에서 해당 도메인을 사용하지 못할 수 있습니다. 자세한 내용은 내 도메인이 일시 중지됨(상태: ClientHold) 단원을 참조하십시오.

내 도메인이 일시 중지됨(상태: ClientHold)

Amazon Route 53가 도메인을 일시 중지할 경우 인터넷에서 도메인을 사용할 수 없게 됩니다. 다음 방법 중 하나를 사용하여 도메인이 일시 중지되었는지 여부를 확인할 수 있습니다.

- Route 53 콘솔의 등록된 도메인(Registered domains) 페이지에서 페이지 하단에 있는 알림(Alerts) 테이블의 도메인 이름을 찾을 수 있습니다. [Status] 열의 값이 [clientHold]일 경우 도메인이 일시 중지된 것입니다.
- 도메인에 대해 WHOIS 쿼리를 보냅니다. [Domain Status] 값이 [clientHold]일 경우 도메인이 일시 중지된 것입니다. WHOIS 명령은 많은 운영 체제에서 사용할 수 있고, 많은 웹 사이트에서 웹 애플리케이션으로도 사용 가능합니다.

또한 도메인을 일시 중지할 때, 일반적으로 도메인 등록자 연락처의 이메일 주소로 이메일을 보냅니다. 하지만 도메인이 법원 명령에 따라 일시 중지된 경우에는 법원이 등록자 연락처로 통보하는 것을 금지할 수 있습니다.

인터넷에서 다시 도메인을 사용하려면 일시 중지를 해제해야 합니다. 다음은 도메인이 일시 중지될 수 있는 이유와 일시 중지를 해제하는 방법입니다.

> **Note**
>
> 도메인 일시 중지를 해제하는 데 도움이 필요한 경우 무료로 AWS Support에 문의할 수 있습니다. 자세한 내용은 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.

주제

- 새 도메인을 등록했지만 확인 이메일에 포함된 링크를 클릭하지 않은 경우
- 도메인 자동 갱신이 비활성화된 상태에서 도메인이 만료
- 등록자 연락처의 이메일 주소를 변경했지만 새 이메일 주소가 유효한지 확인하지 않음
- 자동 도메인 갱신 결제를 처리할 수 없어 도메인이 만료됨

- AWS 이용 정책 위반 때문에 AWS 에서 도메인을 일시 중지
- 법원 명령으로 인해 도메인이 일시 중지되었습니다

새 도메인을 등록했지만 확인 이메일에 포함된 링크를 클릭하지 않은 경우

도메인을 AWS 에 처음 등록할 때 ICANN은 등록자 연락처의 이메일 주소가 유효한지 확인해야 합니다. 확인을 위해 링크가 포함된 이메일을 보내드립니다. 최상위 도메인에 따라 다르지만 3~15일 사이에 링크를 클릭해야 합니다. 이 기간이 지나면 링크 작동이 정지됩니다.

> **Note**
>
> 이미 하나 이상의 도메인을 Amazon Route 53에 등록했고 같은 등록자 연락처 이메일 주소를 사용했다면 확인 이메일이 발송되지 않습니다.

할당된 기간 안에 이메일의 링크를 클릭하지 않으면 ICANN은 도메인 일시 중지를 요구합니다. 등록자 연락처로 확인 이메일을 다시 보내는 자세한 방법은 권한 부여 및 확인 이메일 재전송 단원을 참조하십시오. 사용자가 이메일 주소가 유효함을 확인하면 도메인 일시 중지가 자동으로 해제됩니다.

도메인 자동 갱신이 비활성화된 상태에서 도메인이 만료

도메인에 대해 자동 갱신이 활성화되어 있으면(새 도메인 또는 이전된 도메인의 기본값) 만료 날짜 직전에 자동으로 도메인 등록이 갱신됩니다. 사용자가 자동 갱신을 비활성화한 경우 등록자 연락처의 이메일 주소로 도메인 등록 만료 안내 이메일을 세 번 보냅니다. 첫 번째 이메일은 도메인이 만료하기 45일 전에 발송됩니다.

사용자가 도메인 자동 갱신을 비활성화하고 수동으로 도메인 등록 기간을 연장하지 않는 경우 일반적으로 만료 날짜에 도메인이 일시 중지됩니다. 일부 도메인 등록 기관은 만료 날짜 이전에도 도메인을 삭제할 수 있으므로 유의해야 합니다.

만료된 도메인을 갱신하는 방법에 대한 자세한 내용은 도메인 등록 갱신 단원을 참조하십시오.

등록자 연락처의 이메일 주소를 변경했지만 새 이메일 주소가 유효한지 확인하지 않음

등록자 연락처의 이메일 주소를 이전에 확인하지 않은 주소로 변경하는 경우 ICANN에서는 등록자 연락처의 이메일 주소가 유효한지 확인을 받도록 요구합니다. 확인을 위해 링크가 포함된 이메일을 보내

드립니다. 최상위 도메인에 따라 다르지만 3~15일 사이에 링크를 클릭해야 합니다. 이 기간이 지나면 링크 작동이 정지됩니다.

TLD 등록 기관이 허용하는 기간 안에 이메일의 링크를 클릭하지 않으면 ICANN은 도메인 일시 중지를 요구합니다. 등록자 연락처로 확인 이메일을 다시 보내는 자세한 방법은 권한 부여 및 확인 이메일 재전송 단원을 참조하십시오. 사용자가 이메일 주소가 유효함을 확인하면 도메인 일시 중지가 자동으로 해제됩니다.

자동 도메인 갱신 결제를 처리할 수 없어 도메인이 만료됨

도메인에 대해 자동 갱신이 활성화되어 있지만 결제를 처리할 수 없는 경우(예를 들어 신용 카드가 만료됨) 도메인 등록자 연락처의 이메일 주소로 이메일을 여러 번 발송합니다. 결제가 이루어지지 않으면 일반적으로 만료 날짜에 도메인이 일시 중지됩니다. 일부 도메인 등록 기관은 만료 날짜 이전에도 도메인을 삭제할 수 있으므로 유의해야 합니다.

만료된 도메인을 갱신하는 방법에 대한 자세한 내용은 도메인 등록 갱신 단원을 참조하십시오.

AWS 이용 정책 위반 때문에 AWS 에서 도메인을 일시 중지

AWS 에서 AWS 이용 정책 위반을 사유로 도메인을 일시 중지한 경우 도메인 등록자 연락처로 이메일 알림을 보냅니다. (AWS 계정이 이미 사기로 일시 중지된 경우 알림 이메일을 보내지 않습니다.)

일시 중지에 이의를 제기하려면 trustandsafety@support.aws.com으로 이메일을 보내세요.

법원 명령으로 인해 도메인이 일시 중지되었습니다

법원 명령 때문에 도메인이 일시 중지될 경우 법원 명령이 철회될 때까지는 도메인 일시 중지를 해제할 수 없습니다. 법원 명령의 유효성에 이의를 제기하려면 trustandsafety@support.aws.com으로 이메일을 보내고 해당 문서를 첨부합니다.

내 도메인의 Amazon Route 53 이전 실패

Amazon Route 53으로 도메인 이전이 실패하는 몇몇 일반적인 이유는 다음과 같습니다.

주제

- 승인 이메일의 링크를 클릭하지 않았습니다.
- 현재 등록 대행자로부터 받은 승인 코드가 유효하지 않음
- .es 도메인을 Amazon Route 53으로 이전 시 "Parameters in request are not valid" 오류
- Amazon Route 53으로 이전하려는 다국어 도메인 이름이 퓨니코드로 작성되어 있습니까?

승인 이메일의 링크를 클릭하지 않았습니다.

도메인 등록을 Amazon Route 53으로 이전하는 경우, 도메인 등록 관리 기관인 ICANN은 도메인 등록자 연락처를 이전하기 위한 승인을 받을 것을 요구합니다. 승인을 받으려면 링크가 포함된 이메일을 보내드립니다. 최상위 도메인에 따라 다르지만 5~15일 사이에 링크를 클릭해야 합니다. 이 기간이 지나면 링크 작동이 정지됩니다.

할당된 기간 안에 이메일의 링크를 클릭하지 않으면 ICANN은 이전 취소를 요구합니다. 등록자 연락처로 권한 부여 이메일을 다시 보내는 자세한 방법은 권한 부여 및 확인 이메일 재전송 단원을 참조하십시오.

현재 등록 대행자로부터 받은 승인 코드가 유효하지 않음

도메인을 Amazon Route 53으로 이전하도록 요청했는데 승인 이메일을 받지 못한 경우 Route 53 콘솔의 상태 페이지를 확인하세요. 등록 대행자로부터 받은 이전 승인 코드가 유효하지 않다고 상태 페이지에 표시될 경우 다음과 같이 하십시오.

1. 도메인의 현재 등록 대행자에게 연락하여 새로운 승인 코드를 요청합니다. 다음을 확인합니다.
   - 새로운 승인 코드의 남은 유효 기간. 코드가 만료되기 전에 도메인 이전을 요청해야 합니다.
   - 새로운 승인 코드는 유효하지 않은 코드와 다릅니다. 그렇지 않을 경우 현재 등록 대행자에게 승인 코드 갱신을 요청하십시오.
2. 도메인 이전 요청을 새로 제출합니다. 자세한 내용은 5단계: 이전 요청 주제에서 도메인 등록을 Amazon Route 53으로 이전하기 섹션을 참조하세요.

.es 도메인을 Amazon Route 53으로 이전 시 "Parameters in request are not valid" 오류

.es 도메인을 Route 53으로 이전 시 등록자 연락처의 연락처 유형이 회사(Company)인 경우 Amazon Route 53에서 “Parameters in request are not valid" 오류를 반환합니다. 이전을 완료하려면 등록자의 연락처 유형을 개인(person)으로 변경하고 다시 제출합니다.

Amazon Route 53으로 이전하려는 다국어 도메인 이름이 퓨니코드로 작성되어 있습니까?

새 도메인 이름을 등록하거나 호스팅 영역 및 레코드를 생성할 때, a-z 이외의 문자(예: 프랑스어의 ç), 기타 알파벳 문자(예: 키릴 자모, 아랍어), 중국어, 일본어 또는 한국어 문자를 지정할 수 있습니다.

Amazon Route 53는 이러한 다국어 도메인 이름(IDN)을 퓨니코드로 저장합니다. 그럼 퓨니코드는 유니코드 문자를 ASCII 문자열로 나타냅니다.

IDN을 Route 53으로 이전하는 동안 오류가 발생하면 퓨니코드를 사용하여 나타내고 다시 시도하십시오. 자세한 내용은 다국어 도메인 이름 형식 단원을 참조하십시오.

DNS 설정을 변경하였지만 변경 사항이 적용되지 않음

DNS 설정을 변경하였는데도 변경 사항이 적용되지 않을 때는 몇 가지 공통 이유가 있습니다.

주제

- 지난 48시간이 지나기 이전에 DNS 서비스를 Amazon Route 53으로 이전하였기 때문에 DNS가 여전히 이전 DNS 서비스를 사용하고 있음
- 최근에 DNS 서비스를 Amazon Route 53으로 이전하였지만 이름 서버를 도메인 등록 기관으로 업데이트하지 않음
- DNS 해석기가 여전히 이전 레코드 설정을 사용하고 있음
- 이름이 같은 호스팅 영역이 두 개 이상 있고 도메인에 연결되지 않은 호스팅 영역을 업데이트함

지난 48시간이 지나기 이전에 DNS 서비스를 Amazon Route 53으로 이전하였기 때문에 DNS가 여전히 이전 DNS 서비스를 사용하고 있음

DNS 서비스를 Amazon Route 53으로 이전하면 도메인 등록 기관이 제공한 메서드를 사용하여 이전 DNS 서비스의 이름 서버를 Route 53의 4개 이름 서버로 교체하였습니다.

> **Note**
>
> 이 부분에 대해서 잘 모를 경우에는 최근에 DNS 서비스를 Amazon Route 53으로 이전하였지만 이름 서버를 도메인 등록 기관으로 업데이트하지 않음를 참조하십시오.

도메인 등록 대행자는 일반적으로 이름 서버에 24~48 TTL(Time To Live) 시간을 사용합니다. 이 말은 DNS 해석기가 도메인 이름 서버를 지정할 경우 현재 도메인 이름 서버에 다른 요청을 제출할 때까지 최대 48시간 동안 해당 정보를 사용한다는 것을 의미합니다. 즉, DNS 서비스를 Route 53으로 이전한 후 DNS 설정을 변경하였다고 해도 48시간이 지나기 이전에는 일부 DNS 해석기가 여전히 이전 DNS 서비스를 사용하여 도메인 트래픽을 라우팅합니다.

최근에 DNS 서비스를 Amazon Route 53으로 이전하였지만 이름 서버를 도메인 등록 기관으로 업데이트하지 않음

도메인 등록 대행자는 도메인 DNS 서비스의 이름 서버를 포함하여 도메인에 대한 다양한 정보를 가지고 있습니다. 일반적으로 도메인 등록 대행자 역시 DNS 서비스이기 때문에 도메인에 연결되는 이름 서버는 등록 대행자에 속합니다. 이러한 이름 서버는 도메인 트래픽이, 예를 들어 도메인 웹 서버의 IP 주소로 라우팅되는 방식에 대한 정보를 얻을 수 있는 곳을 DNS에게 알려주는 역할을 합니다.

DNS 서비스를 Amazon Route 53으로 이전할 때는 도메인 등록 기관이 제공하는 메서드를 사용하여 도메인에 연결되는 이름 서버를 변경해야 합니다. 일반적으로 등록 기관이 제공하는 이름 서버를 도메인에 생성한 호스팅 영역과 연결되는 Route 53 이름 서버 4개로 변경하는 경우가 많습니다.

도메인에 새로운 호스팅 영역과 레코드를 생성한 후 이전 DNS 서비스에 사용했던 것과 다른 설정을 지정한 경우, 혹은 DNS가 여전히 트래픽을 이전 리소스로 라우팅하는 경우에는 이름 서버를 도메인 등록 대행자로 업데이트하지 않았을 가능성이 높습니다. 등록 기관이 Route 53 호스팅 영역의 이름 서버를 사용하고 있는지 알아보려면 필요에 따라 도메인 이름 서버를 업데이트한 후 다음 절차를 실시합니다.

호스팅 영역에 이름 서버를 지정한 후 이름 서버 설정을 도메인 등록 대행자로 업데이트하는 방법

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. 탐색 창에서 호스팅 영역(Hosted zones)을 선택합니다.
3. 호스팅 영역(Hosted Zones) 페이지에서 호스팅 영역의(라디오 버튼 대신) 이름을 선택합니다.

   > **Important**
   >
   > 동일한 이름의 호스팅 영역이 2개 이상이라면 이름 서버를 올바른 호스팅 영역에 지정할 수 있도록 주의해야 합니다.

4. 레코드 이름(Record name) 목록에서 이름 서버(Name Servers)에 나열된 4개의 서버를 기록합니다.
5. 도메인 등록 대행자가 제공하는 메서드를 사용하여 도메인 이름 서버 목록을 표시합니다.
6. 도메인 이름 서버가 4단계에서 지정한 이름 서버와 일치한다면 도메인 구성이 정확한 것입니다.

   도메인 이름 서버가 4단계에서 지정한 이름 서버와 일치하지 않는다면 Route 53 이름 서버를 사용하도록 도메인을 업데이트하세요.

7.

> **Important**
>
> 도메인 이름 서버를 Route 53 호스팅 영역의 이름 서버로 변경하더라도 실제로 변경 사항이 적용되어 Route 53가 DNS 서비스로 사용되려면 최대 2일이 걸릴 수 있습니다. 이는 인터넷을 통하는 DNS 해석기가 일반적으로 2일 1회에 한하여 이름 서버를 요청하고 응답을 캐시하기 때문입니다.

DNS 해석기가 여전히 이전 레코드 설정을 사용하고 있음

레코드의 설정을 변경하였는데도 트래픽이 여전히 웹사이트 웹 서버 같은 이전 리소스로 라우팅되고 있다면 한 가지 원인으로 DNS에 아직 이전 설정이 캐싱되어 있을 가능성이 있습니다. 레코드마다 DNS 해석기가 웹 서버의 IP 주소 같은 레코드 정보의 캐싱 시간(초)을 지정하는 TTL(Time To Live) 값이 있습니다. 따라서 DNS 해석기는 TTL 값으로 지정한 시간이 지날 때까지 계속해서 DNS 쿼리에 대한 응답으로 이전 값을 반환합니다. 레코드의 TTL 값을 알고 싶다면 다음 절차를 수행하십시오.

> **Note**
>
> 별칭 레코드의 경우 TTL은 레코드가 트래픽을 라우팅하는 AWS 리소스에 의해 결정됩니다. 자세한 내용은 별칭 또는 비 별칭 레코드 선택 단원을 참조하십시오.

레코드의 TTL을 확인하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.
2. [Hosted Zones] 페이지에서 레코드가 포함된 호스팅 영역의 이름을 선택합니다.
3. 레코드 목록에서 TTL 값을 확인하려는 레코드를 찾아서 [TTL] 열의 값을 확인합니다.

> **Note**
>
> TTL 값을 변경하더라도 변경 사항이 바로 적용되지는 않습니다. DNS 해석기에 이미 TTL 값이 캐싱되어 있으며, 이전 설정에서 지정한 시간이 지날 때까지는 새로운 설정이 적용되지 않기 때문입니다.

이름이 같은 호스팅 영역이 두 개 이상 있고 도메인에 연결되지 않은 호스팅 영역을 업데이트함

동일한 계정을 사용하거나 여러 계정을 사용하여 이름이 같은 호스팅 영역을 두 개 이상 생성할 수 있습니다. Route 53가 도메인의 인터넷 트래픽을 라우팅하는 데 사용하는 호스팅 영역을 지정하려면 해당 호스팅 영역의 Route 53 이름 서버 4개를 가져오고 이러한 이름 서버를 사용하도록 도메인 등록을 업데이트합니다.

한 호스팅 영역에서 레코드를 추가, 변경 또는 삭제하더라도 도메인 등록에 다른 호스팅 영역의 이름 서버가 사용되는 경우 DNS 쿼리에 대한 Route 53 응답에 변경 사항이 반영되지 않습니다. 레코드를 업데이트한 호스팅 영역의 이름 서버가 도메인 등록에 사용되고 있는지 확인하려면 다음 작업을 수행합니다.

1. 도메인 등록에 연결된 이름 서버를 확인합니다. 이름 서버 또는 글루 레코드 추가 또는 변경을 참조하세요.
2. 1단계에서 가져온 이름 서버를 레코드를 업데이트한 호스팅 영역에 Route 53에서 할당한 이름 서버와 비교합니다. 퍼블릭 호스팅 영역에 대한 이름 서버 가져오기을 참조하세요.

도메인 등록의 이름 서버가 레코드를 업데이트한 호스팅 영역의 이름 서버와 일치하지 않는 경우 다음 두 가지 방법을 사용할 수 있습니다.

도메인에 현재 연결된 호스팅 영역의 레코드 변경(권장)

현재 도메인 등록에 연결되지 않은 호스팅 영역에서 변경한 사항을 기록해 둡니다. 그런 다음 도메인 등록에 연결된 호스팅 영역으로 이동하여 동일한 변경을 수행합니다. 변경 사항이 거의 즉시 적용되기 때문에 이 방법이 권장됩니다. 자세한 내용은 레코드 편집 단원을 참조하십시오.

도메인 등록을 업데이트하여 다른 이름 서버 사용

도메인 등록을 변경하여 업데이트한 호스팅 영역의 이름 서버를 사용합니다.

> **Important**
>
> 도메인 등록에 연결된 이름 서버를 변경하면 최대 2일 동안 인터넷에서 도메인을 사용할 수 없습니다. DNS 해석기가 보통 2일 동안 이름 서버의 이름을 캐시하기 때문입니다. 해석기 캐싱 관련 정보를 포함하여 DNS 작동 방식에 대한 개요는 Amazon Route 53가 도메인의 트래픽을 라우팅하는 방법 단원을 참조하십시오.

도메인 등록에 연결된 이름 서버를 변경하면 기본적으로 도메인의 DNS 서비스가 변경됩니다. 도메인이 현재 사용 중인지 여부에 따라 두 가지 옵션이 있습니다.

- 도메인이 사용 중인 경우 Route 53를 사용 중인 도메인에 대한 DNS 서비스로 설정 단원을 참조하십시오.
- 도메인이 현재 비활성 상태인 경우 다음 작업을 수행합니다.
  1. 트래픽을 도메인으로 라우팅하는 데 사용할 호스팅 영역의 이름 서버를 가져옵니다. 퍼블릭 호스팅 영역에 대한 이름 서버 가져오기을 참조하세요.
  2. 1단계에서 이름 서버를 가져온 호스팅 영역에서 NS 레코드가 동일한 4개의 이름 서버를 사용하고 있는지 확인합니다. 그렇지 않은 경우 NS 레코드를 업데이트합니다. 레코드 편집을 참조하세요.
  3. 1단계에서 가져온 이름 서버를 사용하도록 도메인 등록을 업데이트합니다. 이름 서버 또는 글루 레코드 추가 또는 변경을 참조하세요.

내 브라우저에 "Server not found" 오류 표시

도메인(example.com) 또는 서브도메인(www.example.com)으로 이동할 때 브라우저에 "Server not found" 오류가 표시되면 몇 가지 공통적인 이유가 있습니다.

주제

- 도메인 또는 서브도메인 이름에 레코드를 생성하지 않았습니다
- 레코드를 생성하였지만 잘못된 값을 지정함
- 트래픽을 라우팅할 리소스를 사용할 수 없음

도메인 또는 서브도메인 이름에 레코드를 생성하지 않았습니다

도메인 또는 서브도메인에 레코드를 생성하지 않으면 사용자가 브라우저에 해당 이름을 입력하더라도 DNS가 트래픽을 어디로 라우팅해야 할지 모릅니다. 자세한 내용은 레코드 작업 단원을 참조하십시오.

레코드를 생성하였지만 잘못된 값을 지정함

레코드를 생성하는 경우 웹 서버의 IP 주소나 CloudFront가 웹 배포에 할당한 도메인 이름 등을 잘못된 값으로 지정하기 쉽습니다. 레코드가 존재하는데도 "Server not found" 오류가 계속 표시되는 경우에는 값이 올바른지 확인하는 것이 좋습니다.

트래픽을 라우팅할 리소스를 사용할 수 없음

레코드가 사용할 수 없는 웹 서버 같은 리소스를 지정하면 브라우저가 "Server not found" 오류를 반환합니다. 이때는 트래픽을 라우팅할 리소스의 상태를 확인하는 것이 좋습니다.

웹사이트 호스팅에 구성된 Amazon S3 버킷에 트래픽을 라우팅할 수 없음

웹사이트 호스팅에 Amazon S3 버킷을 구성하는 경우 트래픽을 버킷으로 라우팅할 때 사용할 레코드와 동일한 이름을 버킷에 지정해야 합니다. 예를 들어 example.com의 트래픽을 웹사이트 호스팅에 구성된 S3 버킷으로 라우팅하려면 버킷 이름 역시 example.com이 되어야 합니다.

웹 사이트 호스팅용으로 구성된 S3 버킷으로 트래픽을 라우팅하려는 경우 버킷 이름이 Amazon Route 53 콘솔의 별칭 대상 목록에 표시되지 않거나 프로그래밍 방식으로 별칭 레코드를 생성하려고 하는데 Route 53 API, AWS SDKs, AWS CLI또는에서 InvalidInput 오류가 발생하는 경우 다음을 AWS Tools for Windows PowerShell확인합니다.

- 버킷 이름이 레코드 이름(예: example.com, www.example.com)과 정확히 일치합니다.
- S3 버킷이 웹사이트 호스팅에 올바로 구성되어 있습니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3에서 정적 웹 사이트 호스팅을 참조하십시오.

같은 호스팅 영역에 대해 요금이 두 번 청구됨

호스팅 영역을 생성한 후 12시간 이내에 삭제할 경우 요금이 청구되지 않습니다. 12시간이 경과하면 호스팅 영역에 대한 표준 월간 요금이 부과됩니다. 호스팅 영역 월간 요금은 일할 계산되지 않습니다. (도메인을 등록하면 자동으로 생성되는 호스팅 영역에도 동일한 요금이 적용됩니다.)

월말(예: 1월 31일)에 호스팅 영역을 생성할 경우 2월 인보이스에 2월 요금과 함께 1월 요금이 표시될 수 있습니다. Amazon Route 53는 호스팅 영역이 생성된 시간을 결정하기 위해 협정 세계시(UTC)를 시간대로 사용합니다.

도메인에 대해 여러 개의 인보이스 청구

구독에 가입하거나 등록 요금, 이전 요금 또는 선결제 비용이 포함된 갱신 요금을 지불할 때 고유한 청구서가 생성됩니다. 결제 트랜잭션이 실패하더라도 이 청구서는 청구 콘솔에 남아 있습니다. 관련 결제 청구 라인의 항목은 청구 콘솔의 서비스별 청구 세부 정보 탭의 Registrar-Global 하위 섹션에 [x] 수량으로 표시됩니다.

면제된 청구서를 보려면 다음 단계를 완료하세요.

청구 콘솔에서 면제된 청구서를 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/costmanagement/ AWS Billing and Cost Management 콘솔을 엽니다.
2. 탐색 창에서 청구서(Bills)를 선택합니다.
3. 면제된 청구서에 대한 세부 정보를 보려면 청구서를 선택합니다.

청구 콘솔에서 결제 및 환불 성공 내역을 보려면 다음 단계를 완료하세요.

성공적으로 처리된 결제 또는 환불을 확인하려면

1. 탐색 창에서 결제(Payments)를 선택합니다.
2. 트랜잭션 탭을 선택하여 완료된 모든 트랜잭션에 대한 트랜잭션 테이블을 봅니다 AWS.

내 AWS 계정이 닫히거나 영구적으로 닫히고 내 도메인이 Route 53에 등록됨

AWS 계정을 해지하거나 계정이 해지되거나 영구적으로 해지되는 경우 도메인은 삭제 프로세스를 거칩니다.

1. 계정이 폐쇄되고 해당 도메인이 향후 5일 이내에 매일 일시 중지됨을 알려드립니다.
2. 도메인이 일시 중지되면 다음이 수행됩니다.
   - 등록 기관이 Amazon Registrar인 경우 30일 후에 도메인을 삭제한다는 알림을 전송합니다. 자세한 내용은 등록 기관 및 도메인에 대한 기타 정보 찾기 단원을 참조하십시오.
   - 등록 기관이 Gandi인 경우 계정이 영구적으로 폐쇄되면 도메인이 Gandi에 릴리스된다는 알림을 전송합니다.
3. 30일을 기다린 후 계정에서 Amazon Registrar에 등록된 모든 도메인을 삭제하고 업데이트 내용을 전달합니다.
4. 계정이 영구적으로 폐쇄되면 계정에서 Gandi에 등록된 모든 도메인을 Gandi에 릴리스합니다.

도메인을 복구할 수 있는 기간 동안 계정을 다시 열면 도메인 일시 중지가 취소되거나 도메인이 삭제되었지만 복원될 수 있음을 알려줍니다. 자세한 내용은 Amazon Route 53에 등록할 수 있는 도메인 단원을 참조하십시오.

> **Note**
>
> 계정을 해지한 날로부터 90일이 지나면 더 이상 계정을 다시 열 수 없습니다. 자세한 내용은 AWS 계정 관리 설명서의 계정 폐쇄를 참조하세요.

자세한 내용은 도메인 등록 문제에 대한 AWS 지원 문의 단원을 참조하십시오.

Amazon Route 53 서버의 IP 주소 범위

Amazon Web Services(AWS)는 현재 IP 주소 범위를 JSON 형식으로 게시합니다. 방화벽이나 보안 그룹이 소스 IP 주소를 기반으로 들어오는 트래픽을 제한하는 경우 구성에서 해당 IP 주소 범위의 트래픽을 허용하는지 확인합니다.

Route 53의 현재 IP 주소 범위를 보려면, ip-ranges.json을 다운로드하고 파일에서 다음 값을 검색합니다.

- `"service": "ROUTE53"`
- `"service": "ROUTE53_HEALTHCHECKS"`
- `"service": "ROUTE53_HEALTHCHECKS_PUBLISHING"`

AWS 리소스의 IP 주소에 대한 자세한 내용은의 AWS IP 주소 범위를 참조하세요Amazon Web Services 일반 참조.

Route 53 이름 서버의 IP 주소 범위

`"service": "ROUTE53"` – 이러한 IP 주소 범위는 Route 53 이름 서버에서 사용됩니다. Route 53를 하나 이상의 도메인에 대한 DNS 서비스로 사용하고 `dig` 또는 `nslookup` 명령을 사용하여 Route 53 이름 서버를 쿼리할 수 있도록 하려면 이러한 범위를 허용된 IP 주소 범위 목록에 추가합니다.

> **Note**
>
> Amazon은 이름 서버의 IP 주소를 거의 변경하지 않으며, IP 주소를 변경해야 하는 경우 미리 알려 드립니다.

Route 53 상태 확인의 IP 주소 범위

`"service": "ROUTE53_HEALTHCHECKS"` - 이러한 IP 주소 범위는 Route 53 상태 확인 검사기에서 사용됩니다. Route 53 상태 확인을 사용하여 네트워크의 리소스 상태를 확인하는 경우 허용된 IP 주소 범위 목록에 이러한 범위를 추가합니다.

> **Note**
>
> Amazon은 상태 검사기의 IP 주소 범위를 거의 변경하지 않으며, IP 주소 범위를 변경해야 하는 경우 미리 알려 드립니다.

상태 확인을 위한 IP 주소에 대한 자세한 내용은 Amazon Route 53 상태 확인을 위한 라우터 및 방화벽 규칙 구성 단원을 참조하세요.

접두사 목록 참조

접두사 목록은 보안 그룹을 구성하는 데 사용할 수 있는 하나 이상의 CIDR 블록 항목 세트입니다. Amazon EC2 인스턴스 규칙 라우터 및 방화벽은 Route 53 상태 확인 검사기가 사용하는 IP 주소에서 오는 인바운드 트래픽을 반드시 허용해야 합니다. 접두사 목록을 참조하면 규칙의 CIDR 블록 관리를 단순화할 수 있습니다. 여러 규칙 간에 동일한 CIDR을 자주 사용하는 경우 각 규칙의 동일한 CIDR을 반복적으로 참조하는 대신 단일 접두사 목록의 해당 CIDR을 관리할 수 있습니다. 대상 CIDR 블록을 제거해야 하는 경우 영향을 받는 모든 규칙에서 CIDR을 제거하는 대신 접두사 목록에서 해당 항목을 제거할 수 있습니다. 일반적인 접두사 목록에 대한 자세한 내용을 알아보려면 Amazon VPC 사용 설명서의 관리형 접두사 목록을 사용하여 CIDR 블록 그룹화를 참조하세요.

AWS관리형 접두사 목록은 AWS 서비스의 IP 주소 범위 집합입니다. AWS관리형 접두사 목록은에서 생성 AWS 및 유지 관리하며 AWS 계정이 있는 모든 사용자가 사용할 수 있습니다. AWS관리형 접두사 목록은 생성, 수정, 공유 또는 삭제할 수 없습니다.

AWS관리형 접두사 목록에 대한 자세한 내용은 Amazon VPC 사용 설명서의 AWS관리형 접두사 목록 작업을 참조하세요.

Route 53 상태 확인의 내부 IP 주소 범위

`"service": "ROUTE53_HEALTHCHECKS_PUBLISHING"` - Route 53는 이러한 IP 주소 범위를 내부적으로만 사용합니다. 허용된 범위 목록에 이러한 범위를 추가할 필요는 없습니다.

Amazon Route 53 리소스 태그 지정

태그는 AWS 리소스에 할당하는 레이블입니다. 각 태그는 사용자가 정의하는 키와 값으로 구성됩니다. 예를 들어, 키는 "도메인"이고 값은 "example.com"일 수 있습니다. 다양한 목적으로 태그를 사용할 수 있으며, 일반적인 용도 중 하나는 Amazon Route 53 비용을 분류하고 추적하는 것입니다. Route 53 호스팅 영역, 도메인 및 상태 확인에 태그를 적용하면는 사용 및 비용이 태그로 집계된 CSV(쉼표로 구분된 값) 파일로 비용 할당 보고서를 AWS 생성합니다. 비즈니스 범주를 나타내는 태그(예: 비용 센터, 애플리케이션 이름 또는 소유자)를 적용하여 여러 서비스에 대한 비용을 정리할 수 있습니다. 비용 할당 태그 사용에 대한 자세한 내용은 AWS Billing 사용 설명서의 비용 할당 태그 사용을 참조하십시오.

사용 편의성과 최상의 결과를 위해 AWS Management Console에서 태그 편집기를 사용하세요. 태그를 생성하고 관리하는 중앙 통합 방법을 제공합니다. 자세한 내용은 AWS Management Console시작하기에서 태그 편집기로 작업을 참조하세요. Route 53 콘솔을 사용하여 일부 리소스의 태그를 적용할 수도 있습니다.

- 상태 확인 - 자세한 내용은 상태 확인에 대한 이름 및 태그 지정 섹션을 참조하세요.
- Route 53 Resolver 인바운드 엔드포인트— 자세한 내용은 인바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값 섹션을 참조하세요.
- Resolver 아웃바운드 엔드포인트 - 자세한 내용은 아웃바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값 섹션을 참조하세요.
- Resolver 규칙 - 자세한 내용은 규칙을 생성 또는 편집할 때 지정하는 값 섹션을 참조하세요.
- 호스팅 영역 – 자세한 내용은 호스팅 영역 작업 섹션을 참조하세요.

> **Note**
>
> Resolver 엔드포인트에 대한 요금은 Resolver 네트워크 인터페이스별로 할당됩니다. 현재 Resolver 네트워크 인터페이스에 태그를 지정할 수 없으므로 현재 Resolver 엔드포인트에 태그 기반 비용 할당이 지원되지 않습니다. Resolver 요금에 대한 자세한 내용은 Amazon Route 53 요금 섹션을 참조하세요.

Route 53 API를 사용하여 리소스에 태그를 적용할 수도 있습니다. 자세한 내용은 Amazon Route 53 API 참조의 기능별 Route 53 API 작업 주제에서 태그 관련 작업을 참조하세요.

자습서

이 섹션은 다음 자습서를 다룹니다.

하위 도메인의 DNS 서비스로 Route 53 사용

Route 53를 새 하위 도메인 또는 기존 하위 도메인의 DNS 서비스로 사용하면서 상위 도메인에는 다른 DNS 서비스를 사용하는 방법을 알아봅니다.

지연 시간 기반 라우팅으로 전환

Route 53에서 표준 라우팅에서 지연 시간 기반 라우팅으로 점진적으로 마이그레이션하여 사용자를 사용 가능한 가장 짧은 지연 시간 AWS 엔드포인트로 안내하는 방법을 알아봅니다.

가중치 기반 레코드 및 지연 시간 레코드를 결합하여 전체 제어 및 롤백 기능과 함께 원활하고 위험이 낮은 전환을 수행합니다.

지연 시간 기반 라우팅에 다른 리전 추가

새 AWS 리전을 추가하고 트래픽을 새 리전으로 점진적으로 전환하여 지연 시간 기반 라우팅 설정을 확장합니다.

리전의 여러 Amazon EC2 인스턴스로 트래픽 라우팅

지연 시간 레코드 및 가중치 기반 레코드를 함께 사용하여 트래픽을 특정 AWS 리전내의 여러 Amazon EC2 인스턴스로 라우팅합니다.

100건이 넘는 가중치 적용 레코드 관리

가중치 기반 별칭 레코드 및 가중치 기반 레코드의 트리를 생성하여 트래픽을 100개 이상의 엔드포인트로 보내는 방법을 알아봅니다.

내결함성 멀티 레코드 응답 가중치 부여

여러 레코드가 포함된 DNS 응답의 가중치를 지정하여 여러 엔드포인트에서 내결함성과 로드 밸런싱을 제공하는 방법을 이해합니다.

이 자습서에서는 다양한 사용 사례와 시나리오를 다루므로 Route 53의 라우팅 정책, 가중치 기반 레코드, 지연 시간 기반 라우팅을 효과적으로 활용하여 DNS 관리 및 트래픽 라우팅을 최적화하는 데 도움이 됩니다.

주제

- 상위 도메인을 마이그레이션하지 않고 Amazon Route 53를 하위 도메인에 대한 DNS 서비스로 사용
- Transitioning to latency-based routing in Amazon Route 53
- Amazon Route 53의 지연 시간 기반 라우팅에 다른 리전 추가
- Amazon Route 53의 지연 시간 및 가중치 기반 레코드를 사용하여 한 리전의 여러 Amazon EC2 인스턴스로 트래픽 라우팅
- Amazon Route 53에서 100개 이상의 가중치 기반 레코드 관리
- Amazon Route 53에서 내결함성 멀티 레코드 응답 가중치 부여

상위 도메인을 마이그레이션하지 않고 Amazon Route 53를 하위 도메인에 대한 DNS 서비스로 사용

Amazon Route 53는 하위 도메인에 대한 DNS를 유연하게 관리하므로 전체 상위 도메인을 마이그레이션할 필요 없이 해당 기능을 활용할 수 있습니다.

상위 도메인을 다른 DNS 서비스 공급자와 호스팅된 상태로 유지하면서 새 하위 도메인을 생성하거나 기존 하위 도메인을 Route 53으로 마이그레이션할 수 있습니다.

Route 53를 사용하여 새 하위 도메인 생성:

1. 새 하위 도메인에 대한 호스팅 영역을 생성합니다.
2. 하위 도메인에 대해 원하는 DNS 레코드(예: A, CNAME, MX)를 호스팅 영역에 추가합니다.
3. 호스팅 영역에 할당된 Route 53 이름 서버를 가져옵니다.
4. 하위 도메인의 NS(이름 서버) 레코드를 추가하여 Route 53 이름 서버를 가리키도록 상위 도메인의 DNS 구성을 업데이트합니다.

기존 하위 도메인을 Route 53으로 마이그레이션:

1. 하위 도메인에 대한 호스팅 영역을 생성합니다.
2. 기존 DNS 서비스 공급자로부터 하위 도메인에 대한 현재 DNS 구성을 가져옵니다.
3. 호스팅 영역에 해당 DNS 레코드를 추가합니다.
4. 호스팅 영역에 할당된 Route 53 이름 서버를 가져옵니다.
5. 하위 도메인의 NS 레코드를 추가하여 Route 53 이름 서버를 가리키도록 상위 도메인의 DNS 구성을 업데이트합니다.

다음 단계에 따라 하위 도메인에 대해 상태 확인, 라우팅 정책, 트래픽 흐름 관리와 같은 Route 53의 고급 기능을 활용하는 동시에 기존 공급자와 상위 도메인의 DNS 구성을 유지할 수 있습니다.

주제

- 상위 도메인을 마이그레이션하지 않고 Amazon Route 53을 DNS 서비스로 사용하는 하위 도메인 생성하기
- 상위 도메인을 마이그레이션하지 않고 하위 도메인에 대한 DNS 서비스를 Amazon Route 53으로 마이그레이션

상위 도메인을 마이그레이션하지 않고 Amazon Route 53을 DNS 서비스로 사용하는 하위 도메인 생성하기

다른 DNS 서비스로부터 상위 도메인을 마이그레이션하지 않고 Amazon Route 53을 DNS 서비스로 사용하는 하위 도메인을 생성할 수 있습니다.

이 프로세스는 다음과 같은 기본 단계로 이루어집니다.

1. 이 절차를 사용해야 할지 여부를 파악합니다.
2. 하위 도메인에 대한 Route 53 호스팅 영역을 생성합니다.
3. 새로운 하위 도메인에 대한 Route 53 호스팅 영역에 레코드를 추가합니다.
4. API 전용: 모든 Route 53 DNS 서버에 변경 사항이 전파되었는지 확인합니다.

> **Note**
>
> 현재 변경 사항의 전파 여부를 확인하는 유일한 방법은 GetChange API 작업을 사용하는 것입니다. 변경 사항은 일반적으로 60초 이내에 모든 Route 53 이름의 서버로 전파됩니다.

5. 하위 도메인의 이름 서버 레코드를 추가하여 상위 도메인에 대한 DNS 서비스를 업데이트합니다.

하위 도메인 생성에 사용할 절차 결정

이 주제에 나오는 절차에서는 일반적이지 않은 작업을 수행하는 방법을 설명합니다. Route 53을 도메인의 DNS 서비스로 이미 사용하는 경우 하위 도메인(예: www.example.com)의 트래픽을 리소스(예: EC2 인스턴스에서 실행되는 웹 서버)로 라우팅하려면 하위 도메인에 대한 트래픽 라우팅 섹션을 참조하세요.

도메인(예: example.com)의 다른 DNS 서비스를 사용하고 해당 도메인의 새 하위 도메인(예: www.example.com)의 DNS 서비스로 Route 53을 사용하려는 경우에만 이 절차를 사용합니다.

새 하위 도메인에 대한 호스팅 영역 생성

상위 도메인을 마이그레이션하지 않고 Amazon Route 53을 새 하위 도메인의 DNS 서비스로 사용하려면 먼저 하위 도메인에 대한 호스팅 영역을 생성합니다. Route 53은 호스팅 영역에 하위 도메인에 대한 정보를 저장합니다.

Route 53 콘솔을 사용하여 호스팅 영역을 생성하는 방법에 대한 자세한 내용은 퍼블릭 호스팅 영역 생성 섹션을 참조하세요.

레코드 생성

Amazon Route 53 콘솔 또는 Route 53 API를 사용하여 레코드를 생성할 수 있습니다. DNS 서비스를 하위 도메인에 대한 이름 서버 레코드로 업데이트의 설명에 따라 프로세스 후반부에 하위 도메인에 대한 책임을 Route 53에 위임한 후에는 Route 53에서 생성하는 레코드가 DNS에서 사용하는 레코드가 됩니다.

> **Important**
>
> Route 53 호스팅 영역에서 이름 서버(NS) 또는 권한 시작(SOA) 레코드를 추가로 생성하지 말고, 기존 NS 및 SOA 레코드를 삭제하지 마세요.

Route 53 콘솔을 사용하여 레코드를 생성하려면 레코드 작업 섹션을 참조하세요. Route 53 API를 사용하여 레코드를 생성하려면 `ChangeResourceRecordSets` 섹션을 참조하세요. 자세한 내용은 Amazon Route 53 API 참조의 ChangeResourceRecordSets를 참조하세요.

변경 상태 확인(API만 해당)

새 호스팅 영역을 생성하고 레코드를 변경하면 Route 53 DNS 서버로 전파되기까지 시간이 걸립니다. ChangeResourceRecordSets를 사용하여 레코드를 생성하면 `GetChange` 작업을 사용하여 변경 사항이 전파되었는지 확인할 수 있습니다. `ChangeResourceRecordSets`에서 `ChangeId`의 값을 반환하면 후속 `GetChange` 요청에 포함할 수 있습니다. 콘솔을 사용하여 레코드를 생성하면 `ChangeId`을(를) 사용할 수 없습니다. 자세한 내용은 Amazon Route 53 API 참조의 GET GetChange를 참조하세요.

> **Note**
>
> 변경 사항은 일반적으로 60초 이내에 모든 Route 53 이름의 서버로 전파됩니다.

DNS 서비스를 하위 도메인에 대한 이름 서버 레코드로 업데이트

Amazon Route 53 레코드에 대한 변경 사항이 전파된 후(변경 상태 확인(API만 해당) 참조) 하위 도메인의 NS 레코드를 추가하여 상위 도메인에 대한 DNS 서비스를 업데이트합니다. 이것을 하위 도메인에 대한 책임을 Route 53에 위임한다고 합니다. 예를 들어 상위 도메인인 example.com을 다른 DNS 서비스에서 호스팅하고 하위 도메인인 test.example.com을 Route 53에서 생성한 경우, example.com의 DNS 서비스를 test.example.com에 대한 새 NS 레코드로 업데이트해야 합니다.

다음 절차를 수행합니다.

1. DNS 서비스에서 제공하는 방법을 사용하여 상위 도메인에 대한 영역 파일을 백업하십시오.
2. Route 53 콘솔에서 Route 53 호스팅 영역에 대한 이름 서버를 가져옵니다.

   a. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.

   b. 탐색 창에서 호스팅 영역(Hosted Zones)을 클릭합니다.

   c. 호스팅 영역(Hosted zones) 페이지에서 호스팅 영역의 (이름 대신) 라디오 버튼을 선택한 다음 세부 정보 보기(View details)를 선택합니다.

   d. 호스팅 영역에 대한 세부 정보 페이지에서 호스팅 영역 세부 정보(Hosted zone details)를 선택합니다.

   e. 이름 서버(Name servers)에 나열된 서버 4개의 이름을 기록합니다.

   또는 `GetHostedZone` 작업을 사용할 수 있습니다. 자세한 내용은 Amazon Route 53 API 참조의 GetHostedZone을 참조하세요.
3. 상위 도메인의 DNS 서비스에서 제공하는 방법을 사용하여 하위 도메인의 NS 레코드를 상위 도메인의 영역 파일에 추가합니다. 이 NS 레코드에서 1단계에서 생성한 호스팅 영역과 연결된 Route 53 이름 서버 4개를 지정합니다.

> **Important**
>
> SOA(권한 시작) 레코드를 상위 도메인의 영역 파일에 추가하지 마십시오. 하위 도메인은 Route 53을 사용하기 때문에 상위 도메인에 대한 DNS 서비스는 하위 도메인에 대한 권한이 없습니다.
>
> DNS 서비스가 자동으로 하위 도메인의 SOA 레코드에 추가된 경우, 하위 도메인의 레코드를 삭제하십시오. 단, 상위 도메인에 대한 SOA 레코드는 삭제하지 마십시오.

상위 도메인을 마이그레이션하지 않고 하위 도메인에 대한 DNS 서비스를 Amazon Route 53으로 마이그레이션

상위 도메인을 다른 DNS 서비스에서 마이그레이션하지 않고 Amazon Route 53을 DNS 서비스로 사용하도록 하위 도메인을 마이그레이션할 수 있습니다.

이 프로세스는 다음과 같은 기본 단계로 이루어집니다.

1. 이 절차를 사용해야 할지 여부를 파악합니다.
2. 하위 도메인에 대한 Route 53 호스팅 영역을 생성합니다.
3. 현재 DNS 서비스 공급자로부터 상위 도메인에 대한 현재 DNS 구성을 가져옵니다.
4. 새로운 하위 도메인에 대한 Route 53 호스팅 영역에 레코드를 추가합니다.
5. API 전용: 모든 Route 53 DNS 서버에 변경 사항이 전파되었는지 확인합니다.

   > **Note**
   >
   > 현재 변경 사항의 전파 여부를 확인하는 유일한 방법은 GetChange API 작업을 사용하는 것입니다. 변경 사항은 일반적으로 60초 이내에 모든 Route 53 이름의 서버로 전파됩니다.

6. 하위 도메인의 이름 서버 레코드를 추가하여 상위 도메인에 대한 DNS 서비스 공급자로 DNS 구성을 업데이트합니다.

하위 도메인 생성에 사용할 절차 결정

이 주제에 나오는 절차에서는 일반적이지 않은 작업을 수행하는 방법을 설명합니다. Route 53을 도메인의 DNS 서비스로 이미 사용하는 경우 하위 도메인(예: www.example.com)의 트래픽을 리소스(예: EC2 인스턴스에서 실행되는 웹 서버)로 라우팅하려면 하위 도메인에 대한 트래픽 라우팅 섹션을 참조하세요.

도메인(예: example.com)의 다른 DNS 서비스를 사용하고 해당 도메인의 기존 하위 도메인(예: www.example.com)의 DNS 서비스로 Route 53을 사용하려는 경우에만 이 절차를 사용합니다.

하위 도메인에 대한 호스팅 영역 생성

상위 도메인은 마이그레이션하지 않고 하위 도메인을 다른 DNS 서비스에서 Amazon Route 53으로 마이그레이션하려면 먼저 하위 도메인에 대한 호스팅 영역을 생성합니다. Route 53은 호스팅 영역에 하위 도메인에 대한 정보를 저장합니다.

Route 53 콘솔을 사용하여 호스팅 영역을 생성하는 방법에 대한 자세한 내용은 퍼블릭 호스팅 영역 생성 섹션을 참조하세요.

DNS 서비스 공급자로부터 현재 DNS 구성 가져오기

기존 하위 도메인을 Route 53으로 간편하게 마이그레이션하려면 현재 도메인을 서비스하는 DNS 서비스 공급자로부터 도메인에 대한 현재 DNS 구성을 가져옵니다. 이 정보를 토대로 Route 53을 하위 도메인의 DNS 서비스로 구성할 수 있습니다.

요청하는 내용과 형식은 현재 이용 중인 DNS 서비스 공급자에 따라 달라집니다. 현재 구성의 모든 레코드에 대한 정보가 포함된 영역 파일을 해당 회사에서 제공하는 것이 가장 좋습니다. (레코드에서 도메인 및 하위 도메인의 트래픽을 라우팅하려는 방법에 대해 DNS에 설명합니다. 예를 들어, 웹 브라우저에 도메인 이름을 입력하는 경우 그 트래픽이 데이터 센터의 웹 서버, Amazon EC2 인스턴스, CloudFront 배포 또는 다른 위치로 라우팅되도록 하고 싶습니까?) 현재 DNS 서비스 공급자로부터 영역 파일을 가져올 수 있는 경우, 영역 파일을 편집하여 Amazon Route 53으로 마이그레이션하지 않을 레코드를 제거할 수 있습니다. 그런 다음 Route 53 호스팅 영역으로 나머지 레코드를 가져오면 프로세스가 대폭 간소해집니다. 현재 DNS 서비스 공급자에게 영역 파일 또는 레코드 목록을 얻는 방법을 문의하십시오.

레코드 생성

현재 DNS 서비스 공급자로부터 받은 레코드를 발판 삼아, 하위 도메인용으로 만든 Amazon Route 53 호스팅 영역에서 해당하는 레코드를 생성합니다. DNS 서비스를 하위 도메인에 대한 이름 서버 레코드로 업데이트의 설명에 따라 프로세스 후반부에 하위 도메인에 대한 책임을 Route 53에 위임한 후에는 Route 53에서 생성하는 레코드가 DNS에서 사용하는 레코드가 됩니다.

> **Important**
>
> Route 53 호스팅 영역에서 이름 서버(NS) 또는 권한 시작(SOA) 레코드를 추가로 생성하지 말고, 기존 NS 및 SOA 레코드를 삭제하지 마세요.

Route 53 콘솔을 사용하여 레코드를 생성하려면 레코드 작업 섹션을 참조하세요. Route 53 API를 사용하여 레코드를 생성하려면 ChangeResourceRecordSets 섹션을 참조하세요. 자세한 내용은 Amazon Route 53 API 참조의 ChangeResourceRecordSets를 참조하세요.

변경 상태 확인(API만 해당)

새 호스팅 영역을 생성하고 레코드를 변경하면 Route 53 DNS 서버로 전파되기까지 시간이 걸립니다. ChangeResourceRecordSets를 사용하여 레코드를 생성하면 GetChange 작업을 사용하여 변경 사항이 전파되었는지 확인할 수 있습니다. ChangeResourceRecordSets에서 ChangeId의 값을 반환하면 후속 GetChange 요청에 포함할 수 있습니다. 콘솔을 사용하여 레코드를 생성하면 ChangeId을(를) 사용할 수 없습니다. 자세한 내용은 Amazon Route 53 API 참조의 GET GetChange를 참조하세요.

> **Note**
>
> 변경 사항은 일반적으로 60초 이내에 모든 Route 53 이름의 서버로 전파됩니다.

DNS 서비스를 하위 도메인에 대한 이름 서버 레코드로 업데이트

Amazon Route 53 레코드에 대한 변경 사항이 전파된 후(변경 상태 확인(API만 해당) 참조) 하위 도메인의 NS 레코드를 추가하여 상위 도메인에 대한 DNS 서비스를 업데이트합니다. 이것을 하위 도메인에 대한 책임을 Route 53에 위임한다고 합니다. 예를 들어, 상위 도메인인 example.com을 다른 DNS 서비스에서 호스팅하고 하위 도메인인 test.example.com을 Route 53으로 마이그레이션한다고 가정하겠습니다. test.example.com에 대한 호스팅 영역을 생성하고, Route 53에서 test.example.com에 대한 새 호스팅 영역에 할당한 NS 레코드로 example.com의 DNS 서비스를 업데이트해야 합니다.

다음 절차를 수행합니다.

1. DNS 서비스에서 제공하는 방법을 사용하여 상위 도메인에 대한 영역 파일을 백업하십시오.
2. 도메인의 이전 DNS 서비스 공급자에게 이름 서버의 TTL 설정을 변경할 방법이 있는 경우, 설정을 900초로 변경하는 것이 좋습니다. 이렇게 하면 클라이언트 요청에서 폐기된 이름 서버를 사용하여 도메인 이름을 해석하려고 시도하는 시간이 제한됩니다. 현재 TTL이 기본 설정인 172,800초(2일)인 경우, 해석기 및 클라이언트가 이전 TTL을 사용하여 DNS 레코드를 캐시하지 않게 되려면 이틀을 기다려야 합니다. TTL 설정이 만료된 후에는 이전 공급자에 저장된 레코드를 안전하게 삭제할 수 있으며 Route 53으로만 변경 가능합니다.
3. Route 53 콘솔에서 Route 53 호스팅 영역에 대한 이름 서버를 가져옵니다.

a. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/route53/ Route 53 콘솔을 엽니다.

b. 탐색 창에서 호스팅 영역(Hosted Zones)을 클릭합니다.

c. 호스팅 영역(Hosted zones) 페이지에서 호스팅 영역의 (이름 대신) 라디오 버튼을 선택한 다음 세부 정보 보기(View details)를 선택합니다.

d. 호스팅 영역에 대한 세부 정보 페이지에서 호스팅 영역 세부 정보(Hosted zone details)를 선택합니다.

e. 이름 서버(Name servers)에 나열된 서버 4개의 이름을 기록합니다.

또는 `GetHostedZone` 작업을 사용할 수 있습니다. 자세한 내용은 Amazon Route 53 API 참조의 GetHostedZone을 참조하세요.

4. 상위 도메인의 DNS 서비스에서 제공하는 방법을 사용하여 하위 도메인의 NS 레코드를 상위 도메인의 영역 파일에 추가합니다. NS 레코드에 하위 도메인과 같은 이름을 지정합니다. NS 레코드 값에는 2단계에서 생성한 호스팅 영역과 연결된 네 개 Route 53 이름 서버를 지정합니다. 다른 DNS 서비스에서는 다른 용어를 사용하므로 주의하십시오. 이 단계의 수행 방법을 배우기 위해 DNS 서비스에 기술 지원을 문의해야 할 수도 있습니다.

> **Important**
>
> SOA(권한 시작) 레코드를 상위 도메인의 영역 파일에 추가하지 마십시오. 하위 도메인은 Route 53을 사용하기 때문에 상위 도메인에 대한 DNS 서비스는 하위 도메인에 대한 권한이 없습니다.
>
> DNS 서비스가 자동으로 하위 도메인의 SOA 레코드에 추가된 경우, 하위 도메인의 레코드를 삭제하십시오. 단, 상위 도메인에 대한 SOA 레코드는 삭제하지 마십시오.

상위 도메인의 이름 서버에 대한 TTL 설정에 따라, 변경 사항이 DNS 해석기에 전파되기까지 48시간 이상이 걸릴 수 있습니다. 이 기간 동안 DNS 해석기는 계속 상위 도메인의 DNS 서비스에 대한 이름 서버로 요청에 답할 수 있습니다. 또한 클라이언트 컴퓨터는 하위 도메인에 대한 이전 이름 서버를 캐시에 계속 보관할 수 있습니다.

5. 도메인의 등록자 TTL 설정이 완료된 후(2단계 참조), 상위 도메인 영역 파일에서 다음의 레코드를 삭제합니다.

   - 레코드 생성에서 설명한 것과 같이 Route 53에 추가한 레코드입니다.

- DNS 서비스의 NS 레코드입니다. NS 레코드 삭제를 완료하면 4단계에서 생성한 NS 레코드만 영역 파일에 남게 됩니다.

Transitioning to latency-based routing in Amazon Route 53

Amazon Route 53는 지연 시간 기반 라우팅을 통해 사용자를 사용 가능한 가장 짧은 지연 시간 AWS 엔드포인트로 안내할 수 있습니다. 예를 들어 `www.example.com`과 같은 DNS 이름을 ELB Classic, Application 또는 Network Load Balancer나 Amazon EC2 인스턴스 또는 미국 동부(오하이오) 및 유럽(아일랜드) 리전에서 호스팅하는 탄력적 IP 주소와 연결할 수 있습니다. Route 53 DNS 서버는 지난 몇 주간의 네트워크 조건에 따라 특정 사용자에게 제공할 리전 및 해당 리전의 인스턴스를 결정합니다. 런던의 사용자를 유럽(아일랜드) 인스턴스로, 시카고의 사용자를 미국 동부(오하이오) 인스턴스로 보낼 가능성이 있습니다. Route 53는 A, AAAA, TXT 및 CNAME 레코드에 대한 지연 시간 기반 라우팅은 물론 A 및 AAAA 레코드에 대한 별칭도 지원합니다.

> **Note**
>
> 사용자와 리소스 간의 지연 시간에 대한 데이터는 전적으로 사용자와 AWS 데이터 센터 간의 트래픽을 기반으로 합니다. AWS 리전에서 리소스를 사용하지 않는 경우 사용자와 리소스 간의 실제 지연 시간은 AWS 지연 시간 데이터와 크게 다를 수 있습니다. 리소스가 AWS 리전과 동일한 도시에 있더라도 마찬가지입니다.

유연하고 위험 부담이 낮은 전환을 위해 가중치 기반 레코드와 지연 시간 레코드를 결합하여 스탠다드 라우팅에서 지연 시간 기반 라우팅으로 점차 마이그레이션하면서 각 단계에 완벽한 제어 및 롤백 기능을 적용할 수 있습니다. 미국 동부(오하이오) 리전의 Amazon EC2 인스턴스에서 호스팅 중인 `www.example.com`의 예를 살펴보겠습니다. 이 인스턴스에는 엘라스틱 IP 주소 `W.W.W.W`가 있습니다. 사용자를 미국 서부(캘리포니아 북부) 리전(탄력적 IP `X.X.X.X`) 및 유럽(아일랜드) 리전(탄력적 IP `Y.Y.Y.Y`)의 추가 Amazon EC2 인스턴스로 보내는 한편, 가능하면 미국 동부(오하이오) 리전으로 트래픽을 계속 라우팅하려 한다고 가정합시다. `example.com`에 대한 Route 53 호스팅 영역은 이미 유형(Type)이 A이고 값(Value)(IP 주소)이 `W.W.W.W`인 `www.example.com`에 대한 레코드가 있습니다.

다음 예를 완료하면 두 개의 가중치 기반 별칭 레코드가 구성됩니다.

- `www.example.com`에 대한 기존의 레코드를 가중치 기반 별칭 레코드로 변환하여 대부분의 트래픽을 미국 동부(오하이오) 리전에서 기존의 Amazon EC2 인스턴스로 계속 보냅니다.
- 처음에는 트래픽의 일부분만 지연 시간 레코드로 보내는 가중치 기반 별칭 레코드를 하나 더 생성하여 트래픽을 세 리전 모두로 라우팅합니다.

이러한 가중치 기반 별칭 레코드의 가중치를 업데이트하여 미국 동부(오하이오) 리전으로만 트래픽을 라우팅하는 것에서 Amazon EC2 인스턴스가 있는 세 리전 모두로 트래픽을 라우팅하도록 점차 바꿀 수 있습니다.

지연 시간 기반 라우팅으로 전환하려면

1. copy-www.example.com과 같은 새로운 도메인 이름을 사용하여 www.example.com의 레코드를 복사합니다. 새 레코드에 www.example.com의 레코드와 동일한 유형(Type)(A) 및 값(Value)(W.W.W.W)을 지정합니다.
2. www.example.com에 대한 기존의 A 레코드를 업데이트하여 가중치 기반 별칭 레코드로 만듭니다.

   - 값/트래픽 라우팅 대상(Value/Route traffic to)은 이 호스팅 영역의 다른 레코드에 대한 별칭을 선택하고 copy-www.example.com을 지정합니다.
   - 가중치(Weight)는 100을 지정합니다.

   업데이트가 완료되면 Route 53는 이 레코드를 사용하여 W.W.W.W의 IP 주소가 있는 리소스로 모든 트래픽을 라우팅합니다.
3. Amazon EC2 인스턴스별로 다음과 같은 지연 시간 레코드를 생성합니다.

   - 미국 동부(오하이오), 탄력적 IP 주소(W.W.W.W)
   - 미국 서부(캘리포니아 북부), 탄력적 IP 주소(X.X.X.X)
   - 유럽(아일랜드), 탄력적 IP 주소(Y.Y.Y.Y)

   모든 지연 시간 레코드에 www-lbr.example.com 등 동일한 도메인 이름과 동일한 유형 A를 지정합니다.

   지연 시간 레코드가 생성되면 Route 53는 2단계에서 업데이트한 레코드를 사용하여 트래픽을 계속 라우팅합니다.

   각 엔드포인트가 요청을 수락하도록 하는 등 확인 테스트에 www-lbr.example.com을 사용할 수 있습니다.
4. www-lbr.example.com 지연 시간 레코드를 www.example.com 가중치 기반 레코드에 추가한 다음 제한된 트래픽을 해당하는 Amazon EC2 인스턴스로 라우팅하기 시작합니다. 이로써 미국 동부(오하이오) 리전의 Amazon EC2 인스턴스는 양쪽의 가중치 기반 레코드로부터 트래픽을 가져오게 됩니다.

www.example.com에 대한 가중치 기반 별칭 레코드를 하나 더 생성:

- 값/트래픽 라우팅 대상(Value/Route traffic to)은 이 호스팅 영역의 다른 레코드에 대한 별칭을 선택하고 www-lbr.example.com.을 지정합니다.
- 가중치(Weight)는 1을 지정합니다.

작업을 마치고 변경 사항이 Route 53 서버로 동기화된 후, Route 53는 3단계에서 지연 시간 레코드를 생성한 Amazon EC2 인스턴스로 작은 트래픽 조각(1/101)을 라우팅하기 시작합니다.

5. 엔드포인트가 수신 트래픽에 알맞게 적절히 확장된다는 확신이 생기면 그에 따라 가중치를 조정하십시오. 예를 들어 요청의 10%를 지연 시간 기반 라우팅으로 보내려면 가중치를 각각 90 및 10으로 변경합니다.

지연 시간 레코드 생성에 대한 자세한 내용은 Amazon Route 53 콘솔을 사용하여 레코드 생성 단원을 참조하십시오.

Amazon Route 53의 지연 시간 기반 라우팅에 다른 리전 추가

지연 시간 기반 라우팅을 사용 중이고 새로운 리전에 인스턴스를 추가하려는 경우, Transitioning to latency-based routing in Amazon Route 53에서 트래픽을 점차 지연 시간 기반 라우팅으로 바꾼 것과 같은 방식으로 트래픽을 새로운 리전으로 보낼 수 있습니다.

예를 들어, 지연 시간 기반 라우팅을 사용하여www.example.com의 트래픽을 라우팅하고 있으며, 아시아 태평양(도쿄)의 Amazon EC2 인스턴스를 미국 동부(오하이오), 미국 서부(캘리포니아 북부) 및 유럽(아일랜드)의 인스턴스에 추가하려 한다고 가정합시다. 다음 예시 절차는 다른 리전에 인스턴스를 추가하는 한 가지 방식을 설명하고 있습니다.

이 예제의 경우 example.com의 Amazon Route 53 호스팅 영역에는 이미 www-lbr.example.com에 대한 지연 시간 기반 레코드로 트래픽을 라우팅하는 www.example.com의 가중치 기반 별칭 레코드가 있습니다.

- 미국 동부(오하이오), 탄력적 IP 주소(W.W.W.W)
- 미국 서부(캘리포니아 북부), 탄력적 IP 주소(X.X.X.X)
- 유럽(아일랜드), 탄력적 IP 주소(Y.Y.Y.Y)

가중치 기반 별칭 레코드에는 100의 가중치가 있습니다. 지연 시간 기반 라우팅으로 전환한 후, 전환할 때 사용한 다른 가중치 기반 레코드를 삭제했다고 가정하겠습니다.

Route 53의 지연 시간 기반 라우팅에 다른 리전을 추가하려면

1. 원본 리전 세 개와 트래픽을 라우팅할 새 리전을 포함하여 새로운 지연 시간 기반 레코드 네 개를 생성합니다.

   - 미국 동부(오하이오), 탄력적 IP 주소(W.W.W.W)
   - 미국 서부(캘리포니아 북부), 탄력적 IP 주소(X.X.X.X)
   - 유럽(아일랜드), 탄력적 IP 주소(Y.Y.Y.Y)
   - 아시아 태평양(도쿄), 탄력적 IP 주소(Z.Z.Z.Z)

   모든 지연 시간 레코드에 www-lbr-2012-04-30.example.com 등 동일한 새 도메인 이름과 동일한 유형 A를 지정합니다.

   지연 시간 레코드가 생성되면 Route 53는 원래의 가중치 기반 별칭 레코드(www.example.com) 및 지연 시간 레코드(www-lbr.example.com)를 사용하여 트래픽을 계속 라우팅합니다.

   각 엔드포인트가 요청을 수락하도록 하는 등 확인 테스트에 www-lbr-2012-04-30.example.com 레코드를 사용할 수 있습니다.
2. 새로운 지연 시간 레코드에 대한 가중치 기반 별칭 레코드를 생성:

   - 기존의 가중치 기반 별칭 레코드 이름인 www.example.com을 도메인 이름으로 지정합니다.
   - 값/트래픽 라우팅 대상(Value/Route traffic to)은 이 호스팅 영역의 다른 레코드에 대한 별칭을 선택하고 www-lbr-2012-04-30.example.com을 지정합니다.
   - 가중치(Weight)는 1을 지정합니다.

   완료 후, Route 53는 1단계에서 www-lbr-2012-04-30.example.com 지연 시간 레코드를 생성한 Amazon EC2 인스턴스로 작은 트래픽 조각(1/101)을 라우팅하기 시작합니다. 트래픽의 나머지 부분은 아시아 태평양(도쿄) 리전에 Amazon EC2 인스턴스가 없는 www-lbr.example.com 지연 시간 레코드로 계속 라우팅됩니다.
3. 엔드포인트가 수신 트래픽에 알맞게 적절히 확장된다는 확신이 생기면 그에 따라 가중치를 조정하십시오. 예를 들어 요청의 10%를 도쿄 리전이 포함된 지연 시간 레코드로 라우팅하려면 www-lbr.example.com의 가중치를 100에서 90으로, www-lbr-2012-04-30.example.com의 가중치를 1에서 10으로 변경합니다.

레코드 생성에 대한 자세한 내용은 Amazon Route 53 콘솔을 사용하여 레코드 생성 단원을 참조하십시오.

Amazon Route 53의 지연 시간 및 가중치 기반 레코드를 사용하여 한 리전의 여러 Amazon EC2 인스턴스로 트래픽 라우팅

Amazon EC2 리전 둘 이상의 Amazon EC2 인스턴스에서 애플리케이션을 실행 중이고 하나 이상의 리전에 둘 이상의 Amazon EC2 인스턴스가 있는 경우, 지연 시간 기반 라우팅을 사용하여 정확한 리전으로 트래픽을 라우팅할 수 있습니다. 그런 다음 가중 레코드를 사용하여 지정한 가중치에 따라 리전 내 인스턴스로 트래픽을 라우팅합니다.

예를 들어, 미국 동부(오하이오) 리전에 탄력적 IP 주소의 Amazon EC2 인스턴스가 세 개 있고 미국 동부(오하이오) 리전에 속하는 사용자를 위해 세 IP 모두에 균등하게 요청을 배포하려 한다고 가정합시다. 한 번에 여러 리전에 같은 기술을 적용할 수 있지만, 다른 리전에서는 Amazon EC2 인스턴스 하나면 충분합니다.

Amazon Route 53의 지연 시간 및 가중치 기반 레코드를 사용하여 한 리전의 여러 Amazon EC2 인스턴스로 트래픽 라우팅하려면

1. 리전에서 Amazon EC2 인스턴스에 대한 가중치 기반 레코드 그룹을 생성합니다. 다음 사항에 유의하세요.

   - 각 가중치 기반 레코드에 이름(Name)(예: `us-east.example.com`) 및 유형(Type)과 같은 값을 지정합니다.
   - 값/트래픽 라우팅 대상은 IP 주소 또는 레코드 유형에 따라 다른 값을 선택하고, 탄력적 IP 주소 중 하나의 값을 지정합니다.
   - Amazon EC2 인스턴스에 동등하게 가중치를 주려는 경우, 가중치(Weight)에 대한 값을 지정합니다.
   - 각 레코드에 대한 [Set ID]의 고유 값을 지정합니다.

   가중치 기반 레코드에 대한 자세한 내용은 가중치 기반 라우팅 단원을 참조하십시오.
2. 다른 리전에 여러 Amazon EC2 인스턴스가 있는 경우, 해당 리전에 대한 1단계를 반복합니다. 각 리전에서 [Name]에 대한 다른 값을 지정합니다.
3. 여러 Amazon EC2 인스턴스가 있는 각 리전에 대해(예: 미국 동부(오하이오)) 지연 시간 별칭 레코드를 생성합니다. 값/트래픽 라우팅 대상(Value/Route traffic to)에 이 호스팅 영역의 다른 레코드에 대한 별칭(Alias to another record in this hosted zone)을 선택하고, 해당 리전의 가중 레코드에 할당한 레코드 이름(Record name) 필드(예: `us-east.example.com`)의 값을 지정합니다.
4. Amazon EC2 인스턴스 한 개가 있는 각 리전에 대해 지연 시간 레코드를 생성합니다. 레코드 이름(Record name)은 3단계에서 생성한 지연 시간 별칭 레코드와 동일한 값을 지정합니다. 값/트래

픽 라우팅 대상(Value/Route traffic to)은 IP 주소 또는 레코드 유형에 따라 다른 값(IP address or another value depending on the record type)을 선택하고, 해당 리전에 있는 Amazon EC2 인스턴스의 탄력적 IP 주소를 지정합니다.

Amazon EC2 인스턴스의 별칭 레코드 추가에 대한 자세한 내용은 Amazon EC2 인스턴스로 트래픽 라우팅 단원을 참조하십시오.

레코드 생성에 대한 자세한 내용은 Amazon Route 53 콘솔을 사용하여 레코드 생성 단원을 참조하십시오.

Amazon Route 53에서 100개 이상의 가중치 기반 레코드 관리

Amazon Route 53를 통해 가중치 기반 레코드를 구성할 수 있습니다. 주어진 이름 및 유형(예: `www.example.com`, 유형 A)에 각각 가중치가 있는 최대 100개의 대체 응답을 구성할 수 있습니다. `www.example.com`에 대한 쿼리에 응답할 때 Route 53 DNS 서버는 DNS 해석기에 반환하기 위한 임의 가중치 기반 응답을 선택합니다. 2의 가중치가 있는 가중치 기반 레코드 값은 평균적으로 1의 가중치가 있는 가중치 기반 레코드 값과 마찬가지로 두 번 반환됩니다.

100개 이상의 엔드포인트로 트래픽을 보내려면 가중치 기반 별칭 레코드 및 가중치 기반 레코드의 트리를 사용할 수 있습니다. 예를 들어, 트리의 첫 번째 “수준”은 최대 100개의 가중치 기반 별칭 레코드일 수 있으며, 별칭 레코드 각각은 최대 100개의 가중치 기반 레코드를 차례로 가리킬 수 있습니다. Route 53에서는 최대 3가지 수준의 재귀를 허용하므로 최대 1,000,000개의 고유한 가중치 기반 엔드포인트를 관리할 수 있습니다.

간단한 2단계 트리의 모습은 다음과 같습니다.

가중치 기반 별칭 레코드

- 가중치 1의 `www-a.example.com`에 대한 `www.example.com` 별칭
- 가중치 1의 `www-b.example.com`에 대한 `www.example.com` 별칭

가중치 기반 레코드

- `www-a.example.com`, 유형 A, 값 192.0.2.1, 가중치 1
- `www-a.example.com`, 유형 A, 값 192.0.2.2, 가중치 1

- `www-b.example.com`, 유형 A, 값 192.0.2.3, 가중치 1

- www-b.example.com, 유형 A, 값 192.0.2.4, 가중치 1

레코드 생성에 대한 자세한 내용은 레코드 작업 단원을 참조하십시오.

Amazon Route 53에서 내결함성 멀티 레코드 응답 가중치 부여

> **Note**
>
> 다중 응답 라우팅 정책을 사용하는 레코드는 이 자습서에서 설명하는 구성과 거의 비슷하게 동작합니다. 주된 차이점은 자습서 구성에서는 가중치를 지정할 수 있다는 점입니다. 이는 엔드포인트 용량이 서로 다를 때 유용할 수 있습니다. 자세한 내용은 다중값 응답 라우팅 단원을 참조하십시오.

Amazon Route 53 가중치 기반 레코드는 오직 하나의 레코드와 연결할 수 있습니다. 즉, 이름 하나(예: example.com)와 레코드 유형 하나(예: A)만 조합할 수 있습니다. 그러나 여러 레코드가 포함된 DNS 응답에 가중치를 부여하는 것이 바람직한 경우가 많습니다.

예를 들어, 서비스의 탄력적 IP 엔드포인트 또는 Amazon EC2 인스턴스가 여덟 개 있을 수 있습니다. 해당 서비스의 클라이언트가 일반적인 브라우저와 같이 연결 재시도를 지원하는 경우, DNS 응답에 IP 주소 여러 개를 제시하면 특정 엔드포인트에 장애가 있을 때 그러한 클라이언트에게 대체 엔드포인트를 제시할 수 있습니다. 둘 이상의 가용 영역에서 호스팅하는 IP 조합을 넣어 응답을 구성하는 경우, 가용 영역의 장애까지 대비할 수 있습니다.

멀티 레코드 응답은 다수의 클라이언트(예: 모바일 웹 애플리케이션)가 작은 DNS 캐시 세트를 공유할 때도 유용합니다. 이 경우, 클라이언트는 공유 캐시에서 일반적인 DNS 응답을 받았더라도 멀티 레코드 응답을 토대로 요청을 여러 엔드포인트로 보낼 수 있습니다.

이러한 유형의 가중치 기반 멀티 레코드 응답은 레코드와 가중치 기반 별칭 레코드의 조합을 사용하여 얻을 수 있습니다. 엔드포인트 여덟 개를 각각 IP 주소 네 개를 포함하는 레코드 세트 두 그룹으로 나눌 수 있습니다.

다음 값을 가진 endpoint-a.example.com, 유형 A

- 192.0.2.1
- 192.0.2.2
- 192.0.2.128
- 192.0.2.129

다음 값을 가진 `endpoint-b.example.com`, 유형 A

- 192.0.2.3
- 192.0.2.4
- 192.0.2.130
- 192.0.2.131

그런 다음 각 그룹을 가리키는 가중치 기반 별칭 레코드를 생성할 수 있습니다.

- `endpoint-a.example.com`에 대한 `www.example.com` 별칭, 유형 A, 가중치 1
- `endpoint-b.example.com`에 대한 `www.example.com` 별칭, 유형 A, 가중치 1

레코드 생성에 대한 자세한 내용은 레코드 작업 단원을 참조하십시오.

Amazon Route 53 모범 사례

이 섹션에서는 다음을 포함하여 Amazon Route 53의 다양한 구성 요소에 대한 모범 사례를 제공합니다.

1. DNS 모범 사례:
   - TTL(Time to Live) 값과 응답성 대 신뢰성 간의 균형을 이해합니다.
   - 성능 개선 및 비용 절감을 위해 가능하면 CNAME 레코드 대신 별칭 레코드를 사용합니다.
   - 모든 클라이언트가 응답을 받도록 기본 라우팅 정책을 구성합니다.
   - 지연 시간 기반 라우팅을 활용하여 애플리케이션 지연 시간 및 지리적 위치/지리 근접성 라우팅을 최소화하고 안정성과 예측성을 높입니다.
   - 자동화된 워크플로용 `GetChange` API를 사용하여 변경 전파를 확인합니다.
   - 일관된 라우팅을 위해 상위 영역에서 하위 도메인을 위임합니다.
   - 다중 값 응답 라우팅을 사용하여 대규모 단일 응답을 피합니다.
2. Resolver 모범 사례:
   - 동일한 VPC를 Resolver 규칙 및 인바운드 엔드포인트와 연결하지 않게 하여 라우팅 루프를 방지합니다.
   - 보안 그룹 규칙을 구현하여 연결 추적 오버헤드를 줄이고 쿼리 처리량을 극대화합니다.
   - 중복을 위해 여러 가용 영역에 IP 주소를 사용하여 인바운드 엔드포인트를 구성합니다.
   - 잠재적 DNS 영역 보행 공격에 유의하고 엔드포인트에 제한이 발생하는 경우 AWS Support에 문의하세요.
3. 상태 확인 모범 사례:
   - Amazon Route 53 상태 확인을 최적화하기 위한 권장 사항을 준수하여 리소스를 안정적으로 모니터링

이러한 모범 사례를 준수하면 DNS 인프라의 성능, 안정성, 보안을 최적화하여 애플리케이션과 서비스로 트래픽을 효율적이고 효과적으로 라우팅할 수 있습니다.

주제

Amazon Route 53 DNS 모범 사례

다음 모범 사례를 따르면 Amazon Route 53 DNS 서비스를 사용할 때 최상의 결과를 얻을 수 있습니다.

DNS 장애 조치 및 앱 복구에 데이터 영역 기능 사용

상태 확인 및 Amazon Application Recovery Controller(ARC) 라우팅 제어를 포함한 Route 53용 데이터 플레인은 전 세계에 분산되고, 심각한 이벤트 중에도 100% 가용성과 기능을 제공하도록 설계되었습니다. 이들은 서로 통합되며 제어 영역 기능에 의존하지 않습니다. 콘솔을 포함한 이러한 서비스의 제어 영역은 일반적으로 매우 안정적이지만, 중앙 집중식으로 설계되어 고가용성 대신에 내구성과 일관성을 우선시합니다. 재해 복구 중 장애 조치와 같은 시나리오의 경우, 데이터 플레인 기능에 의존하는 Route 53 상태 확인 및 ARC 라우팅 제어와 같은 기능을 사용하여 DNS를 업데이트하는 것이 좋습니다. 자세한 정보는 제어 및 데이터 영역 개념 및 블로그: Amazon Route 53를 사용하여 재해 복구 메커니즘 생성을 참조하세요.

DNS 레코드에 대한 TTL 값 선택

DNS TTL은 DNS 해석기가 Route 53에 다른 쿼리를 수행하지 않고 레코드가 캐시될 수 있는 기간을 결정하는 데 사용하는 숫자 값(초)입니다. 모든 DNS 레코드에는 TTL이 지정되어 있어야 합니다. TTL 값의 권장 범위는 60초에서 172,800초입니다.

지연 시간과 안정성, 변화에 대한 응답성 사이의 절충을 위해 TTL을 선택합니다. 레코드의 TTL이 짧을수록 DNS 해석기는 더 자주 쿼리해야 하므로 레코드에 대한 업데이트를 더 빠르게 알립니다. 이렇게 하면 쿼리 볼륨(및 비용)이 증가합니다. TTL을 늘리면 DNS 해석기가 캐시의 쿼리에 더 자주 응답합니다. 이는 일반적으로 더 빠르고 저렴하며 일부 상황에서는 인터넷을 통한 쿼리를 피할 수 있기 때문에 더 안정적입니다. 올바른 값은 없지만 응답성과 신뢰성 중 무엇이 중요한지 생각해 보는 것은 가치가 있습니다.

TTL 값을 설정할 때 고려할 사항은 다음을 포함합니다.

- 변경 사항이 적용될 때까지 기다릴 수 있는 시간의 길이에 대해 DNS 레코드 TTL을 설정합니다. 이는 특히 위임(NS 레코드 세트) 또는 거의 변경되지 않는 다른 레코드(예: MX 레코드)에 해당됩니다. 이러한 레코드의 경우 긴 TTL을 권장합니다. 한 시간(3600초)과 하루(86,400초) 사이의 값을 일반적으로 선택합니다.
- 신속한 장애 조치 메커니즘의 일부로 변경해야 하는 레코드(특히 상태 확인된 레코드)의 경우 짧은 TTL이 적합합니다. 이 시나리오에서는 TTL을 60초 또는 120초로 설정하는 것이 일반적입니다.
- 중요한 DNS 항목을 변경하는 경우 일시적으로 TTL을 줄이는 것이 좋습니다. 그런 다음 변경, 관찰 및 필요한 경우 빠르게 롤백할 수 있습니다. 변경이 완료되고 예상대로 작동하면 TTL을 늘릴 수 있습니다.

자세한 정보는 TTL(초)을 참조하세요.

CNAME 레코드

DNS CNAME 레코드는 한 도메인 이름을 다른 도메인 이름으로 가리키는 방법입니다. DNS 해석기가 domain-1.example.com을 확인하고 domain-2.example.com을 가리키는 CNAME을 찾으면 DNS 해석기는 응답하기 전에 domain-2.example.com을 확인해야 합니다. 이러한 레코드는 웹 사이트에 도메인 이름이 두 개 이상일 때 일관성을 유지하는 것과 같은 여러 상황에서 유용합니다.

그러나 DNS 해석기는 CNAME에 응답하기 위해 더 많은 쿼리를 작성해야 하므로 지연 시간과 비용이 증가합니다. 가능하면 Route 53 별칭 레코드를 사용하는 것이 더 빠르고 저렴한 대안입니다. 별칭 레코드를 사용하면 Route 53가 동일한 호스팅 영역 내의 AWS 리소스(예: 로드 밸런서) 및 다른 도메인에 대한 직접 응답으로 응답할 수 있습니다.

자세한 내용은 AWS 리소스로 인터넷 트래픽 라우팅 단원을 참조하십시오.

고급 DNS 라우팅

- 지리적 위치, 지리적 근접성 또는 지연 시간 기반 라우팅을 사용할 때 일부 클라이언트가 응답 없음 응답을 받기 원하지 않는 한 항상 기본값을 설정하세요.
- 애플리케이션 지연 시간을 최소화하려면 지연 시간 기반 라우팅을 사용합니다. 이러한 유형의 라우팅 데이터는 자주 변경될 수 있습니다.
- 라우팅 안정성과 예측 가능성을 제공하려면 지리적 위치 또는 지리적 근접성 라우팅을 사용합니다.

자세한 내용은 지리적 라우팅, 지리 근접 라우팅, 지연 시간 기반 라우팅 섹션을 참조하세요.

DNS 변경 전파

Route 53 콘솔 또는 API를 사용하여 레코드 또는 호스트 영역을 생성하거나 업데이트하는 경우 변경 사항이 인터넷에 반영되기까지 약간의 시간이 걸립니다. 이는 변경 전파라고 불립니다. 일반적으로 전파에는 전역적으로 1분 미만이 걸리지만, 예를 들어 한 위치에 동기화하는 문제나 드문 경우 중앙 제어 영역 내의 문제로 인해 가끔 지연될 수 있습니다. 자동화된 프로비저닝 워크플로를 구축하고 있고 다음 워크플로 단계로 진행하기 전에 변경 전파가 완료될 때까지 기다리는 것이 중요한 경우 GetChange API를 사용하여 DNS 변경이 적용되었는지 확인하세요(`Status =INSYNC`).

DNS 위임

DNS에서 여러 수준의 하위 도메인을 위임하는 경우, 항상 상위 영역에서 위임해야 합니다. 예를 들어 www.dept.example.com을 위임하는 경우 example.com 영역이 아니라 dept.example.com 영역에서 그렇게 해야 합니다. 조부모에서 자식 영역으로 위임하는 것은 전혀 작동하지 않거나 일관성 없이 작동할 수 있습니다. 자세한 내용은 하위 도메인에 대한 트래픽 라우팅 단원을 참조하십시오.

DNS 응답의 크기

대규모 단일 응답을 생성하지 마십시오. 응답이 512바이트를 초과하면 많은 DNS 해석기가 UDP 대신 TCP를 통해 재시도해야 하므로 안정성이 저하되고 응답이 느려질 수 있습니다. 응답을 512바이트 경계 내로 유지하려면 8개의 정상적인 임의 IP 주소를 선택하는 다중 응답 라우팅을 사용하는 것이 좋습니다.

자세한 내용은 다중값 응답 라우팅 및 DNS 응답 크기 테스트 서버를 참조하세요.

Resolver 모범 사례

이 섹션에서는 다음 주제를 다루는 Amazon Route 53 Resolver 최적화 모범 사례를 제공합니다.

1. Resolver 엔드포인트를 사용하여 루프 구성 방지:
   - 동일한 VPC가 Resolver 규칙 및 인바운드 엔드포인트와 모두 연결되지 않게 하여 라우팅 루프를 방지합니다.
   - 적절한 라우팅 구성을 유지하면서 계정 간에 VPCs 공유 AWS RAM 하려면를 사용합니다.

   자세한 내용은 Resolver 엔드포인트를 사용하여 루프 구성을 방지합니다. 단원을 참조하세요.
2. Resolver 엔드포인트 크기 조정:
   - 연결 상태를 기반으로 트래픽을 허용하는 보안 그룹 규칙을 구현하여 연결 추적 오버헤드를 줄입니다.
   - 인바운드 및 아웃바운드 Resolver 엔드포인트에 권장되는 보안 그룹 규칙을 준수하여 쿼리 처리량을 극대화합니다.
   - DNS 트래픽을 생성하는 고유한 IP 주소 및 포트 조합을 모니터링하여 용량 제한을 방지합니다.

   자세한 내용은 Resolver 엔드포인트 크기 조정 단원을 참조하세요.
3. Resolver 엔드포인트의 고가용성:
   - 중복을 위해 두 개 이상의 가용 영역에 IP 주소를 사용하여 인바운드 엔드포인트를 구성합니다.
   - 추가 네트워크 인터페이스를 프로비저닝하여 유지 관리 또는 트래픽 급증 중에 가용성을 보장합니다.

   자세한 내용은 Resolver 엔드포인트의 고가용성 단원을 참조하세요.
4. DNS 영역 보행 공격 방지:
   - 공격자가 DNSSEC 서명 DNS 영역에서 모든 콘텐츠를 검색하려고 시도하는 잠재적 DNS 영역 보행 공격에 유의합니다.

- 의심스러운 영역 걷기로 인해 엔드포인트가 제한되는 경우 AWS Support에 문의하여 지원을 받으세요.

자세한 내용은 DNS zone walking 단원을 참조하세요.

이 모범 사례를 따르면 Route 53 Resolver 배포의 성능, 확장성, 보안을 최적화하여 애플리케이션 및 리소스에 대한 안정적이고 효율적인 DNS 확인을 보장할 수 있습니다.

Resolver 엔드포인트를 사용하여 루프 구성을 방지합니다.

동일한 VPC를 (엔드포인트의 직접 대상이든, 온프레미스 DNS 서버를 통해서든) Resolver 규칙 및 인바운드 엔드포인트에 연결하지 마세요. Resolver 규칙의 아웃바운드 엔드포인트가 VPC를 규칙과 공유하는 인바운드 엔드포인트를 가리키면 쿼리가 인바운드 엔드포인트와 아웃바운드 엔드포인트 간에 지속적으로 전달되는 루프가 발생할 수 있습니다.

전달 규칙은 AWS Resource Access Manager ()를 사용하여 다른 VPCs와 연결할 수 있습니다AWS RAM. 허브 또는 중앙 VPC와 연결된 프라이빗 호스팅 영역은 여전히 인바운드 엔드포인트에 대한 쿼리에서 해석됩니다. 해석기 전달 규칙이 이 해석을 변경하지 않기 때문입니다.

Resolver 엔드포인트 크기 조정

Resolver 엔드포인트 보안 그룹은 연결 추적을 사용해 엔드포인트에서 송수신하는 트래픽에 대한 정보를 수집합니다. 각 엔드포인트 인터페이스에는 추적할 수 있는 최대 연결 수가 있으며 많은 양의 DNS 쿼리가 연결 수를 초과하면 제한 및 쿼리 손실이 발생할 수 있습니다. 추적되는 연결 수를 줄이려면 트래픽의 연결 상태에 따라 트래픽을 허용하는 보안 그룹 규칙을 구현하세요. 자세한 내용은 Amazon EC2 사용 설명서의 보안 그룹 및 연결 추적을 참조하세요.

Network Load Balancer 및 AWS Lambda (전체 목록은 자동 추적 연결 참조)와 같은 애플리케이션을 통해 이루어진 연결은 보안 그룹 구성에 추적이 필요하지 않은 경우에도 자동으로 추적됩니다.

제한적인 보안 그룹 규칙을 사용하여 연결 추적을 적용하거나 Network Load Balancer 통해 쿼리를 라우팅하는 경우 엔드포인트에 대한 IP 주소별 초당 전체 최대 쿼리는 최소 1,500개가 될 수 있습니다.

인바운드 Resolver 엔드포인트에 대한 수신 및 송신 보안 그룹 규칙 권장 사항

수신 규칙

프로토콜 유형	포트 번호	소스 IP

TCP	53	0.0.0.0/0
UDP	53	0.0.0.0/0

송신 규칙

프로토콜 유형	포트 번호	목적지 IP
TCP	All	0.0.0.0/0
UDP	All	0.0.0.0/0

아웃바운드 Resolver 엔드포인트에 대한 수신 및 송신 보안 그룹 규칙 권장 사항

수신 규칙

프로토콜 유형	포트 번호	소스 IP
TCP	All	0.0.0.0/0
UDP	All	0.0.0.0/0

송신 규칙

프로토콜 유형	포트 번호	목적지 IP
TCP	All	0.0.0.0/0
UDP	All	0.0.0.0/0

인바운드 Resolver 엔드포인트

인바운드 Resolver 엔드포인트를 사용하는 클라이언트의 경우 DNS 트래픽을 생성하는 40,000개 이상의 고유 IP 주소 및 포트 조합이 있는 경우 탄력적 네트워크 인터페이스 용량에 영향을 미칩니다.

Resolver 엔드포인트의 고가용성

Route 53 Resolver 인바운드 엔드포인트를 만드는 경우 Route 53에서는 네트워크의 DNS Resolver가 쿼리를 전달할 IP 주소를 두 개 이상 만들어야 합니다. 또한 중복성을 위해 가용 영역 2개 이상에서 IP 주소를 지정해야 합니다.

항상 둘 이상의 탄력적 네트워크 인터페이스 엔드포인트를 사용할 수 있어야 하는 경우 네트워크 인터페이스를 필요한 수보다 하나 더 생성하여 트래픽 급증 가능성에 대비할 수 있는 추가 용량을 확보하는 것이 좋습니다. 또한 추가 네트워크 인터페이스는 유지 관리 또는 업그레이드와 같은 서비스 운영 중에도 가용성을 보장합니다.

자세한 내용은 상세한 블로그 기사 Route 53 Resolver 엔드포인트를 사용하여 DNS 고가용성을 달성하는 방법과 인바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값을 참조하세요.

DNS zone walking

DNS zone walking 공격은 DNSSEC 서명 DNS 영역에서 모든 콘텐츠를 가져오려고 시도합니다. Route 53 Resolver 팀이 엔드포인트에서 DNS 영역을 탐색(walk)할 때 생성된 트래픽 패턴과 일치하는 트래픽 패턴을 감지하면 서비스 팀에서 엔드포인트의 트래픽을 제한합니다. 따라서 DNS 쿼리 시간 초과의 비율이 높아질 수 있습니다.

엔드포인트의 용량 감소를 목격하고 엔드포인트 제한이 잘못되었다고 생각하면 https://console.aws.amazon.com/support/home#/으로 이동하여 지원 사례를 만듭니다.

Amazon Route 53 상태 확인의 모범 사례

고가용성과 복원력을 갖춘 인프라를 유지하려면 효과적인 상태 확인 구성이 필수적입니다. 다음은 Amazon Route 53 상태 확인을 설정하고 관리할 때 고려해야 할 몇 가지 모범 사례입니다.

1. 상태 확인 엔드포인트에 탄력적 IP 주소 사용:
   - 상태 확인 엔드포인트에 탄력적 IP 주소를 활용하여 일관된 모니터링을 보장합니다.
   - Amazon EC2 인스턴스를 더 이상 사용하지 않는 경우 잠재적인 보안 위험 또는 데이터 손상을 방지하려면 관련 상태 확인을 삭제해야 합니다.

   자세한 내용은 상태 확인 생성 또는 업데이트 시 지정하는 값을 참조하세요.
2. 적절한 상태 확인 간격 구성:
   - 애플리케이션의 요구 사항과 모니터링된 리소스의 중요도에 따라 상태 확인 간격을 설정합니다.
   - 간격이 짧을수록 장애 감지가 빨라지지만 Route 53 비용과 리소스의 부담이 증가할 수 있습니다.
   - 간격이 길수록 비용과 리소스 리소스의 부담은 줄어들지만 장애 감지가 지연될 수 있습니다.

   자세한 내용은 고급 구성("Monitor an endpoint" 전용)을 참조하세요.
3. 경보 알림 구현:
   - 상태 확인이 실패하거나 복구될 때 알림을 받도록 Amazon CloudWatchalarms를 구성합니다.

- 애플리케이션의 요구 사항과 리소스의 예상 동작에 따라 적절한 경보 임계값을 설정합니다.
- 알림과 모니터링 및 인시던트 대응 프로세스를 통합합니다.

자세한 내용은 CloudWatch를 이용한 상태 확인 모니터링을 참조하세요.

4. 상태 확인 리전을 전략적으로 활용:
   - 사용자 및 리소스의 지리적 분포를 기반으로 상태 확인 리전을 선택합니다.
   - 중요 리소스에 여러 상태 확인 리전을 사용하여 신뢰성을 개선하고 리전 중단의 영향을 줄이는 것을 고려합니다.
5. 상태 확인 로그 및 지표 모니터링:
   - Route 53 상태 확인 로그 및 CloudWatch 지표를 정기적으로 검토하여 잠재적 문제 또는 성능 병목 현상을 식별합니다.
   - 상태 확인 실패 이유를 분석하고 기본 문제를 해결하기 위해 적절한 조치를 취합니다.
6. 장애 조치 및 장애 복구 전략 구현:
   - Route 53의 장애 조치 라우팅 정책을 활용하여 장애 발생 시 트래픽을 정상 리소스로 자동 라우팅합니다.
   - 장애 조치 및 장애 복구 프로세스를 계획하고 테스트하여 중단 및 복구 중에 원활한 전환을 보장합니다.

   자세한 내용은 DNS 장애 조치 구성을 참조하세요.
7. 상태 확인 정기 검토 및 업데이트:
   - 최적의 모니터링 및 성능을 유지하기 위해 필요에 따라 상태 확인 엔드포인트, 간격, 경보 임계값을 업데이트합니다.

이러한 모범 사례를 따르면 Amazon Route 53 상태 확인을 효과적으로 활용하여 리소스의 상태와 가용성을 모니터링하고 애플리케이션 및 서비스에 대한 안정적인 고성능 인프라를 보장할 수 있습니다.

할당량

Amazon Route 53 API 요청 및 엔터티에는 다음 할당량(과거의 “한도”)이 적용됩니다.

주제

Service Quotas를 사용하여 할당량 확인 및 관리

Service Quotas 서비스를 사용하여 할당량을 확인하고 각종 AWS 서비스의 할당량 증가를 요청할 수 있습니다. 자세한 내용은 Service Quotas 사용 설명서를 참조하세요. (현재 Service Quotas를 사용하여 도메인, Route 53 및 Route 53 Resolver 할당량을 보고 관리할 수 있습니다.)

> **Note**
>
> 할당량을 확인하고 Route 53에 대해 더 많은 할당량을 요청하려면 리전을 미국 동부(버지니아 북부)로 변경해야 합니다. 할당량을 확인하고 Resolver에 대해 더 많은 할당량을 요청하려면 해당 리전으로 변경하세요.

엔터티에 대한 할당량

Amazon Route 53 엔터티에는 다음 할당량이 적용됩니다.

현재 할당량(과거의 “한도”)을 가져오는 방법에 대한 자세한 내용은 다음 Route 53 작업을 참조하세요.

- GetAccountLimit - 상태 확인, 호스팅 영역, 재사용 가능한 위임 세트, 트래픽 흐름 정책 및 트래픽 흐름 정책 레코드에 대한 할당량 가져오기
- GetHostedZoneLimit - 프라이빗 호스팅 영역과 연결할 수 있는 Amazon VPC와 호스팅 영역에 있는 레코드에 대한 할당량 가져오기
- GetReusableDelegationSetLimit - 재사용 가능 위임 세트와 연결할 수 있는 호스팅 영역의 수에 대한 할당량 가져오기

주제

도메인에 대한 할당량

개체	할당량
도메인	AWS 계정당 20* 더 높은 할당량 요청.

*2021년 3월 현재 신규 고객의 경우 한도는 20개입니다.

기존 계정이 있고 기본 한도가 50인 경우 해당 계정은 50으로 유지됩니다.

호스팅 영역에 대한 할당량

개체	할당량
호스팅 영역	AWS 계정당 초기 할당량은 500개이지만 필요에 따라 더 높은 할당량을 요청할 수 있습니다. 더 높은 할당량 요청.
재사용 가능한 동일 위임 세트를 사용할 수 있는 호스팅 영역	100

개체	할당량
	더 높은 할당량 요청.
호스팅 영역당 프라이빗 호스팅 영역과 연결할 수 있는 Amazon VPC	300 300개 이상의 연결을 원하는 경우 Route 53 Profiles를 사용하는 것이 좋습니다. 자세한 내용은 Amazon Route 53 Profiles란? 단원을 참조하십시오.
VPC를 연결할 수 있는 프라이빗 호스팅 영역	할당량 없음*
한 계정에서 생성된 VPC를 다른 계정에서 생성된 호스팅 영역과 연결할 수 있도록 생성 가능한 권한	1000
호스팅 영역당 생성할 수 있는 키 서명 키(KSK) 수	2

* VPC를 AWS 계정을 통해 제어하는 프라이빗 호스팅 영역 중 일부 또는 전부와 연결할 수 있습니다. 예를 들어 AWS 계정 3개가 있고 3개 모두 기본 할당량이 호스팅 영역 500개라고 가정해 보겠습니다. 3개 계정 모두에 프라이빗 호스팅 영역 500개를 만들 경우, 하나의 VPC를 1,500개의 프라이빗 호스팅 영역 모두와 연결할 수 있습니다.

레코드에 대한 할당량

개체	할당량
레코드	호스팅 영역당 10,000개 더 높은 할당량 요청.

개체	할당량
	호스팅 영역의 레코드가 10,000개 이상인 할당량에는 추가 요금이 적용됩니다. 자세한 내용은 Amazon Route 53 요금 단원을 참조하세요.
레코드 세트의 레코드 개수	레코드 세트당 400개
지리적 위치, 지연 시간, 다중 값 응답, 가중치, IP 기반 레코드	이름 및 유형이 동일한 레코드 100개
지리 근접 레코드	이름 및 유형이 동일한 레코드 30개
CIDR 컬렉션	당 5개 AWS 계정. 더 높은 할당량 요청.
CIDR 블록	CIDR 컬렉션당 1000개. 더 높은 할당량 요청.

Route 53 Resolver의 할당량

이 섹션에는 모든 Route 53 Resolver 할당량이 포함되어 있습니다.

Route 53 Resolver의 할당량

Route 53 Resolver의 할당량을 늘리려면 다음 절차를 따르세요.

Resolver 할당량을 늘리려면

1. https://console.aws.amazon.com/servicequotas/home/services/route53resolver/quotas에서 Service Quotas 콘솔을 엽니다.
2. 한도를 늘릴 리전으로 이동합니다.
3. 늘리려는 Route 53 Resolver 할당량 이름을 선택합니다.
4. 할당량 증가 요청을 선택하고 할당량 값을 입력한 다음 요청을 선택합니다.

Route 53 Resolver 엔드포인트의 할당량

개체	할당량
AWS 리전당 엔드포인트	AWS 계정당 4개 더 높은 할당량 요청.
엔드포인트당 IP 주소	6 더 높은 할당량 요청.
규칙당 IP 주소	6
AWS 리전당 규칙	AWS 계정당 1,000개 더 높은 할당량 요청.
AWS 리전당 규칙과 VPCs 간의 연결	AWS 계정당 2,000개 더 높은 할당량 요청.
엔드포인트의 각 IP 주소에 대한 초당 UDP 쿼리	10,000*

* 엔드포인트의 각 IP 주소는 초당 UDP DNS 쿼리(QPS)를 10,000개까지 처리할 수 있습니다. DNS QPS의 수는 쿼리 유형, 응답 크기, 대상 이름 서버의 상태, 쿼리 응답 시간,왕복 지연 시간,및 사용 중인 프로토콜에 따라 다릅니다. 예를 들어 응답 속도가 느린 대상 이름 서버에 대한 쿼리는 네트워크 인터페이스의 용량을 크게 줄일 수 있습니다. 또한 고가용성을 보장하기 위해 Route 53 Resolver는 수신하는 각 DNS 요청에 대해 중복 아웃바운드 쿼리를 생성합니다. 따라서 각 아웃바운드 네트워크 인터페이스의 QPS는 Route 53 Resolver에 전송된 QPS와 일치하지 않습니다. CloudWatch 지표를 사용하여 각 네트워크 인터페이스로 전송되는 쿼리 수를 측정할 수 있습니다. 자세한 내용은 Resolver IP 주소에 대

한 지표 섹션을 참조하세요. 최대 쿼리 속도가 엔드포인트의 네트워크 인터페이스 용량의 50%를 초과하는 경우 네트워크 인터페이스를 더 많이 추가하여 엔드포인트 용량을 늘릴 수 있습니다.

Network Load Balancer 및 AWS Lambda (전체 목록은 자동 추적 연결 참조)와 같은 애플리케이션을 통해 이루어진 연결은 보안 그룹 구성에 추적이 필요하지 않은 경우에도 자동으로 추적됩니다.

제한적인 보안 그룹 규칙을 사용하여 연결 추적을 적용하거나 Network Load Balancer를 통해 쿼리를 라우팅하는 경우 인바운드 엔드포인트에 대한 IP 주소별 초당 전체 최대 쿼리는 최소 1,500개가 될 수 있습니다.

Route 53 Resolver 쿼리 로그의 할당량

개체	할당량
AWS 리전당 쿼리 로그 구성	20
AWS 리전별 쿼리 로그 구성 VPC 연결*	100
구성을 공유한 계정에 대한 AWS 리전당 계정당 쿼리 로그 구성 VPC 연결입니다(RAM을 통해 공유됨).	100

* 이것은 하드 제한입니다. 동일한에서 다른 쿼리 로그 구성을 생성하고 AWS 리전 추가 100VPCs를 연결할 수 없습니다.

Route 53 Resolver DNS 방화벽의 할당량

개체	할당량
AWS 리전별 단일 계정의 VPC와 연결된 규칙 그룹 수	5
AWS 리전당 단일 계정에 대한 단일 Amazon S3 파일의 DNS 방화벽 도메인 수	250,000 더 높은 할당량 요청.

개체	할당량
AWS 리전당 단일 계정의 DNS 방화벽 규칙 그룹 수	1,000 더 높은 할당량 요청.
AWS 리전당 단일 계정의 규칙 그룹 내 규칙 수	100 더 높은 할당량 요청.
AWS 리전당 단일 계정의 도메인 목록 수	1000 더 높은 할당량 요청.
AWS 리전별 단일 계정의 모든 도메인 목록에서 지정할 수 있는 최대 도메인 수	100,000건 더 높은 할당량 요청.

Outpost의 해석기 할당량

개체	할당량
Outpost의 해석기 인스턴스 한도	6개(최소 4개 필요)

Resolver on Outpost 인스턴스 유형 및 각 인스턴스 유형에서 수용할 수 있는 초당 DNS 쿼리 수:

인스턴스 유형	초당 쿼리 수
c5.large	최대 7,000개
c5.xlarge	최대 1만 2,000개
c5.2xlarge	최대 2만 4,000개

인스턴스 유형	초당 쿼리 수
c5.4xlarge	최대 5만 6,000개
c5d.large	최대 7,000개
c5d.xlarge	최대 1만 2,000개
c5d.2xlarge	최대 2만 4,000개
c5d.4xlarge	최대 5만 6,000개
m5.large	최대 7,000개
m5.xlarge	최대 1만 2,000개
m5.2xlarge	최대 2만 4,000개
m5.4xlarge	최대 5만 6,000개
m5d.large	최대 7,000개
m5d.xlarge	최대 1만 2,000개
m5d.2xlarge	최대 2만 4,000개
m5d.4xlarge	최대 5만 6,000개
r5.large	최대 7,000개
r5.xlarge	최대 1만 2,000개

인스턴스 유형	초당 쿼리 수
r5.2xlarge	최대 2만 4,000개
r5.4xlarge	최대 5만 6,000개
r5d.large	최대 7,000개
r5d.xlarge	최대 1만 2,000개
r5d.2xlarge	최대 2만 4,000개
r5d.4xlarge	최대 5만 6,000개

Resolver on Outpost 엔드포인트 인스턴스 유형 및 각 인스턴스 유형에서 수용할 수 있는 초당 DNS 쿼리 수:

인스턴스 유형	초당 쿼리 수
c5.large	최대 5,000개
c5.xlarge	최대 10,000
c5.2xlarge	최대 1만 8,000개
c5.4xlarge	최대 3만 개
c5d.large	최대 5,000개
c5d.xlarge	최대 10,000
c5d.2xlarge	최대 1만 8,000개

인스턴스 유형	초당 쿼리 수
c5d.4xlarge	최대 3만 개
m5.large	최대 5,000개
m5.xlarge	최대 10,000
m5.2xlarge	최대 1만 8,000개
m5.4xlarge	최대 3만 개
m5d.large	최대 5,000개
m5d.xlarge	최대 10,000
m5d.2xlarge	최대 1만 8,000개
m5d.4xlarge	최대 3만 개
r5.large	최대 5,000개
r5.xlarge	최대 10,000
r5.2xlarge	최대 1만 8,000개
r5.4xlarge	최대 3만 개
r5d.large	최대 5,000개

인스턴스 유형	초당 쿼리 수
r5d.xlarge	최대 10,000
r5d.2xlarge	최대 1만 8,000개
r5d.4xlarge	최대 3만 개

상태 확인에 대한 할당량

개체	할당량
상태 확인	AWS 계정당 활성 상태 확인 200개 더 높은 할당량 요청.
계산된 상태 확인이 모니터링할 수 있는 하위 상태 확인	255
상태 확인 요청에 대한 응답의 최대 총 헤더 길이	16,384바이트(16K)

쿼리 로그 구성에 대한 할당량

개체	할당량
쿼리 로그 구성	호스팅 영역당 1개

트래픽 흐름 정책 및 정책 레코드에 대한 할당량

개체	할당량
트래픽 정책 Route 53 트래픽 흐름에 대한 자세한 내용은 트래픽 흐름을 사용하여 DNS 트래픽 라우팅 섹션을 참조하세요.	AWS 계정당 50개 더 높은 할당량 요청.
트래픽 정책 버전	트래픽 정책당 1,000개
트래픽 정책 레코드(Route 53 API AWS Command Line Interface, AWS SDKs 및에서 "정책 인스턴스"라고 함 AWS Tools for Windows PowerShell)	AWS 계정당 5개 더 높은 할당량 요청.

재사용 가능한 위임 세트에 대한 할당량

개체	할당량
재사용 가능한 위임 세트	AWS 계정당 100개 더 높은 할당량 요청.

Route 53 Profiles의 할당량

개체	할당량
AWS 계정 리전의 별 Route 53 프로파일 수	5 더 높은 할당량 요청.

개체	할당량
프로파일에 연결할 수 있는 VPC 수	1000 더 높은 할당량 요청.
프로파일당 DNS 방화벽 규칙 그룹 수	5
프로파일당 Resolver 규칙 수	1000 더 높은 할당량 요청.
프로파일당 프라이빗 호스팅 영역 수	1,000 더 높은 할당량 요청.

API 요청에 대한 최댓값

Amazon Route 53 API 요청에는 다음 최댓값이 적용됩니다.

주제

- ChangeResourceRecordSets 요청의 요소 및 문자 수
- Amazon Route 53 Resolver API 요청 빈도
- Route 53 Resolver API 요청 빈도

ChangeResourceRecordSets 요청의 요소 및 문자 수

`ResourceRecord` 요소

요청은 1,000개 이하의 `ResourceRecord` 요소를 포함할 수 있습니다(별칭 레코드 포함). `Action` 요소의 값이 `UPSERT`이면 `ResourceRecord` 요소가 각각 두 번 계산됩니다.

최대 문자 수

요청의 모든 `Value` 요소의 문자 수 합계(공백 포함)는 32,000자를 초과할 수 없습니다. `Action` 요소의 값이 `UPSERT`이면 `Value` 요소의 문자가 각각 두 번 계산됩니다.

Amazon Route 53 Resolver API 요청 빈도

모든 Amazon Route 53 API 요청

Amazon Route 53 APIs5개의 요청입니다. AWS 초당 다섯 개를 초과하여 요청을 제출하면 Amazon Route 53에서 HTTP 400 오류(`Bad request`)를 반환합니다. 또한 응답 헤더에는 값이 `Throttling`인 `Code` 요소와 값이 `Rate exceeded`인 `Message` 요소가 포함되어 있습니다.

> **Note**
>
> 응용 프로그램이 이 제한을 초과하는 경우, 재시도에서는 지수 백오프를 구현하는 것이 좋습니다. 자세한 내용은 Amazon Web Services 일반 참조의 AWS의 오류 재시도 및 지수 백오프 단원을 참조하세요.

`ChangeResourceRecordSets` 요청

Route 53에서 다음 요청이 도착하기 전에 요청을 처리할 수 없는 경우, 동일한 호스팅 영역에 대한 다음 요청을 거부하고 HTTP 400 오류(`Bad request`)를 반환합니다. 또한 응답 헤더에는 값이 `PriorRequestNotComplete`인 `Code` 요소와 값이 `The request was rejected because Route 53 was still processing a prior request.`인 `Message` 요소가 포함되어 있습니다.

`CreateHealthCheck` 요청

2초마다 `CreateHealthCheck` 요청을 제출할 수 있습니다 AWS 계정.

Route 53 Resolver API 요청 빈도

모든 요청

리전별 AWS 계정당 초당 5개의 요청. 리전별 초당 5개가 넘는 요청을 제출하면 Resolver에서 HTTP 400 오류(`Bad request`)를 반환합니다. 또한 응답 헤더에는 값이 `Throttling`인 `Code` 요소와 값이 `Rate exceeded`인 `Message` 요소가 포함되어 있습니다.

> **Note**
>
> 응용 프로그램이 이 제한을 초과하는 경우, 재시도에서는 지수 백오프를 구현하는 것이 좋습니다. 자세한 내용은 Amazon Web Services 일반 참조의 AWS의 오류 재시도 및 지수 백오프 단원을 참조하세요.

관련 정보

다음의 관련 리소스는 이 서비스 사용 시 도움이 될 수 있습니다.

주제

- AWS 리소스
- 타사 도구 및 라이브러리
- 그래픽 사용자 인터페이스

AWS 리소스

Amazon Web Services에서 몇 가지 유용한 가이드, 포럼, 기타 리소스를 얻을 수 있습니다.

- Amazon Route 53 API 참조 - 참조 가이드로서, 스키마 위치를 비롯해 API 작업, 매개 변수, 데이터 유형에 대한 설명, 서비스가 반환하는 오류 목록을 제공합니다.
- AWS CloudFormation 사용 설명서의AWS::Route53::RecordSet- Amazon Route 53를와 함께 사용하여 AWS CloudFormation 스택 AWS CloudFormation 에 대한 사용자 지정 DNS 이름을 생성하기 위한 속성입니다.
- 토론 포럼 - Route 53에 관련된 기술적 질문을 논의할 수 있는 개발자를 위한 커뮤니티 기반 포럼입니다.
- AWS 지원 센터 -이 사이트에서는 최근 지원 사례 및 AWS Trusted Advisor 및 상태 확인 결과에 대한 정보와 토론 포럼, 기술 FAQs, 서비스 상태 대시보드 및 AWS 지원 계획에 대한 정보에 대한 링크를 제공합니다.
- AWS 프리미엄 지원 정보 - AWS 인프라 서비스에서 애플리케이션을 구축하고 실행하는 데 도움이 되는 one-on-one 빠른 응답 지원 채널인 AWS 프리미엄 지원에 대한 정보를 제공하는 기본 웹 페이지입니다.
- 문의처 - 청구 또는 계정과 관련하여 문의할 수 있는 링크. 기술적인 질문의 경우, 토론 포럼이나 위의 지원 링크를 사용하세요.
- Route 53 제품 정보 - 기능, 요금 등 Route 53에 대한 정보를 얻을 수 있는 기본 웹 페이지입니다.

- 클래스 및 워크숍 - AWS 기술을 연마하고 실용적인 경험을 얻는 데 도움이 되는 자기 주도형 랩 외에도 역할 기반 및 특수 과정으로 연결되는 링크입니다.
- AWS 개발자 센터 - 자습서를 살펴보고, 도구를 다운로드하고, AWS 개발자 이벤트에 대해 알아봅니다.

- AWS 개발자 도구 - AWS 애플리케이션 개발 및 관리를 위한 개발자 도구, SDKs, IDE 도구 키트 및 명령줄 도구에 대한 링크입니다.
- 리소스 센터 시작하기 -를 설정하고 AWS 계정, AWS 커뮤니티에 가입하고, 첫 번째 애플리케이션을 시작하는 방법을 알아봅니다.
- 실습 튜토리얼 – 단계별 튜토리얼에 따라 AWS에서 첫 번째 애플리케이션을 시작합니다.
- AWS 백서 - 아키텍처, 보안 및 경제와 같은 주제를 다루고 Solutions Architects 또는 기타 기술 전문가가 작성한 AWS 포괄적인 기술 AWS 백서 목록으로 연결되는 링크입니다.
- AWS Support 센터 - AWS Support 사례를 생성하고 관리하기 위한 허브입니다. 포럼, 기술 FAQs, 서비스 상태 및 같은 기타 유용한 리소스에 대한 링크도 포함되어 있습니다 AWS Trusted Advisor.
- 지원 - 클라우드에서 애플리케이션을 구축하고 실행하는 데 도움이 지원되는 one-on-one 빠른 응답 지원 채널에 대한 정보를 제공하는 기본 웹 페이지입니다.
- Contact Us(문의처) - AWS 결제, 계정, 이벤트, 침해 및 기타 문제에 대해 문의할 수 있는 중앙 연락 창구입니다.
- AWS 사이트 약관 - 저작권 및 상표, 계정, 라이선스 및 사이트 액세스, 기타 주제에 대한 자세한 정보입니다.

타사 도구 및 라이브러리

AWS 리소스 외에도 Amazon Route 53에서 작동하는 다양한 타사 도구 및 라이브러리를 찾을 수 있습니다.

- AmazonRoute53AppsScript(webos-goodies 경유)

  Amazon Route 53의 Google 스프레드시트 관리입니다.
- AWS .NET용 구성 요소(SprightlySoft를 통해)

  REST 작업 및 Route 53을 지원하는 Amazon Web Services를 위한 SprightlySoft .NET 구성 요소입니다.
- Boto API download(github 경유)

  Amazon Web Services에 대한 Boto Python 인터페이스.입니다.
- cli53(github 경유)

  Route 53을 위한 명령줄 인터페이스입니다.
- Dasein Cloud API

Java 기반 API입니다.

- R53.py(github 경유)

  DNS 구성의 정식 버전을 소스 제어 아래에서 유지 관리하고 구성을 변경하는 데 필요한 변경 사항의 최소 세트를 계산합니다.

- route53d

  Route 53 API에 대한 DNS 프런트 엔드입니다(증진적 영역 전송(IXFR)을 활성화합니다).

- Route53Manager(github 경유)

  웹 기반 인터페이스입니다.

- Ruby Fog(github 경유)

  Ruby 클라우드 서비스 라이브러리입니다.

- WebService::Amazon::Route53(CPAN 경유)

  Amazon Route 53 API에 대한 Perl 인터페이스입니다.

그래픽 사용자 인터페이스

다음의 서드 파티 도구들은 Amazon Route 53에서 사용할 수 있는 그래픽 사용자 인터페이스(GUI)를 제공합니다.

- R53 Fox
- Ylastic

문서 기록

다음 항목은 Route 53 설명서의 각 릴리스에서 변경된 중요 사항에 대해 설명합니다. 이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

주제

2025년 릴리스

2025년 1월 14일

Amazon Route 53는 이제 OpenSearch Service 사용자 지정 도메인 엔드포인트에 대한 별칭 레코드를 지원합니다. 자세한 내용은 Amazon OpenSearch Service 도메인 엔드포인트로 트래픽 라우팅 단원을 참조하십시오.

2025년 1월 13일

Security Hub에 Route 53 Resolver DNS 방화벽 조사 결과를 추가했습니다. 자세한 내용은 Route 53 Resolver DNS 방화벽에서 Security Hub로 조사 결과 전송 단원을 참조하십시오.

2024년 릴리스

2024년 11월 15일

DNS 터널링 및 도메인 생성 알고리즘(DGA) 기반 위협과 같은 고급 DNS 위협과 관련된 DNS 트래픽을 식별하고 차단할 수 있는 Route 53 Resolver DNS 방화벽의 새로운 기능 세트인 Route 53 Resolver DNS Firewall Advanced가 추가되었습니다. 자세한 내용은 Route 53 Resolver DNS 방화벽 고급 단원을 참조하십시오.

2024년 10월 29일

HTTPS, SSHFP, SVCB 및 TLSA DNS 레코드 유형에 대한 지원이 추가되었습니다. 자세한 내용은 지원되는 DNS 레코드 유형 단원을 참조하십시오.

2024년 10월 3일

DoH 아웃바운드 Resolver 엔드포인트에 대한 Service Name Indication(SNI) 지원이 추가되었습니다. 자세한 내용은 규칙을 생성 또는 편집할 때 지정하는 값 단원을 참조하십시오.

2024년 9월 3일

이제 `route53:VPCs` 정책 조건을 사용하여 VPC의 호스팅 영역 연결 관리를 위한 세분화된 액세스 권한을 부여할 수 있습니다. 자세한 내용은 IAM 정책 조건을 사용하여 세분화된 액세스 제어 구현 단원을 참조하십시오.

2024년 8월 27일

`AmazonRoute53ProfilesFullAccess`이 `GetProfilePolicy` 및 `PutProfilePolicy`에 대한 권한을 추가했습니다. 이는 권한 전용 IAM 작업입니다. IAM 보안 주체에게 이러한 권한이 부여되지 않은 경우 AWS RAM 서비스를 사용하여 프로필을 공유하려고 할 때 오류가 발생합니다. 자세한 내용은 AWS 관리형 정책: AmazonRoute53ProfilesFullAccess 단원을 참조하십시오.

2024년 8월 27일

`AmazonRoute53ProfilesReadOnlyAccess`이 `GetProfilePolicy`에 대한 권한을 추가했습니다. 권한 전용 IAM 작업입니다. IAM 보안 주체에게이 권한이 부여되지 않은 경우 AWS RAM 서비스를 사용하여 프로파일의 정책에 액세스하려고 할 때 오류가 발생합니다. 자세한 내용은 AWS 관리형 정책: AmazonRoute53ProfilesReadOnlyAccess 단원을 참조하십시오.

2024년 8월 5일

관리형 정책 `AmazonRoute53ResolverFullAccess`을 고유하게 식별하는 문 ID(Sid)가 추가되었습니다. 자세한 내용은 AWS 관리형 정책: AmazonRoute53ResolverFullAccess 단원을 참조하십시오.

2024년 8월 5일

관리형 정책 AmazonRoute53ResolverReadOnlyAccess을 고유하게 식별하는 문 ID(Sid)가 추가되었습니다. 자세한 내용은 AWS 관리형 정책: AmazonRoute53ResolverReadOnlyAccess 단원을 참조하십시오.

2024년 7월 18일

전체 Route 53 가이드를 상태 확인에 대한 새로운 콘솔 환경으로 업데이트했습니다. 자세한 내용은 상태 확인의 생성, 업데이트 및 삭제 단원을 참조하십시오.

2024년 4월 30일

이제 DNS 방화벽 규칙이 DNS 리디렉션 체인을 검사(기본값)하거나 신뢰하도록 결정할 수 있습니다. 자세한 내용은 Route 53 Resolver DNS 방화벽 구성 요소 및 설정 및 DNS 방화벽의 규칙 설정 단원을 참조하세요.

2024년 4월 22일

이제 Route 53 Profiles를 사용하여 여러 VPCs 및 AWS 계정과 DNS별 구성을 공유할 수 있습니다. 자세한 내용은 Amazon Route 53 Profiles란? 단원을 참조하십시오.

2024년 4월 22일

Amazon Route 53 Profiles에 대한 읽기 전용 및 전체 액세스 권한을 부여하기 위해 관리형 정책 AmazonRoute53ProfilesReadOnlyAccess 및 AmazonRoute53ProfilesFullAccess가 추가되었습니다. 자세한 내용은 AWS Amazon Route 53에 대한 관리형 정책 단원을 참조하십시오.

2024년 2월 5일

이제 Amazon EventBridge를 사용하여 DNS 방화벽의 실시간 알림을 받을 수 있습니다. 자세한 내용은 를 사용하여 Route 53 Resolver DNS 방화벽 이벤트 관리 Amazon EventBridge 단원을 참조하십시오.

2024년 1월 9일

이제 DNS 쿼리 유형을 DNS 방화벽 규칙의 선택적 값으로 사용하여 특정 DNS 쿼리 유형에 대한 규칙의 응답을 구분할 수 있습니다. 자세한 내용은 Route 53 Resolver DNS 방화벽 구성 요소 및 설정 및 DNS 방화벽의 규칙 설정 단원을 참조하세요.

2024년 1월 9일

이제 빠른 레코드 생성 또는 레코드 생성 마법사를 사용하여 지리 근접 라우팅 레코드를 생성할 수 있습니다. 자세한 내용은 지리 근접 라우팅, 지리 근접성 레코드에 특정된 값, 지리 근접성 별칭 레코드에 특정된 값 섹션을 참조하세요.

2023년 릴리스

2023년 12월 20일

이제 Route 53 Resolver 엔드포인트에서 HTTPS를 통한 DNS를 사용할 수 있습니다. 자세한 내용은 엔드포인트 프로토콜 선택 단원을 참조하십시오.

2023년 7월 20일

이제 Amazon Route 53 on Outposts를 AWS Outposts 랙에서 사용할 수 있습니다. AWS Outposts에서 발생하는 모든 DNS 쿼리를 캐싱하는 해석기가 포함되어 있습니다. 또한 인바운드 및 아웃바운드 엔드포인트를 배포할 때 Outpost와 온프레미스 DNS 해석기 간에 하이브리드 연결을 설정할 수 있습니다. 자세한 내용은 Amazon Route 53 on Outposts란 무엇인가요? 단원을 참조하십시오.

2023년 7월 19일

이제 로컬 영역을 활성화한 후 지리 근접 라우팅(트래픽 흐름만 해당)과 함께 사용할 수 있습니다. 자세한 내용은 지리 근접 라우팅 및 Traffic Policy Document Format을 참조하세요.

2023년 3월 22일

전체 Route 53 가이드를 도메인에 대한 새로운 콘솔 환경으로 업데이트했습니다. 새 콘솔 환경을 사용하여 도메인을 한에서 AWS 계정 다른 로 이전할 수도 있습니다 AWS 계정. 자세한 내용은 새 도메인 등록 및 도메인 이전 단원을 참조하세요.

2023년 3월 10일

이제 Amazon Route 53 Resolver를 통해 IPv4, IPv6 또는 듀얼 스택 엔드포인트를 사용하여 리소스에 연결할 수 있습니다. 자세한 내용은 인바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값 및 아웃바운드 엔드포인트를 생성 또는 편집할 때 지정하는 값 단원을 참조하세요.

2022년 릴리스

2022년 9월 21일

이제 정책 조건을 사용하여 Amazon Route 53 리소스 레코드 세트 업데이트에 대해 세분화된 액세스 권한을 사용자에게 부여할 수 있습니다. 자세한 내용은 IAM 정책 조건을 사용하여 세분화된 액세스 제어 구현 단원을 참조하십시오.

2022년 8월 30일

Amazon Route 53는 이제 2022년 8월 1일 이후에 생성된 AWS App Runner 서비스에 대한 별칭 레코드를 지원합니다. 자세한 내용은 AWS App Runner 서비스로 트래픽 라우팅 단원을 참조하십시오.

2022년 6월 1일

이제 Amazon Route 53에서 IP 기반 라우팅 옵션을 사용할 수 있습니다. 자세한 내용은 IP 기반 라우팅 단원을 참조하십시오.

2022년 3월 16일

Amazon Route 53에서 프라이빗 호스팅 영역에 대해 지리적 위치 및 지연 시간 기반 라우팅 옵션을 정식 지원합니다. 자세한 내용은 프라이빗 호스팅 영역 작업 시 고려 사항 단원을 참조하십시오.

2022년 1월 25일

.com.au 및 .net.au TLD에 대한 소유권 변경 프로세스가 두 개의 이메일에 대한 응답(이전 등록자와 새 등록자 모두)을 포함하고 양식 작성은 포함되지 않도록 간소화되었습니다. 자세한 내용은 .com.au(호주) 및 .net.au(호주) 단원을 참조하세요.

2021년 릴리스 정보

2021년 10월 26일

Amazon Route 53에서 기본 역방향 DNS 규칙을 비활성화할 수 있는 지원이 추가되었습니다. 이제 이러한 규칙의 생성을 비활성화하고 역방향 DNS 네임스페이스에 대한 쿼리를 원하는 대로 외부 서버로 전달할 수 있습니다. 자세한 내용은 해석기의 역방향 DNS 쿼리에 대한 전달 규칙 단원을 참조하십시오.

2021년 9월 1일

정적 웹 사이트에 Amazon CloudFront 배포 생성을 안내하는 새로운 시작 주제 추가 자세한 내용은 Amazon CloudFront 배포를 사용하여 정적 웹 사이트 제공 섹션을 참조하세요.

2021년 7월 14일

Amazon Route 53에 대한 AWS 관리형 정책 추적을 시작했습니다. 자세한 내용은 AWS Amazon Route 53에 대한 관리형 정책 단원을 참조하십시오.

2021년 3월 31일

Route 53 Resolver DNS 방화벽 추가 DNS 방화벽을 사용하면 VPC의 아웃바운드 DNS 요청에 대해 보호를 제공할 수 있습니다. 자세한 내용은 DNS 방화벽을 사용하여 아웃바운드 DNS 트래픽 필터링 섹션을 참조하세요.

2020년 릴리스 정보

2020년 12월 17일

Route 53 Resolver에 DNSSEC 서명 지원 추가 자세한 내용은 Amazon Route 53에서 DNSSEC 서명 구성 섹션을 참조하세요.

Route 53 Resolver에 DNSSEC 검증 지원 추가 자세한 내용은 Amazon Route 53에서 DNSSEC 검증 활성화 섹션을 참조하세요.

2020년 9월 23일

전체 Route 53 가이드를 새로운 콘솔 환경으로 업데이트했습니다. 자세한 내용은 Amazon Route 53는 무엇인가요? 섹션을 참조하세요.

2020년 9월 1일

Resolver 쿼리 로그에 대한 지원 추가 자세한 내용은 Resolver 쿼리 로깅 섹션을 참조하세요.

2018 릴리스

2018년 12월 20일

API Gateway API 또는 Amazon VPC 인터페이스 엔드포인트로 트래픽을 라우팅하는 Route 53 별칭 레코드를 만들 수 있습니다. 자세한 내용은 값/트래픽 라우팅 대상 섹션을 참조하세요.

2018년 11월 28일

Route 53 Auto Naming(서비스 검색이라고도 함)은 이제 별도의 서비스입니다 AWS Cloud Map. 자세한 내용은 개발자 안내서AWS Cloud Map를 참조하세요.

2018년 11월 19일

Route 53 Resolver를 사용하여 Direct Connect 또는 VPN 연결을 통해 VPC와 네트워크 간 DNS 확인을 구성할 수 있습니다. (Resolver는 Amazon Virtual Private Cloud(Amazon VPC)에서 모든 고객

에게 기본적으로 제공하는 재귀 DNS 서비스의 새로운 이름입니다.) 이를 통해 DNS 쿼리를 네트워크 상의 해석기에서 Route 53 Resolver로 전달할 수 있습니다. Resolver를 통해 선택한 도메인 이름(example.com)과 하위 도메인 이름(api.example.com)에 대한 쿼리를 VPC에서 네트워크 상의 해석기로 전달할 수도 있습니다. 자세한 내용은 Amazon Route 53 Resolver란 무엇인가요? 섹션을 참조하세요.

2018년 11월 7일

Route 53 트래픽 흐름과 지리 근접 라우팅을 사용하는 경우, 대화형 맵을 사용하여 최종 사용자가 전 세계 엔드포인트로 어떻게 라우팅되는지 시각화할 수 있습니다. 자세한 내용은 지리 근접 설정의 효과를 볼 수 있는 지도 보기 섹션을 참조하세요.

2018년 10월 18일

Route 53 콘솔 및 API를 사용하여 Route 53 상태 확인을 일시적으로 비활성화할 수 있습니다. 이로써 경보를 트리거하거나 불필요한 로그 또는 상태 메시지를 생성하지 않고 웹 서버 같은 엔드포인트의 모니터링을 간편하게 일시 중지하고 엔드포인트에서 유지 관리를 수행할 수 있습니다. 자세한 내용은 상태 확인 생성 또는 업데이트 시 지정하는 값의 '비활성화됨'을 참조하십시오. 이 기능은 엔드포인트를 모니터링하는 상태 확인, 다른 상태 확인을 모니터링하는 상태 확인, CloudWatch 경보를 모니터링하는 상태 확인 등 세 가지 유형의 Route 53 상태 확인에서 모두 사용할 수 있습니다.

2018년 3월 13일

자동 이름 지정 기능을 사용하는 경우 앞으로는 타사 상태 확인으로 리소스 상태를 평가할 수 있습니다. 이것은 인스턴스가 Amazon VPC에 있다거나 하는 이유로 인터넷에서 리소스를 사용할 수 없는 경우에 유용합니다. 자세한 내용은 Amazon Route 53 API 참조의 HealthCheckCustomConfig를 참조하세요.

2018년 3월 9일

IAM에 자동 이름 지정의 관리형 정책이 포함됩니다. 자세한 내용은 AWS Amazon Route 53에 대한 관리형 정책 섹션을 참조하세요.

2018년 2월 6일

이제 자동 이름 지정을 구성하여 ELB 로드 밸런서로 트래픽을 라우팅하는 별칭 레코드를 만들거나 CNAME 레코드를 만들 수 있습니다. 자세한 내용은 Amazon Route 53 API 참조의 RegisterInstance API 설명서에 있는 속성을 참조하세요.

2017 릴리스

2017년 12월 5일

이제 Route 53 자동 이름 지정 API를 사용하여 마이크로서비스용 인스턴스를 프로비저닝할 수 있습니다. 자동 이름 지정을 사용하면 자동으로 DNS 레코드를 생성하고, 선택적으로 사용자가 지정하는 템플릿을 기반으로 상태 확인을 생성할 수 있습니다. 자세한 내용은 AWS Cloud Map 개발자 안내서의 AWS Cloud Map이란 무엇입니까?를 참조하세요.

2017년 11월 16일

이제 호스팅 영역 및 상태 확인 등 Route 53 리소스에 대한 현재 할당량, 그리고 현재 사용 중인 각 리소스의 수 모두를 프로그래밍 방식으로 가져올 수 있습니다. 자세한 내용은 Amazon Route 53 API 참조의 GetAccountLimit,GetHostedZoneLimit 및 GetReusableDelegationSetLimit을 참조하세요.

2017년 10월 3일

Route 53는 이제 HIPAA 적격 서비스입니다. 자세한 내용은 Amazon Route 53의 규정 준수 확인 섹션을 참조하세요.

2017년 9월 29일

이제 특정 도메인을 Route 53로 이전할 수 있는지 여부를 프로그래밍 방식으로 확인할 수 있습니다. 자세한 내용은 Amazon Route 53 API 참조의 CheckDomainTransferability를 참조하세요.

2017년 9월 11일

이제 Elastic Load Balancing Network Load Balancer로 인터넷 트래픽을 라우팅하는 Route 53 별칭 레코드를 생성할 수 있습니다. 별칭 레코드에 대한 자세한 내용은 별칭 또는 비 별칭 레코드 선택 단원을 참조하십시오.

2017년 9월 7일

Route 53를 신뢰할 수 있는 퍼블릭 DNS 서비스로 사용하는 경우 이제 Route 53가 수신하는 DNS 쿼리를 로깅할 수 있습니다. 자세한 내용은 퍼블릭 DNS 쿼리 로깅 섹션을 참조하세요.

2017년 9월 1일

Route 53 트래픽 흐름을 사용하는 경우 이제 사용자와 리소스 사이의 물리적 거리를 기반으로 트래픽을 라우팅할 수 있는 지리 근접 라우팅을 사용할 수 있습니다. 또한 양 또는 음의 바이어스를 지정하여 각 리소스로 라우팅되는 트래픽을 증감할 수도 있습니다. 자세한 내용은 지리 근접 라우팅 섹션을 참조하세요.

2017년 8월 21일

이제 Route 53를 사용하여 인증 기관 권한 부여(CAA) 레코드를 생성할 수 있습니다. 그러면 도메인 또는 하위 도메인에 대한 인증서를 발급할 수 있는 인증 기관을 지정할 수 있습니다. 자세한 내용은 CAA 레코드 유형 섹션을 참조하세요.

2017년 8월 18일

이제 Route 53 콘솔을 사용하여 Route 53로 다수의 도메인을 이전할 수 있습니다. 자세한 내용은 도메인 등록을 Amazon Route 53으로 이전하기 섹션을 참조하세요.

2017년 8월 4일

도메인을 등록할 때 일부 최상위 도메인(TLD)의 등록 기관은 등록자에게 등록자 연락처로 유효한 이메일 주소를 지정했는지 확인할 것을 요구합니다. 이제 도메인 등록 과정에서 확인 이메일을 발송하고 이메일 주소가 성공적으로 확인되었다는 확인을 받을 수 있습니다. 자세한 내용은 새 도메인 등록 섹션을 참조하세요.

2017년 6월 21일

트래픽을 거의 무작위적으로 웹 서버 같은 다수의 리소스로 라우팅하려는 경우 이제 리소스마다 하나씩 다중값 응답 레코드를 생성하고, 선택적으로 Route 53 상태 확인을 각 레코드에 연결할 수 있습니다. Route 53는 최대 8개의 정상 레코드로 각 DNS 쿼리에 응답하며, DNS 해석기마다 다른 응답을 제공합니다. 자세한 내용은 다중값 응답 라우팅 섹션을 참조하세요.

2017년 10월 4일

Route 53 콘솔을 사용하여 도메인 등록을 Route 53로 이전할 때 이제 다음 옵션 중 하나를 선택하여 도메인의 DNS 서비스의 이름 서버를 이전된 도메인 등록과 연결할 수 있습니다.

- 선택한 Route 53 호스팅 영역의 이름 서버를 사용
- 도메인의 현재 DNS 서비스의 이름 서버를 사용
- 지정한 이름 서버를 사용

Route 53가 자동으로 이러한 이름 서버를 이전된 도메인 등록과 연결합니다.

2016 릴리스

2016년 11월 21일

IPv6 주소를 사용하여 엔드포인트의 상태를 확인하는 상태 확인을 만들 수 있습니다. 자세한 내용은 상태 확인의 생성 및 업데이트 섹션을 참조하세요.

2016년 11월 15일

Route 53 API 작업을 사용하여 하나의 계정에서 만든 Amazon VPC를 다른 계정에서 만든 프라이빗 호스팅 영역과 연결할 수 있습니다. 자세한 내용은 Amazon VPC와 다른 AWS 계정에서 생성한 프라이빗 호스팅 영역 연결 섹션을 참조하세요.

2016년 8월 30일

이번 릴리스에는 Route 53에 다음과 같은 새로운 기능이 추가되었습니다.

- 이름 인증 포인터(NAPTR) 레코드 - Dynamic Delegation Discovery System(DDDS) 애플리케이션에서 하나의 값을 다른 값으로 변환하거나 대체하기 위해 사용하는 NAPTR 레코드를 생성할 수 있습니다. 예를 들어, 하나의 일반적인 용도는 전화번호를 SIP URI로 변환하는 것입니다. 자세한 내용은 NAPTR 레코드 유식 섹션을 참조하세요.
- DNS 쿼리 테스트 도구 - 레코드에 대해 DNS 쿼리를 시뮬레이션하여 Route 53가 반환하는 값을 확인할 수 있습니다. 또한 지리 위치 및 지연 시간 레코드에 대해 특정 DNS 해석기 및/또는 클라이언트 IP 주소로부터의 요청을 시뮬레이션하여 Route 53에서 해당 해석기 및 IP 주소의 클라이언트로 반환하는 응답을 확인할 수 있습니다. 자세한 내용은 Route 53에서 DNS 응답 확인 섹션을 참조하세요.

2016년 8월 11일

이 릴리스에서는 트래픽을 ELB Application Load Balancer로 라우팅하는 별칭 레코드를 생성할 수 있습니다. 이 프로세스는 Classic Load Balancer의 경우와 동일합니다. 자세한 내용은 값/트래픽 라우팅 대상 섹션을 참조하세요.

2016년 8월 9일

이 릴리스에서 Route 53에는 도메인 등록을 위해 DNSSEC 지원이 추가되었습니다. DNSSEC를 통해 중간자 공격이라고도 하는 DNS 스푸핑 공격으로부터 도메인을 보호할 수 있습니다. 자세한 내용은 도메인에 대해 DNSSEC 구성 섹션을 참조하세요.

2016년 7월 7일

도메인에 대한 등록을 수동으로 확장하고, 등록소에서 지정한 최소 등록 기간보다 오래 된 등록 기간으로 도메인을 등록할 수 있습니다. 자세한 내용은 도메인의 등록 기간 연장 섹션을 참조하세요.

2016년 7월 6일

연락처 주소가 인도 내인 AISPL 고객은 이제 Route 53를 사용하여 도메인을 등록할 수 있습니다. 자세한 내용은 인도 내 계정 관리 단원을 참조하십시오.

2016년 5월 26일

이번 릴리스에서는 Route 53에 다음과 같은 새로운 기능이 추가되었습니다.

- 도메인 결제 보고서 - 지정된 기간 동안 모든 도메인 등록 요금이 도메인별로 나열된 보고서를 다운로드할 수 있습니다. 이 보고서에는 도메인 등록, Route 53로 도메인 이전, 도메인 등록 갱신, 도메인 소유자 변경(일부 TLD의 경우)을 비롯해 요금이 부과되는 모든 도메인 등록 작업이 포함됩니다. 자세한 내용은 다음 설명서를 참조하세요.
  - Route 53 콘솔 - 도메인 결제 보고서 다운로드 섹션 참조
  - Route 53 API - Amazon Route 53 API 참조의 ViewBilling을 참조하세요.
- 새 TLD - 이제 .college, .consulting, .host, .name, .online, .republican, .rocks, .sucks, .trade, .website 및 .uk. 같은 TLD를 사용하여 도메인을 등록할 수 있습니다. 자세한 내용은 Amazon Route 53에 등록할 수 있는 도메인 섹션을 참조하세요.
- 도메인 등록을 위한 새 API - 새 도메인 등록 등 등록자 연락처 이메일 주소가 유효한지 확인이 필요한 작업의 경우, 이제 확인 이메일에서 등록자 연락처가 링크를 클릭했는지, 클릭하지 않았다면 해당 링크가 여전히 유효한지 여부를 프로그래밍 방식으로 확인할 수 있습니다. 다른 확인 이메일을 보내도록 프로그래밍 방식으로 요청할 수도 있습니다. 자세한 내용은 Amazon Route 53 API 참조에서 다음과 같은 설명서를 참조하세요.
  - GetContactReachabilityStatus
  - ResendContactReachabilityEmail

2016년 4월 5일

이번 릴리스에서는 Route 53에 다음과 같은 새로운 기능이 추가되었습니다.

- CloudWatch 지표를 기반으로 상태 확인 - 이제 CloudWatch 지표의 경보 상태를 기반으로 상태 확인을 생성할 수 있습니다. 이 방법은 프라이빗 IP 주소만 있는 Amazon Virtual Private Cloud(VPC) 내의 인스턴스와 같이 표준 Route 53 상태 확인으로 도달할 수 없는 엔드포인트의 상태를 확인하는 데 유용합니다. 자세한 내용은 다음 설명서를 참조하세요.
  - Route 53 콘솔 - "상태 확인 생성 또는 업데이트 시 지정하는 값" 주제의 CloudWatch 경보 모니터링 섹션을 참조하세요.
  - Route 53 API - Amazon Route 53 API 참조의 CreateHealthCheck 및 UpdateHealthCheck를 참조하세요.
- 구성 가능한 상태 확인 위치 - 이제 리소스의 상태를 확인하는 Route 53 상태 확인 리전을 선택할 수 있습니다. 이렇게 하면 상태 확인으로 인해 엔드포인트에 적용되는 부하를 줄일 수 있습니다. 이 방법은 고객이 하나 또는 소수의 지리적 리전에 집중되는 경우에 유용합니다. 자세한 내용은 다음 설명서를 참조하세요.
  - Route 53 콘솔 - "상태 확인 생성 또는 업데이트 시 지정하는 값" 주제의 고급 구성("Monitor an endpoint" 전용) 섹션을 참조하세요.

    - Route 53 API - Amazon Route 53 API 참조에서 CreateHealthCheck 및 UpdateHealthCheck에 대한 `Regions` 요소를 참조하세요.
- 프라이빗 호스팅 영역의 장애 조치 - 프라이빗 호스팅 영역에서 장애 조치 및 장애 조치 별칭 레코드를 생성할 수 있습니다. 이 기능을 지표 기반 상태 확인과 결합하면 프라이빗 IP 주소만 있고 표준 Route 53 상태 확인을 사용하여 도달할 수 없는 엔드포인트에 대해서도 DNS 장애 조치를 구성할 수 있습니다. 자세한 내용은 다음 설명서를 참조하세요.
    - Route 53 콘솔 - 프라이빗 호스팅 영역에서 장애 조치 구성 섹션을 참조하세요.
    - Route 53 API - Amazon Route 53 API 참조에서 ChangeResourceRecordSets를 참조하세요.
- 프라이빗 호스팅 영역의 별칭 레코드 - 과거에는 동일한 호스팅 영역의 다른 Route 53 레코드로만 DNS 쿼리를 라우팅하는 별칭 레코드를 생성할 수 있었습니다. 이 릴리스에서는 리전화된 하위 도메인, Elastic Load Balancing 로드 밸런서 및 Amazon S3 버킷이 있는 Elastic Beanstalk 환경으로 DNS 쿼리를 라우팅하는 별칭 레코드도 생성할 수 있습니다. (DNS 쿼리를 CloudFront 배포로 라우팅하는 별칭 레코드는 여전히 생성할 수 없습니다.) 자세한 내용은 다음 설명서를 참조하세요.
    - Route 53 콘솔 - 별칭 또는 비 별칭 레코드 선택 섹션을 참조하세요.
    - Route 53 API - Amazon Route 53 API 참조에서 ChangeResourceRecordSets를 참조하세요.

2016년 2월 23일

HTTPS 상태 확인을 생성하거나 업데이트할 때 Route 53를 구성하여 TLS 협상 중에 엔드포인트로 호스트 이름을 보낼 수 있습니다. 그러면 엔드포인트에서 해당하는 SSL/TLS 인증서를 사용하여 HTTPS 요청에 응답할 수 있습니다. 자세한 내용은 '상태 확인 생성 또는 업데이트 시 지정하는 값' 주제에서 고급 구성("Monitor an endpoint" 전용) 필드의 SNI에 대한 설명을 참조하세요. API를 사용하여 상태 확인을 생성하거나 업데이트할 때 SNI를 활성화하는 방법에 대한 자세한 내용은 Amazon Route 53 API 참조의 CreateHealthCheck 및 UpdateHealthCheck를 참조하세요.

2016년 1월 27일

이제 .accountants, .band, .city 등 100개 이상의 최상위 도메인(TLD)의 도메인을 등록할 수 있습니다. 지원되는 TLD 전체 목록은 Amazon Route 53에 등록할 수 있는 도메인 단원을 참조하십시오.

2016년 1월 19일

이제 Elastic Beanstalk 환경으로 트래픽을 라우팅하는 별칭 레코드를 생성할 수 있습니다. Route 53 콘솔을 사용하여 레코드를 생성하는 방법에 대한 자세한 내용은 Amazon Route 53 콘솔을 사용하여 레코드 생성 섹션을 참조하세요. API를 사용하여 레코드를 생성하는 방법에 대한 자세한 내용은 Amazon Route 53 API 참조의 ChangeResourceRecordSets를 참조하세요.

2015 릴리스

2015년 12월 3일

이제 Route 53 콘솔에는 Route 53 가중치 기반, 지연, 장애 조치 및 지리 위치 라우팅 정책의 조합을 사용하는 복잡한 라우팅 구성을 빠르게 만들 수 있는 시각적 편집기가 포함되어 있습니다. 그런 다음 동일한 호스팅 영역이나 여러 호스팅 영역의 하나 이상의 도메인 이름(예: example.com) 또는 하위 도메인 이름(예: www.example.com)과 해당 구성을 연결할 수 있습니다. 새 구성이 예상대로 수행되지 않을 경우 업데이트를 롤백할 수도 있습니다. Route 53 API, AWS SDKs, AWS CLI및 를 사용하여 동일한 기능을 사용할 수 있습니다 AWS Tools for Windows PowerShell. 시각적 편집기 사용에 대한 자세한 내용은 트래픽 흐름을 사용하여 DNS 트래픽 라우팅 단원을 참조하십시오. API를 사용하여 트래픽 흐름 구성을 생성하는 방법에 대한 자세한 내용은 Amazon Route 53 API 참조를 참조하세요.

2015년 10월 19일

이번 릴리스에서는 Route 53에 다음과 같은 새로운 기능이 추가되었습니다.

- Amazon Registrar, Inc.의 .com 및 .net 도메인에 대한 도메인 등록 - 이제 Amazon은 Amazon Registrar, Inc.를 통해 .com 및 .net 최상위 도메인(TLD)에 대한 ICANN 인가 등록 기관입니다. Route 53를 사용하여 .com 또는 .net 도메인을 등록하면 Amazon Registrar가 레코드 등록 기관이 되어 Whois 쿼리 결과에 “스폰서 등록 기관(Sponsoring Registrar)”으로 나열됩니다. Route 53를 사용하여 도메인을 등록하는 방법에 대한 자세한 내용은 Amazon Route 53를 사용하여 도메인 등록 및 관리 섹션을 참조하세요.
- .com 및 .net 도메인에 대한 개인 정보 보호 - Route 53를 사용하여 .com 또는 .net 도메인을 등록할 경우 이제 성 및 이름을 비롯한 모든 개인 정보가 숨겨집니다. Route 53를 사용하여 등록하는 다른 도메인에 대해서는 성 및 이름이 숨겨지지 않습니다. 개인 정보 보호에 대한 자세한 내용은 도메인 연락처 정보의 개인 정보 보호 활성화 또는 비활성화 단원을 참조하십시오.

2015년 9월 15일

이번 릴리스에서는 Route 53에 다음과 같은 새로운 기능이 추가되었습니다.

- 계산된 상태 확인 – 다른 상태 확인의 상태에 의해 상태가 결정되는 상태 확인을 생성할 수 있습니다. 자세한 내용은 상태 확인의 생성 및 업데이트 섹션을 참조하세요. 또한 Amazon Route 53 API 참조의 CreateHealthCheck을 참조하세요.
- 상태 확인을 위한 지연 시간 측정 - Route 53를 구성하여 상태 확인 프로그램과 엔드포인트 사이의 지연 시간을 측정할 수 있습니다. 지연 시간 데이터는 Route 53 콘솔의 Amazon CloudWatch 그래프에 표시됩니다. 새 상태 확인에 대한 대기 시간 측정을 활성화하려면 상태 확인 생성 또는 업데이트 시 지정하는 값 주제의 고급 구성("Monitor an endpoint" 전용)에서 지연 시간 측정 설정

을 참조하세요. (기존 상태 확인에 대한 지연 시간 측정을 활성화할 수 없습니다.) 또한, Amazon Route 53 API 참조의 CreateHealthCheck 주제에서 MeasureLatency를 참조하세요.

- Route 53 콘솔에서 상태 확인 대시보드로 업데이트 - 상태 확인 모니터링을 위한 대시보드가 다양한 방식으로 개선되었으며, 여기에는 Route 53 상태 확인 프로그램과 엔드포인트 사이의 지연 시간 모니터링을 위한 CloudWatch 그래프가 포함됩니다. 자세한 내용은 상태 확인의 상태 모니터링 및 알림 수신 섹션을 참조하세요.

2015년 3월 3일

Amazon Route 53 개발자 안내서에서는 이제 Route 53 호스팅 영역에 대해 화이트 레이블 이름 서버를 구성하는 방법을 설명합니다. 자세한 내용은 화이트 레이블 이름 서버 구성 섹션을 참조하세요.

2015년 2월 26일

이제 Route 53 API를 사용하여 AWS 계정과 연결된 호스팅 영역을 이름별로 알파벳 순으로 나열할 수 있습니다. 또한 계정과 연결된 호스팅 영역의 개수를 가져올 수 있습니다. 자세한 내용은 Amazon Route 53 API 참조에서 ListHostedZonesByName 및 GetHostedZoneCount를 참조하세요.

2015년 2월 11일

이번 릴리스에서는 Route 53에 다음과 같은 새로운 기능이 추가되었습니다.

- 상태 확인 상태 - 이제 Route 53 콘솔의 상태 확인 페이지에 모든 상태 확인의 전체 상태를 볼 수 있는 상태 열이 포함됩니다. 자세한 내용은 상태 확인의 상태 및 상태 확인 실패 이유 보기 단원을 참조하십시오.
- 통합 AWS CloudTrail - Route 53는 이제 CloudTrail과 함께 작동하여 AWS 계정이 Route 53 API로 보내는 모든 요청에 대한 정보를 캡처합니다. Route 53와 CloudTrail을 통합하면 Route 53 API에 대해 이뤄진 요청의 종류, 각 요청이 이뤄진 소스 IP 주소, 요청한 사람, 요청이 이뤄진 시기 등을 확인할 수 있습니다. 자세한 내용은 를 사용하여 Amazon Route 53 API 호출 로깅 AWS CloudTrail 섹션을 참조하세요.
- 상태 확인에 대한 빠른 경보 - Route 53 콘솔을 사용하여 상태 확인을 생성하는 동시에 Route 53에서 엔드포인트가 1분간 비정상으로 인식될 때 Amazon CloudWatch 상태 확인 경보를 생성하고 경보를 받을 사람도 지정할 수 있습니다. 자세한 내용은 상태 확인의 생성 및 업데이트 섹션을 참조하세요.
- 호스팅 영역 및 도메인에 대한 태그 지정 - 이제 일반적으로 Route 53 호스팅 영역 및 도메인으로 비용 할당에 사용되는 태그를 배정할 수 있습니다. 자세한 내용은 Amazon Route 53 리소스 태그 지정 섹션을 참조하세요.

2015년 2월 5일

이제 Route 53 콘솔을 사용하여 도메인에 대한 연락처 정보를 업데이트할 수 있습니다. 자세한 내용은 도메인을 등록하거나 이전할 때 지정하는 값 섹션을 참조하세요.

2015년 1월 22일

이제 Route 53에 새 도메인 이름을 등록할 때 국제화된 도메인 이름을 지정할 수 있습니다. (Route 53에서는 호스팅 영역 및 레코드에 대한 국제화된 도메인 이름을 이미 지원하고 있습니다.) 자세한 내용은 DNS 도메인 이름 형식 섹션을 참조하세요.

2014 릴리스

2014년 11월 25일

이번 릴리스에서는 호스팅 영역을 생성할 때 지정한 설명을 편집할 수 있습니다. 콘솔에서 [Comment] 필드 옆의 연필 아이콘을 클릭한 다음 새 값을 입력하면 됩니다. Route 53 API를 사용하여 설명을 변경하는 방법에 대한 자세한 내용은 Amazon Route 53 API 참조의 UpdateHostedZoneComment를 참조하세요.

2014년 11월 5일

이번 릴리스에서는 Route 53에 다음과 같은 새로운 기능이 추가되었습니다.

- Amazon Virtual Private Cloud 서비스로 생성한 VPC용 프라이빗 DNS - 이제 Route 53를 사용하여 퍼블릭 인터넷에 DNS 데이터를 노출하지 않고 VPC의 내부 도메인 이름을 관리할 수 있습니다. 자세한 내용은 프라이빗 호스팅 영역 사용 섹션을 참조하세요.
- 상태 확인 실패 사유 - 이제 선택된 상태 확인의 현재 상태 및 각 Route 53 상태 확인 프로그램에서 보고한 상태 확인 실패의 세부 정보를 볼 수 있습니다. 상태에는 문자열 일치 실패 및 응답 시간 초과 등 수많은 실패 유형에 대한 정보 등 실패 사유 및 HTTP 상태 코드가 포함됩니다. 자세한 내용은 상태 확인의 상태 및 상태 확인 실패 이유 보기 섹션을 참조하세요.
- 재사용 가능한 위임 세트 - 이제 동일한 권한 이름 서버 4개 세트(위임 세트)를 다양한 도메인 이름에 해당하는 여러 호스팅 영역에 적용할 수 있습니다. 이렇게 하면 DNS 서비스를 Route 53로 마이그레이션하는 프로세스를 대폭 간소화하고, 수많은 호스팅 영역을 관리할 수 있습니다. 현재 재사용 가능한 위임 세트를 사용하려면 Route 53 API 또는 AWS SDK를 사용해야 합니다. 자세한 내용은 Amazon Route 53 API Reference를 확인하십시오.
- 지리적 라우팅 개선 - Amazon은 EDNS0의 edns-client-subnet 확장자에 대한 지원을 강화하여 지리적 라우팅의 정확성을 더욱 높였습니다. 자세한 내용은 지리적 라우팅 섹션을 참조하세요.

- 서명 버전 4에 대한 지원 - 이제 모든 Route 53 API 요청에 서명 버전 4로 서명할 수 있습니다. 자세한 내용은 Amazon Route 53 API 참조의 Route 53 API 요청 서명을 참조하세요.

2014년 7월 31일

이번 릴리스부터는 다음을 수행할 수 있습니다.

- Route 53를 사용하여 새 도메인 이름을 등록합니다. 자세한 내용은 Amazon Route 53를 사용하여 도메인 등록 및 관리 섹션을 참조하세요.
- 쿼리가 시작된 지리적 위치에 따라 DNS 쿼리에 응답하도록 Route 53를 구성할 수 있습니다. 자세한 내용은 지리적 라우팅 섹션을 참조하세요.

2014년 7월 2일

이번 릴리스부터는 다음을 수행할 수 있습니다.

- 상태 확인의 값 대부분을 편집할 수 있습니다. 자세한 내용은 상태 확인의 생성, 업데이트 및 삭제 섹션을 참조하세요.
- Route 53 API를 사용하여 Route 53 상태 확인 프로그램이 리소스 상태 확인에 사용하는 IP 범위 목록을 가져옵니다. 이러한 IP 주소로 라우터 및 방화벽 규칙을 구성하여 상태 확인 프로그램이 리소스 상태를 확인하도록 할 수 있습니다. 자세한 내용은 Amazon Route 53 API 참조의 GetCheckerIpRanges를 참조하세요.
- 상태 확인에 비용 할당 태그를 지정하면 상태 확인에 이름을 지정할 수 있습니다. 자세한 내용은 상태 확인에 대한 이름 및 태그 지정 단원을 참조하십시오.
- Route 53 API를 사용하여 AWS 계정과 연결된 상태 확인 수를 가져옵니다. 자세한 내용은 Amazon Route 53 API 참조의 GetHealthCheckCount를 참조하세요.

2014년 4월 30일

이번 릴리스부터는 상태 확인을 생성하고 IP 주소 대신 도메인 이름을 사용하여 엔드포인트를 지정할 수 있습니다. 이렇게 하면 엔드포인트의 IP 주소가 고정되지 않았거나 Amazon EC2 또는 Amazon RDS 인스턴스 등 여러 IP에서 IP 주소를 제공할 때 유용합니다. 자세한 내용은 상태 확인의 생성 및 업데이트 섹션을 참조하세요.

또한, Route 53 API를 사용하는 방법에 대한 몇 가지 정보는 전에 있었던 Amazon Route 53 개발자 안내서에서 이동하였습니다. 이제 모든 API 설명서는Amazon Route 53 API 참조에 있습니다.

2014년 4월 18일

이 릴리스에서 Route 53는 상태 확인포트 값이 443이고 프로토콜 값이 HTTPS인 경우 `Host` 헤더의 다른 값을 전달합니다. 상태 확인 중에 Route 53는 엔드포인트에 호스트 이름 필드 값을 포함하

는 Host 헤더를 전달합니다. CreateHealthCheck API 작업을 사용하여 상태 확인을 생성한 경우, 이것이 FullyQualifiedDomainName 요소의 값이 됩니다.

자세한 내용은 상태 확인의 생성, 업데이트 및 삭제 섹션을 참조하세요.

2014년 4월 9일

이번 릴리스에서는 Route 53 상태 확인 프로그램에서 현재 보고하는 정상 엔드포인트의 비율을 확인할 수 있습니다.

또한 Amazon CloudWatch의 상태 확인 상태 지표는 0(주어진 시간 동안 엔드포인트가 비정상인 경우) 또는 1(주어진 시간 동안 엔드포인트가 정상인 경우)만 보여줍니다. 엔드포인트가 정상임을 보고하는 Route 53 상태 확인 부분에 따라 더 이상 지표에 0~1 사이의 값이 표시되지 않습니다.

자세한 내용은 CloudWatch를 이용한 상태 확인 모니터링 섹션을 참조하세요.

2014년 2월 18일

이번 릴리스에서는 Route 53에 다음과 같은 새로운 기능이 추가되었습니다.

- 상태 확인 장애 조치 임계값: 이제 Route 53가 엔드포인트를 비정상 상태로 간주하는 엔드포인트 상태 확인의 연속 실패 횟수를 1~10회 사이로 지정할 수 있습니다. 비정상 엔드포인트는 같은 횟수의 확인을 통과해야 정상 상태로 간주됩니다. 자세한 내용은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 섹션을 참조하세요.
- 상태 확인 요청 간격: 엔드포인트의 정상 여부를 결정하기 위해 Route 53가 엔드포인트로 보내는 요청의 횟수를 지정할 수 있습니다. 유효한 설정은 10초에서 30초 사이입니다. 자세한 내용은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 섹션을 참조하세요.

2014년 1월 30일

이번 릴리스에서는 Route 53에 다음과 같은 새로운 기능이 추가되었습니다.

- HTTP 및 HTTPS 문자열 매치 상태 확인: Route 53는 이제 응답 본문에 지정된 문자열의 모양에 따라 엔드포인트의 상태를 결정하는 상태 확인을 지원합니다. 자세한 내용은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 섹션을 참조하세요.
- HTTPS 상태 확인: Route 53는 이제 안전한 SSL 전용 웹 사이트를 위한 상태 확인을 지원합니다. 자세한 내용은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 섹션을 참조하세요.
- **ChangeResourceRecordSets** API 작업에 대한 **UPSERT**: 이제 ChangeResourceRecordSets API 작업을 사용하여 레코드를 생성하거나 변경할 때 UPSERT 작업으로 새 레코드를 생성하거나(이름 및 유형이 없는 경우) 기존 레코드를 업데이트할 수 있습니다. 자세한 내용은 Amazon Route 53 API 참조의 ChangeResourceRecordSets를 참조하세요.

2014년 1월 7일

이번 릴리스에서 Route 53는 응답 본문에 지정된 문자열이 있는지 여부에 따라 엔드포인트의 상태를 결정하는 상태 확인을 추가로 지원합니다. 자세한 내용은 Amazon Route 53가 상태 확인이 정상인지 여부를 판단하는 방법 섹션을 참조하세요.

2013 릴리스

2013년 8월 14일

이번 릴리스부터 Route 53는 BIND 형식의 영역 파일을 가져와 레코드를 생성할 수 있도록 추가 지원합니다. 자세한 내용은 영역 파일을 가져와 레코드 생성 섹션을 참조하세요.

더불어 Route 53 상태 확인에 대한 CloudWatch 지표를 Route 53 콘솔에 통합하고 간소화했습니다. 자세한 내용은 CloudWatch를 이용한 상태 확인 모니터링 섹션을 참조하세요.

2013년 6월 26일

이번 릴리스부터 Route 53는 상태 확인에 CloudWatch 지표를 통합하여 다음 작업을 수행할 수 있도록 추가로 지원합니다.

- 상태 확인이 적절하게 구성되었는지 확인합니다.
- 상태 확인 엔드포인트의 상태를 지정된 기간 동안 검토합니다.
- 모든 Route 53 상태 확인 프로그램이 지정된 엔드포인트를 비정상으로 간주하는 경우 Amazon Simple Notification Service(Amazon SNS) 알림을 보내도록 CloudWatch를 구성합니다.

자세한 내용은 CloudWatch를 이용한 상태 확인 모니터링 섹션을 참조하세요.

2013년 6월 11일

이번 릴리스부터 Route 53는 DNS 쿼리를 Amazon CloudFront 배포의 대체 도메인 이름으로 라우팅하는 별칭 레코드 생성을 추가로 지원합니다. 이 기능을 Zone Apex의 대체 도메인 이름(example.com)과 하위 도메인의 대체 도메인 이름(www.example.com)에 모두 사용할 수 있습니다. 자세한 내용은 도메인 이름을 사용하여 Amazon CloudFront 배포로 트래픽 라우팅 섹션을 참조하세요.

2013년 5월 30일

이번 릴리스부터 Route 53는 ELB 로드 밸런서 및 연결된 Amazon EC2 인스턴스의 상태를 평가할 수 있도록 추가 지원합니다. 자세한 내용은 Amazon Route 53 상태 확인 생성 섹션을 참조하세요.

2013년 3월 28일

상태 확인 및 장애 조치에 대한 설명서를 다시 작성하여 활용도를 높였습니다. 자세한 내용은 Amazon Route 53 상태 확인 생성 섹션을 참조하세요.

2013년 2월 11일

이번 릴리스부터 Route 53는 장애 조치 및 상태 확인을 추가로 지원합니다. 자세한 내용은 Amazon Route 53 상태 확인 생성 섹션을 참조하세요.

2012 릴리스

2012년 3월 21일

이번 릴리스부터 Route 53에서 지연 시간 레코드를 생성할 수 있습니다. 자세한 내용은 지연 시간 기반 라우팅 섹션을 참조하세요.

2011 릴리스

2011년 12월 21일

이 릴리스에서는의 Route 53 콘솔을 AWS Management Console 사용하여 호스팅 영역 ID와 Load Balancer서의 DNS 이름을 수동으로 입력하는 대신 목록에서 Elastic Load Balancer를 선택하여 별칭 레코드를 생성할 수 있습니다. 새로운 기능이 Amazon Route 53 개발자 안내서에 설명되어 있습니다.

2011년 11월 16일

이 릴리스에서는의 Route 53 콘솔 AWS Management Console 을 사용하여 호스팅 영역을 생성 및 삭제하고 레코드를 생성, 변경 및 삭제할 수 있습니다. 새로운 기능이 Amazon Route 53 개발자 안내서 전체에 걸쳐 해당 부분에 설명되어 있습니다.

2011년 10월 18일

Amazon Route 53 시작 안내서는 Amazon Route 53 개발자 안내서에 통합되었으며, 개발자 안내서는 유용성을 향상시키기 위해 재구성되었습니다.

2011년 5월 24일

Amazon Route 53의 이번 릴리스에는 zone apex 별칭, 가중치 기반 레코드, 새로운 API(2011-05-05), 서비스 수준 계약을 생성할 수 있도록 별칭 레코드를 도입했습니다. 또한 6개

월의 베타 기간이 지나면 Route 53를 상용 버전으로 사용할 수 있습니다. 자세한 내용은 Amazon Route 53 개발자 안내서의 Amazon Route 53 제품 페이지 및 별칭 또는 비 별칭 레코드 선택를 참조하세요.

2010 릴리스

2010년 12월 5일

이 안내서는 Amazon Route 53 개발자 안내서의 최초 릴리스입니다.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.