사용자 가이드

AWS Amplify 호스팅

AWS Amplify 호스팅: 사용자 가이드

Table of Contents

AWS Amplify 호스팅에 오신 것을 환영합니다

Amplify Hosting은 연속 배포를 통해 풀 스택 서버리스 웹 애플리케이션을 호스팅하기 위한 Git 기반 워크플로를 제공합니다. Amplify는 앱을 AWS 글로벌 콘텐츠 전송 네트워크 (CDN) 에 배포합니다. 이 사용 설명서는 Amplify Hosting을 시작하는 데 필요한 정보를 제공합니다.

지원되는 프레임워크

Amplify Hosting은 다음을 포함하여 많은 일반 SSR 프레임워크, 단일 페이지 애플리케이션 (SPA) 프레임워크 및 정적 사이트 생성기를 지원합니다.

SSR 프레임워크

- Next.js
- Nuxt
- 커뮤니티 어댑터를 사용하는 Astro
- SvelteKit 커뮤니티 어댑터 사용
- 사용자 지정 어댑터가 있는 모든 SSR 프레임워크

SPA 프레임워크

- React
- Angular(각)
- Vue.js
- 이오니아
- 사계 대재일의

정적 사이트 생성기

- 일레븐티
- 개츠비
- 휴고
- 지킬
- VuePress

Amplify Hosting 기능

피처 브랜치

새로운 브랜치를 연결하여 프런트엔드 및 백엔드용 프로덕션 및 스테이징 환경을 관리합니다.

사용자 지정 도메인

애플리케이션을 사용자 지정 도메인에 연결합니다.

풀 리퀘스트 프리뷰

코드 검토 중에 변경 사항을 미리 볼 수 있습니다.

E nd-to-end 테스트

end-to-end 테스트를 통해 앱 품질을 개선하세요.

비밀번호로 보호된 브랜치

암호로 웹 애플리케이션을 보호하므로 공개적으로 액세스할 수 없어도 새로운 기능을 사용할 수 있습니다.

리디렉션 및 재작성

다시 쓰기 및 리디렉션을 설정하여 SEO 순위를 유지하고 클라이언트 앱 요구 사항에 따라 트래픽을 라우팅합니다.

아토믹 디플로이먼트

Atomic 배포는 전체 배포가 완료된 후에만 웹 앱이 업데이트되도록 하여 유지 관리 기간을 없애줍니다. 이렇게 하면 파일을 제대로 업로드하지 못하는 시나리오가 제거됩니다.

Amplify 호스팅 시작하기

Amplify 호스팅을 시작하려면 자습서를 참조하십시오. Amplify Hosting 시작하기 자습서를 완료하면 Git 리포지토리 (, GitHub BitBucket GitLab, 또는 AWS CodeCommit) 에서 웹 앱을 연결하고 연속 배포를 통해 Amplify Hosting에 배포하는 방법을 알게 됩니다.

백엔드를 구축하세요.

AWS Amplify Gen 2에서는 백엔드를 정의하기 TypeScript 위한 코드 우선 기반의 개발자 환경을 도입합니다. Amplify Gen 2를 사용하여 백엔드를 빌드하고 앱에 연결하는 방법을 알아보려면 Amplify 문서에서 백엔드 구축 및 연결을 참조하십시오.

CLI와 Amplify Studio를 사용하여 1세대 앱을 위한 백엔드를 구축하는 방법에 대한 설명서를 찾으려면 1세대 Amplify 문서에서 백엔드 구축 및 연결을 참조하십시오.

Amplify 호스팅 가격

AWS Amplify 의 AWS 프리 티어일부입니다. 무료로 시작한 다음 프리 티어 한도를 초과하면 사용한 만큼 지불할 수 있습니다. Amplify 호스팅 요금에 대한 자세한 내용은 요금을 참조하십시오AWS Amplify .

Amplify Hosting 시작하기

Amplify Hosting의 작동 방식을 이해하는 데 도움이 되도록 이 자습서에서는 Git 리포지토리에서 Next.js 애플리케이션을 빌드하고 배포하는 방법을 안내합니다.

주제

필수 조건

이 자습서를 시작하기 전에 다음 사전 요구 사항을 완료하세요.

등록하여 AWS 계정

아직 AWS 고객이 아닌 경우 온라인 지침에 따라 AWS 계정가입해야 합니다. 가입하면 Amplify 및 애플리케이션과 함께 사용할 수 있는 기타 AWS 서비스에 액세스할 수 있습니다.

애플리케이션 생성

Next.js 설명서의 create-next-app지침에 따라 이 자습서에 사용할 기본 Next.js 애플리케이션을 만드십시오.

Git 리포지토리 만들기

Amplify는 비트버킷 GitHub, GitLab 및 을 지원합니다. AWS CodeCommit`create-next-app`애플리케이션을 Git 리포지토리로 푸시합니다.

1단계: Git 리포지토리 연결

이 단계에서는 Git 리포지토리의 Next.js 애플리케이션을 Amplify 호스팅에 연결합니다.

Git 리포지토리의 앱을 연결하려면

1. Amplify 콘솔을 엽니다.
2. 현재 지역에 첫 번째 앱을 배포하는 경우 기본적으로 AWS Amplify서비스 페이지에서 시작하게 됩니다.

   a. 페이지 상단에서 새 앱 만들기를 선택합니다.

   b. 페이지 하단에서 시작 방법 섹션을 찾아 새 앱 만들기를 선택합니다.
3. Amplify로 빌드 시작 페이지에서 Git 리포지토리 공급자를 선택한 후 다음을 선택합니다.

   GitHub 리포지토리의 경우 Amplify는 GitHub 앱 기능을 사용하여 Amplify 액세스를 승인합니다. 앱 설치 및 인증에 대한 자세한 내용은 을 참조하십시오. GitHub GitHub 리포지토리에 대한 Amplify 액세스 설정

   > **Note**
   >
   > GitLabBitbucket을 사용하여 Amplify 콘솔을 승인하면 Amplify는 리포지토리 공급자로부터 액세스 토큰을 가져오지만 토큰을 서버에 저장하지는 않습니다. AWS CodeCommit AWS Amplify는 특정 리포지토리에만 설치된 배포 키를 사용하여 리포지토리에 액세스합니다.
4. 리포지토리 브랜치 추가 페이지에서 다음을 수행하십시오.

   a. 연결할 리포지토리의 이름을 선택합니다.

   b. 연결할 리포지토리 브랜치의 이름을 선택합니다.

   c. 다음을 선택합니다.

2단계: 빌드 설정 확인

Amplify는 배포 중인 브랜치에 대해 실행할 빌드 명령 시퀀스를 자동으로 감지합니다. 이 단계에서는 빌드 설정을 검토하고 확인합니다.

앱의 빌드 설정을 확인하려면

1. 앱 설정 페이지에서 빌드 설정 섹션을 찾으세요.

   프런트엔드 빌드 명령과 빌드 출력 디렉터리가 올바른지 확인하세요. 이 Next.js 예제 앱의 경우 빌드 출력 디렉터리는 로 `.next` 설정되어 있습니다.

2. 서비스 역할을 추가하는 절차는 새 역할을 만들지 아니면 기존 역할을 사용할지에 따라 달라집니다.
   - 새 역할을 만들려면:
     - 새 서비스 역할 생성 및 사용을 선택합니다.
   - 기존 역할을 사용하려면:
     a. 기존 역할 사용을 선택합니다.
     b. 서비스 역할 목록에서 사용할 역할을 선택합니다.
3. 다음을 선택합니다.

3단계: 애플리케이션 배포

이 단계에서는 AWS 글로벌 콘텐츠 전송 네트워크 (CDN) 에 앱을 배포합니다.

앱을 저장하고 배포하려면

1. 검토 페이지에서 리포지토리 세부 정보 및 앱 설정이 올바른지 확인합니다.
2. 저장 및 배포를 선택합니다. 프런트 엔드 빌드는 일반적으로 1~2분 정도 소요되지만 앱 크기에 따라 달라질 수 있습니다.
3. 배포가 완료되면 `amplifyapp.com` 기본 도메인으로 연결되는 링크를 사용하여 앱을 볼 수 있습니다.

> **Note**
>
> Amplify 애플리케이션의 보안을 강화하기 위해 amplifyapp.com 도메인은 공개 서픽스 목록(PSL)에 등록되어 있습니다. 보안 강화를 위해 Amplify 애플리케이션의 기본 도메인 이름에 민감한 쿠키를 설정해야 하는 경우, `__Host-` 접두사가 있는 쿠키를 사용하는 것이 좋습니다. 이렇게 쿠키를 설정하면 교차 사이트 요청 위조 시도(CSRF)로부터 도메인을 보호하는 데 도움이 됩니다. 자세한 내용은 Mozilla 개발자 네트워크의 Set-Cookie 페이지를 참조하십시오.

4단계: (선택사항) 리소스 정리

자습서를 위해 배포한 앱이 더 이상 필요하지 않은 경우 삭제할 수 있습니다. 이렇게 하면 사용하지 않는 리소스에 요금이 청구되지 않습니다.

앱을 삭제하려면

1. 탐색 패널의 앱 설정 메뉴에서 일반 설정을 선택합니다.
2. 일반 설정 페이지에서 앱 삭제를 선택합니다. 확인 창에서 를 입력합니다**delete**. 그런 다음 앱 삭제를 선택합니다.

앱에 기능 추가

이제 Amplify에 앱을 배포했으므로 호스팅된 응용 프로그램에서 사용할 수 있는 다음 기능 중 일부를 살펴볼 수 있습니다.

환경 변수

응용 프로그램에는 런타임 시 구성 정보가 필요한 경우가 많습니다. 이러한 구성은 데이터베이스 연결 세부 정보, API 키 또는 매개변수일 수 있습니다. 환경 변수는 빌드 시 이러한 구성을 노출하는 방법을 제공합니다. 자세한 내용은 환경 변수를 참조하십시오.

사용자 지정 도메인

이 자습서에서 Amplify는 다음과 같은 URL을 사용하여 기본 `amplifyapp.com` 도메인에서 앱을 호스팅합니다. `https://branch-name.d1m7bkiki6tdw1.amplifyapp.com` 앱을 사용자 지정 도메인에 연결하면 사용자는 앱이 `https://www.example.com`과 같은 사용자 지정 URL에서 호스팅되는 것을 볼 수 있습니다. 자세한 내용은 사용자 지정 도메인 설정을 참조하십시오.

pull 요청 미리 보기

웹 풀 리퀘스트 미리보기를 통해 팀은 코드를 프로덕션 또는 통합 브랜치에 병합하기 전에 풀 리퀘스트 (PR) 의 변경 사항을 미리 볼 수 있습니다. 자세한 내용은 풀 리퀘스트의 웹 미리보기를 참조하십시오.

여러 환경 관리

Amplify가 기능 분기 및 GitFlow 워크플로와 함께 작동하여 다중 배포를 지원하는 방법을 알아보려면 기능 분기 배포 및 팀 워크플로를 참조하세요.

Amplify Hosting을 통해 서버 측 렌더링 앱 배포

를 사용하여 서버 측 렌더링 (SSR) AWS Amplify 을 사용하는 웹 앱을 배포하고 호스팅할 수 있습니다. Amplify Hosting에서는 Next.js 프레임워크를 사용하여 생성한 애플리케이션이 자동으로 감지되며 AWS Management Console에서 수동으로 구성할 필요가 없습니다. Amplify에서는 애플리케이션의 빌드 출력을 Amplify Hosting에서 예상하는 디렉터리 구조로 변환하는 오픈 소스 빌드 어댑터가 있는 Javascript 기반 SSR 프레임워크도 지원됩니다.

Amplify가 SSR을 지원하는 방법에 대해 알아보려면 다음 주제를 검토하십시오.

주제

- 서버 측 렌더링 소개
- SSR 프레임워크를 위한 Amplify 지원
- Amplify Hosting 배포 사양을 참조하여 빌드 출력 구성
- SSR 앱을 위한 이미지 최적화
- Next.js 앱에 대한 Node.js 버전 지원
- SSR 배포 문제 해결
- Next.js 지원을 Amplify

서버 측 렌더링 소개

Amplify에서는 React와 같이 단일 페이지 애플리케이션(SPA) 프레임워크로 만든 정적 웹 앱이나 Gatsby와 같이 정적 사이트 생성기(SSG)로 만든 앱의 배포 및 호스팅이 지원됩니다. 정적 웹 앱은 HTML, CSS, 파일 등의 JavaScript 파일 조합으로 구성되며 CDN (콘텐츠 전송 네트워크) 에 저장됩니다. 클라이언트 브라우저가 웹사이트에 요청을 보내면, 서버는 HTTP 응답과 함께 페이지를 클라이언트에 반환하고 클라이언트 브라우저는 콘텐츠를 해석하여 사용자에게 표시합니다.

Amplify에서는 서버 측 렌더링(SSR)을 사용하는 웹 앱도 지원됩니다. 클라이언트가 SSR 페이지에 요청을 보내면 각 요청마다 페이지의 HTML이 서버에 생성됩니다. 개발자는 SSR을 통해 요청 및 사용자별로 웹사이트를 사용자 지정할 수 있습니다. 또한 SSR은 웹사이트의 성능 및 검색 엔진 최적화(SEO)를 개선할 수 있습니다.

SSR 프레임워크를 위한 Amplify 지원

Amplify 호스팅은 Amplify에서 예상하는 빌드 출력을 준수하는 배포 번들이 포함된 모든 JavaScript 기반 SSR 프레임워크를 지원합니다. Amplify Hosting에서는 애플리케이션의 모든 SSR 프레임워크를 위한 빌드 출력의 파일 및 디렉터리 구조를 표준화하는 배포 사양이 제공됩니다.

프레임워크 작성자는 파일 시스템 기반 배포 사양을 참조하여 특정 프레임워크용으로 사용자 지정한 오픈 소스 빌드 어댑터를 개발할 수 있습니다. 이러한 어댑터에서는 앱의 빌드 출력이 Amplify Hosting의 예상 디렉터리 구조에 부합하는 배포 번들로 변환됩니다. 이 배포 번들에는 라우팅 규칙과 같은 런타임 구성을 비롯해 앱을 호스팅하는 데 필요한 모든 파일과 자산이 포함됩니다.

프레임워크 또는 프레임워크 어댑터를 사용하지 않는다면 자체 솔루션을 개발하여 Amplify Hosting의 예상 디렉터리 구조에 부합하는 배포 번들을 생성하면 됩니다.

Amplify Hosting에서는 정적 자산, 컴퓨팅, 이미지 최적화, 라우팅 규칙과 같은 기본 요소가 지원됩니다. 이러한 기본 요소를 활용하여 기능이 더 풍부한 애플리케이션을 배포할 수 있습니다. 각 기본 요소에 대한 자세한 내용은 Amplify SSR 기본 요소 지원 섹션을 참조하세요.

다음 시나리오 중에서 선택하여 Amplify에 SSR 앱 배포를 시작하세요.

Next.js 앱 배포

Amplify에서는 어댑터나 콘솔의 수동 구성 없이 Next.js를 사용하여 만든 애플리케이션이 지원됩니다. 자세한 정보는 Next.js 지원을 Amplify을 참조하세요.

프레임워크 어댑터가 사용된 앱 배포

SSR 앱을 Amplify Hosting에 배포할 때 사용 가능한 모든 오픈 소스 프레임워크 어댑터를 참조할 수 있습니다. 자세한 정보는 프레임워크 어댑터 사용을 참조하세요.

Nuxt 프레임워크에 어댑터를 사용할 수 있습니다. 이 어댑터 사용에 대한 자세한 내용은 Nuxt 설명서를 참조하세요.

프레임워크 어댑터 빌드

프레임워크 제공 기능을 통합하려는 프레임워크 작성자는 Amplify Hosting 배포 사양을 참조하여 Amplify의 예상 구조에 부합하도록 빌드 출력을 구성할 수 있습니다. 자세한 정보는 배포 매니페스트를 사용하여 Express 서버 배포을 참조하세요.

빌드 후 스크립트 구성

Amplify Hosting 배포 사양을 참조하여 특정 시나리오에 필요한 대로 빌드 출력을 조작할 수 있습니다. 자세한 정보는 Amplify Hosting 배포 사양을 참조하여 빌드 출력 구성을 참조하세요. 예시는 배포 매니페스트를 사용하여 Express 서버 배포단원을 참조하세요.

Amplify에 SSR 앱 배포

이 주제의 지침을 참조하여 Amplify의 예상 빌드 출력에 부합하는 배포 번들과 모든 프레임워크로 만든 앱을 배포할 수 있습니다. Next.js 애플리케이션을 배포하는 경우 어댑터가 필요하지 않습니다.

프레임워크 어댑터가 사용되는 SSR 앱을 배포한다면 먼저 어댑터를 설치하고 구성해야 합니다. 지침은 프레임워크 어댑터 사용을 참조하세요.

Amplify Hosting에 SSR 앱을 배포하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 모든 앱 페이지에서 새 앱 생성을 선택합니다.
3. Amplify로 빌드 시작 페이지에서 Git 리포지토리 공급자를 선택한 후 다음을 선택합니다.
4. 리포지토리 브랜치 추가 페이지에서 다음을 수행하십시오.

   a. 연결할 리포지토리의 이름을 선택합니다.
   b. 연결할 리포지토리 브랜치의 이름을 선택합니다.
   c. 다음을 선택합니다.
5. 앱 설정 페이지에서 Amplify는 Next.js SSR 앱을 자동으로 탐지합니다.

   다른 프레임워크용 어댑터를 사용하는 SSR 앱을 배포하는 경우 Amazon Logs를 명시적으로 활성화해야 합니다. CloudWatch 고급 설정 섹션을 연 다음 서버 측 렌더링 (SSR) 배포 섹션에서 SSR 앱 로그 활성화를 선택합니다.
6. Amplify가 AWS 계정으로 로그를 전달하는 IAM 서비스 역할이 앱에 필요합니다.

   서비스 역할을 추가하는 절차는 새 역할을 만들지 기존 역할을 사용할지에 따라 달라집니다.
   - 새 역할을 만들려면:
     - 새 서비스 역할 생성 및 사용을 선택합니다.
   - 기존 역할을 사용하려면:

     a. 기존 역할 사용을 선택합니다.

b. 서비스 역할 목록에서 사용할 역할을 선택합니다.

7. 다음을 선택합니다.
8. 검토 페이지에서 저장 및 배포를 선택합니다.

프레임워크 어댑터 사용

Amplify Hosting과 통합용으로 생성된 모든 SSR 프레임워크 빌드 어댑터를 설치하고 사용할 수 있습니다. 어댑터가 제공되는 각 프레임워크에 따라 어댑터가 구성되고 빌드 프로세스에 연결되는 방식이 결정됩니다. 일반적으로 npm 개발 종속 항목으로 어댑터를 설치하게 됩니다.

프레임워크로 앱을 만든 후에는 프레임워크 설명서에 따라 Amplify Hosting 어댑터를 설치하고 애플리케이션의 구성 파일에서 어댑터를 구성하는 방법을 알아보세요.

다음으로, 프로젝트의 루트 디렉터리에 `amplify.yml` 파일을 생성합니다. `amplify.yml` 파일에서 `baseDirectory`를 애플리케이션의 빌드 출력 디렉터리에 설정합니다. 프레임워크에서는 빌드 프로세스 중에 어댑터가 실행되어 출력이 Amplify Hosting 배포 번들로 변환됩니다.

빌드 출력 디렉터리의 이름은 무엇이든 상관없지만, `.amplify-hosting` 파일 이름은 중요합니다. Amplify에서는 먼저 `baseDirectory`로 정의된 디렉터리를 찾습니다. 디렉터리가 있으면 Amplify에서는 거기에서 빌드 출력을 찾습니다. 디렉터리가 없으면 고객이 정의하지 않았더라도 Amplify가 `.amplify-hosting` 내부에서 빌드 출력을 찾습니다.

다음은 앱의 빌드 설정 예시입니다. 빌드 출력이 `.amplify-hosting` 폴더에 있다는 것을 나타내도록 `baseDirectory`가 `.amplify-hosting`으로 설정되어 있습니다. `.amplify-hosting` 폴더의 콘텐츠가 Amplify Hosting 배포 사양과 일치하기만 하면 앱이 배포됩니다.

```
version: 1
frontend:
  preBuild:
    commands:
      - npm install
  build:
    commands:
      - npm run build
  artifacts:
    baseDirectory: .amplify-hosting
```

프레임워크 어댑터가 사용되도록 앱을 구성한 후 Amplify Hosting에 배포할 수 있습니다. 자세한 지침은 Amplify에 SSR 앱 배포 단원을 참조하십시오.

Amplify Hosting 배포 사양을 참조하여 빌드 출력 구성

Amplify 배포 사양을 참조하여 Amplify Hosting과 통합하려는 SSR 프레임워크용 빌드 출력을 구성합니다. 프레임워크 작성자는 배포 사양을 토대로 Amplify의 예상 빌드 출력을 구조화하는 방법을 이해할 수 있습니다. 프레임워크를 사용하지 않는다면 자체 솔루션을 개발하여 Amplify의 예상 빌드 출력을 생성할 수 있습니다.

Amplify Hosting 배포 사양

Amplify Hosting 배포 사양은 Amplify Hosting으로 배포를 촉진하도록 디렉터리 구조를 정의하는 파일 시스템 기반 사양입니다. 프레임워크에서는 Amplify Hosting의 서비스 기본 요소가 프레임워크에서 활용되도록 이러한 예상 디렉터리 구조를 빌드 명령의 출력으로 생성할 수 있습니다. Amplify Hosting은 배포 번들의 구조를 파악하고 적절히 배포합니다.

다음은 Amplify에서 예상하는 배포 번들 폴더 구조의 예시입니다. 상위 수준에는 이름이 `static`인 폴더, 이름이 `compute`인 폴더 및 이름이 `deploy-manifest.json`인 배포 매니페스트 파일이 있습니다.

```
.amplify-hosting/
### compute/
#   ### default/
#       ### chunks/
#       #   ### app/
#       #       ### _nuxt/
#       #       #   ### index-xxx.mjs
#       #       #   ### index-styles.xxx.js
#       #       ### server.mjs
#       ### node_modules/
#       ### server.js
### static/
#   ### css/
#   #   ### nuxt-google-fonts.css
#   ### fonts/
#   #   ### font.woff2
#   ### _nuxt/
#   #   ### builds/
#   #   #   ### latest.json
#   #   ### entry.xxx.js
#   ### favicon.ico
#   ### robots.txt
### deploy-manifest.json
```

Amplify SSR 기본 요소 지원

Amplify Hosting 배포 사양에는 다음과 같은 기본 요소에 긴밀하게 매핑되는 계약이 정의됩니다.

정적 자산

정적 파일을 호스팅하는 기능을 프레임워크에 제공합니다.

컴퓨팅

포트 3000에서 Node.js HTTP 서버를 실행하는 기능을 프레임워크에 제공합니다.

이미지 최적화

런타임 시 이미지를 최적화하는 서비스를 프레임워크에 제공합니다.

라우팅 규칙

수신되는 요청 경로를 특정 대상에 매핑하는 메커니즘을 프레임워크에 제공합니다.

.amplify-hosting/static 디렉터리

애플리케이션 URL에서 제공하기로 되어 있으며 공개적으로 액세스할 수 있는 모든 정적 파일을 `.amplify-hosting/static` 디렉터리에 배치해야 합니다. 이 디렉터리 내부의 파일은 정적 자산 기본 요소를 통해 제공됩니다.

정적 파일은 콘텐츠, 파일 이름 또는 확장명을 변경하지 않고 애플리케이션 URL의 루트(/)에서 액세스할 수 있습니다. 또한 하위 디렉터리는 URL 구조에 보존되며 파일 이름 앞에 표시됩니다. 예를 들면 `.amplify-hosting/static/favicon.ico`는 `https://myAppId.amplify-hostingapp.com/favicon.ico`에서 제공되고 `.amplify-hosting/static/_nuxt/main.js`는 `https://myAppId.amplify-hostingapp.com/_nuxt/main.js`에서 제공됩니다.

프레임워크에서 애플리케이션의 기본 경로를 수정하는 기능이 지원되면 `.amplify-hosting/static` 디렉터리 내부의 정적 자산 앞에 기본 경로를 추가해야 합니다. 예를 들어 기본 경로가 `/folder1/folder2`인 경우에는 `main.css`라는 정적 자산의 빌드 출력이 `.amplify-hosting/static/folder1/folder2/main.css`가 됩니다.

.amplify-hosting/compute 디렉터리

단일 컴퓨팅 리소스는 `.amplify-hosting/compute` 디렉터리 내에 포함된 `default`라는 단일 하위 디렉터리로 표시됩니다. 경로는 `.amplify-hosting/compute/default`입니다. 이 컴퓨팅 리소스는 Amplify Hosting의 컴퓨팅 기본 요소에 매핑됩니다.

default 하위 디렉터리의 콘텐츠는 다음 규칙을 준수해야 합니다.

- 컴퓨팅 리소스의 진입점 역할을 하려면 파일이 default 하위 디렉터리의 루트에 있어야 합니다.
- 진입점 파일은 Node.js 모듈이어야 하며 포트 3000에서 수신 대기하는 HTTP 서버가 시작되어야 합니다.
- 다른 파일을 default 하위 디렉터리에 배치하고 진입점 파일의 코드에서 해당 파일을 참조할 수 있습니다.
- 하위 디렉터리의 콘텐츠는 독립적이어야 합니다. 진입점 모듈의 코드에서는 하위 디렉터리 외부의 모듈을 참조할 수 없습니다. 참고로, 프레임워크에서는 원하는 방식으로 HTTP 서버를 번들링할 수 있습니다. 하위 디렉터리 내에서 항목 파일의 이름이 server.js is인 node server.js 명령으로 컴퓨팅 프로세스를 시작할 수 있으면 Amplify에서는 디렉터리 구조가 배포 사양을 준수하는 것으로 간주합니다.

Amplify Hosting에서는 default 하위 디렉터리 내부의 모든 파일을 번들링하여 프로비저닝한 컴퓨팅 리소스에 배포합니다. 각 컴퓨팅 리소스에는 512MB의 임시 스토리지가 할당됩니다. 이 스토리지는 실행 인스턴스 간에 공유되지 않지만, 동일한 실행 인스턴스 내의 후속 간접 호출 간에는 공유됩니다. 실행 인스턴스의 최대 실행 시간은 15분으로 제한되며, 실행 인스턴스 내 쓰기 가능한 경로는 /tmp 디렉터리뿐입니다. 각 컴퓨팅 리소스 번들의 압축된 크기는 220MB를 초과할 수 없습니다. 예를 들어 .amplify/compute/default 하위 디렉터리는 압축 시 220MB를 초과할 수 없습니다.

.amplify-hosting/deploy-manifest.json 파일

deploy-manifest.json 파일을 사용하여 배포의 구성 세부 정보와 메타데이터를 저장합니다. deploy-manifest.json 파일에는 최소한 version 속성, catch-all 라우팅이 지정된 routes 속성, 프레임워크 메타데이터가 지정된 framework 속성이 포함되어야 합니다.

다음 객체 정의에서는 배포 매니페스트의 구성을 보여줍니다.

```
type DeployManifest = {
  version: 1;
  routes: Route[];
  computeResources?: ComputeResource[];
  imageSettings?: ImageSettings;
  framework: FrameworkMetadata;
};
```

다음 주제에서는 배포 매니페스트의 각 속성에 대한 세부 정보 및 사용법을 설명합니다.

version 속성 사용

`version` 속성에서는 구현 중인 배포 사양의 버전이 정의됩니다. 현재 Amplify Hosting 배포 사양의 버전은 버전 1뿐입니다. 다음 JSON 예시에서는 `version` 속성의 사용법을 보여줍니다.

```
"version": 1
```

routes 속성 사용

`routes` 속성을 통해 프레임워크에서 Amplify Hosting 라우팅 규칙 기본 요소를 활용할 수 있습니다. 라우팅 규칙은 수신되는 요청 경로를 배포 번들의 특정 대상으로 라우팅하는 메커니즘을 제공합니다. 라우팅 규칙은 수신되는 요청의 목적지만 지정하며, 다시 쓰기 및 리디렉션 규칙에 따라 요청이 변환된 후에 라우팅 규칙이 적용됩니다. Amplify Hosting에서 다시 쓰기와 리디렉션을 처리하는 방식에 대한 자세한 내용은 리디렉션 사용 섹션을 참조하세요.

라우팅 규칙은 요청을 다시 쓰거나 변환하지 않습니다. 수신되는 요청이 라우팅의 경로 패턴과 일치하면 요청이 그대로 대상에 라우팅됩니다.

`routes` 배열에 지정된 라우팅 규칙에서는 다음과 같은 규칙을 준수해야 합니다.

- catch-all 라우팅이 지정되어야 합니다. catch-all 라우팅에는 수신되는 모든 요청과 일치하는 `/*` 패턴이 있습니다.
- `routes` 배열에는 최대 25개 항목이 포함될 수 있습니다.
- `Static` 경로 또는 `Compute` 경로를 지정해야 합니다.
- `Static` 경로를 지정하는 경우 `.amplify-hosting/static` 디렉터리가 있어야 합니다.
- `Compute` 경로를 지정하는 경우 `.amplify-hosting/compute` 디렉터리가 있어야 합니다.
- `ImageOptimization` 경로를 지정하는 경우 `Compute` 경로도 지정해야 합니다. 완전히 정적인 애플리케이션에는 아직 이미지 최적화가 지원되지 않기 때문에 이 작업이 필요합니다.

다음 객체 정의에서는 `Route` 객체의 구성을 보여줍니다.

```
type Route = {
  path: string;
  target: Target;
  fallback?: Target;
}
```

다음 테이블에는 `Route` 객체의 속성이 설명되어 있습니다.

키	유형	필수	설명
경로	String	예	수신되는 요청 경로와 일치하는 패턴을 정의합니다(쿼리 문자열 제외). 최대 경로 길이는 255자입니다. 경로는 슬래시(/)로 시작해야 합니다. 경로에는 [A-Z], [a-z], [0-9], [_-.*$/~"'@:+] 문자가 포함될 수 있습니다. 패턴 일치에는 다음과 같은 와일드카드 문자만 지원됩니다. • *(0개 이상의 문자와 일치) • 이 /* 패턴은 catch-all 패턴이라고 하며 수신되는 모든 요청과 일치합니다.
대상	대상	예	일치하는 요청을 라우팅할 대상이 정의되는 객체입니다. Compute 경로를 지정하면 해당하는 ComputeResource 가 있어야 합니다.

키	유형	필수	설명
			ImageOptimization 경로를 지정하면 imageSettings 도 지정해야 합니다.
fallback	대상	아니요	원래 대상에서 404 오류가 반환되는 경우 대체할 대상이 정의되는 객체입니다. 지정한 경로의 target 종류와 fallback 종류는 같을 수 없습니다. 예를 들면 Static에서 Static으로의 대체는 허용되지 않습니다. 본문이 없는 GET 요청에만 대체가 지원됩니다. 요청에 본문이 있으면 대체 중에 본문이 삭제됩니다.

다음 객체 정의에서는 Target 객체의 구성을 보여줍니다.

```
type Target = {
  kind: TargetKind;
  src?: string;
  cacheControl?: string;
}
```

다음 테이블에는 Target 객체의 속성이 설명되어 있습니다.

키	유형	필수	설명
kind	Targetkind	예	대상 유형이 정의되는 enum입니다. 유효한 값은 `Static`, `Compute`, `ImageOptimization` 입니다.
src	String	`Compute`의 경우 예 기타 기본 요소의 경우 아니요	기본 요소의 실행 코드가 포함되어 있는 배포 번들의 하위 디렉터리 이름이 지정되는 문자열입니다. 컴퓨팅 기본 요소의 경우에만 유효하고 필요합니다. 값은 배포 번들에 있는 컴퓨팅 리소스 중 하나를 가리켜야 합니다. 현재 이 필드에서 지원되는 유일한 값은 `default`입니다.
cacheControl	String	아니요	응답에 적용할 Cache-Control 헤더의 값을 지정하는 문자열입니다. 정적 및 ImageOptimization 프리미티브에만 유효합니다. 지정한 값은 사용자 지정 헤더에 의해 재정의됩니다. Amplify Hosting 사용자 지정 헤더에 대한 자세한 내

키	유형	필수	설명
			용은 사용자 지정 헤더 섹션을 참조하세요. Note 이 Cache-Control 헤더는 상태 코드가 200 (OK) 으로 설정된 성공적인 응답에만 적용됩니다.

다음 객체 정의에서는 `TargetKind` 열거의 사용법을 보여줍니다.

```
enum TargetKind {
  Static = "Static",
  Compute = "Compute",
  ImageOptimization = "ImageOptimization"
}
```

다음 목록을 통해 `TargetKind` 열거형의 유효한 값이 지정됩니다.

정적

요청을 정적 자산 기본 요소로 라우팅합니다.

컴퓨팅

요청을 컴퓨팅 기본 요소로 라우팅합니다.

ImageOptimization

요청을 이미지 최적화 기본 요소로 라우팅합니다.

다음 JSON 예시에서는 여러 라우팅 규칙이 지정된 `routes` 속성의 사용법을 보여줍니다.

```
"routes": [
```

```
    {
      "path": "/_nuxt/image",
      "target": {
        "kind": "ImageOptimization",
        "cacheControl": "public, max-age=3600, immutable"
      }
    },
    {
      "path": "/_nuxt/builds/meta/*",
      "target": {
        "cacheControl": "public, max-age=31536000, immutable",
        "kind": "Static"
      }
    },
    {
      "path": "/_nuxt/builds/*",
      "target": {
        "cacheControl": "public, max-age=1, immutable",
        "kind": "Static"
      }
    },
    {
      "path": "/_nuxt/*",
      "target": {
        "cacheControl": "public, max-age=31536000, immutable",
        "kind": "Static"
      }
    },
    {
      "path": "/*.*",
      "target": {
        "kind": "Static"
      },
      "fallback": {
        "kind": "Compute",
        "src": "default"
      }
    },
    {
      "path": "/*",
      "target": {
        "kind": "Compute",
        "src": "default"
      }
```

```
    }
  ]
```

배포 매니페스트의 라우팅 규칙 지정에 대한 자세한 내용은 라우팅 규칙 구성 모범 사례 섹션을 참조하세요.

computeResources 속성 사용

프로비저닝한 컴퓨팅 리소스에 대한 메타데이터가 이 computeResources 속성을 통해 프레임워크에서 제공될 수 있습니다. 모든 컴퓨팅 리소스는 해당하는 경로와 연결되어 있어야 합니다.

다음 객체 정의에서는 ComputeResource 객체의 사용법을 보여줍니다.

```
type ComputeResource = {
  name: string;
  runtime: ComputeRuntime;
  entrypoint: string;
};

type ComputeRuntime = 'nodejs16.x' | 'nodejs18.x' | 'nodejs20.x';
```

다음 테이블에는 ComputeResource 객체의 속성이 설명되어 있습니다.

키	유형	필수	설명
이름	String	예	컴퓨팅 리소스의 이름을 지정합니다. 이름은 .amplify-hosting/compute directory 내부의 하위 디렉터리 이름과 일치해야 합니다. 배포 사양 버전 1의 경우 유효한 값은 default뿐입니다.

키	유형	필수	설명
런타임	ComputeRuntime	예	프로비저닝한 컴퓨팅 리소스의 런타임을 정의합니다. 유효한 값은 `nodejs16.x` , `nodejs18.x` , `nodejs20.x` 입니다.
entrypoint	String	예	지정한 컴퓨팅 리소스에 대해 코드가 실행될 시작 파일의 이름을 지정합니다. 파일은 컴퓨팅 리소스를 나타내는 하위 디렉터리 내부에 있어야 합니다.

다음과 같은 디렉터리 구조가 있는 경우입니다.

```
.amplify-hosting
|---compute
|   |---default
|       |---index.js
```

`computeResource` 속성의 JSON은 다음과 같습니다.

```
"computeResources": [
    {
      "name": "default",
      "runtime": "nodejs16.x",
      "entrypoint": "index.js",
    }
  ]
```

imageSettings 속성 사용

이 `imageSettings` 속성을 통해 런타임 시 이미지의 온디맨드 최적화가 제공되는 이미지 최적화 기본 요소의 동작을 프레임워크에서 사용자 지정할 수 있습니다.

다음 객체 정의에서는 `ImageSettings` 객체의 사용법을 보여줍니다.

```
type ImageSettings = {
  sizes: number[];
  domains: string[];
  remotePatterns: RemotePattern[];
  formats: ImageFormat[];
  minumumCacheTTL: number;
  dangerouslyAllowSVG: boolean;
};

type ImageFormat = 'image/avif' | 'image/webp' | 'image/png' | 'image/jpeg';
```

다음 테이블에는 `ImageSettings` 객체의 속성이 설명되어 있습니다.

키	유형	필수	설명
크기	Number[]	예	지원되는 이미지 너비의 배열입니다.
domains	String[]	예	이미지 최적화를 사용하도록 허용된 외부 도메인의 배열입니다. 배포 도메인에서만 이미지 최적화가 사용되도록 하려면 배열을 비워 둡니다.
remotePatterns	RemotePattern[]	예	이미지 최적화를 사용하도록 허용된 외부 패턴의 배열입니다. 도메인과 비슷하지만, 정규 표현식(regex)이 제공되어 추가로 제어할 수 있습니다.

키	유형	필수	설명
formats	ImageFormat[]	예	허용된 출력 이미지 형식의 배열입니다.
minimumCacheTTL	숫자	예	최적화된 이미지의 캐시 기간(초)입니다.
dangerouslyAllowSVG	불	예	SVG 입력 이미지 URL을 허용합니다. 보안을 위해 기본적으로 비활성화되어 있습니다.

다음 객체 정의에서는 `RemotePattern` 객체의 사용법을 보여줍니다.

```
type RemotePattern = {
  protocol?: 'http' | 'https';
  hostname: string;
  port?: string;
  pathname?: string;
}
```

다음 테이블에는 `RemotePattern` 객체의 속성이 설명되어 있습니다.

키	유형	필수	설명
프로토콜	String	아니요	허용된 원격 패턴의 프로토콜입니다. 유효한 값은 `http` 또는 `https`입니다.
hostname	String	예	허용된 원격 패턴의 호스트 이름입니다. 리터럴 또는 와일드카드를 지정할 수 있습니다. 1개(`*`)는 하나의 하위 도메인과 일치합

키	유형	필수	설명
			니다. 2개(`**`)는 모든 하위 도메인의 수와 일치합니다. Amplify에서는 `**`만 지정하는 포괄적인 와일드카드가 허용되지 않습니다.
포트	String	아니요	허용된 원격 패턴의 포트입니다.
pathname	String	아니요	허용된 원격 패턴의 경로 이름입니다.

다음 예시에서는 `imageSettings` 속성을 보여줍니다.

```
"imageSettings": {
    "sizes": [
      100,
      200
    ],
    "domains": [
      "example.com"
    ],
    "remotePatterns": [
      {
        "protocol": "https",
        "hostname": "example.com",
        "port": "",
        "pathname": "/**",
      }
    ],
    "formats": [
      "image/webp"
    ],
    "minumumCacheTTL": 60,
    "dangerouslyAllowSVG": false
  }
```

framework 속성 사용

`framework` 속성을 사용하여 프레임워크 메타데이터를 지정합니다.

다음 객체 정의에서는 `FrameworkMetadata` 객체의 구성을 보여줍니다.

```
type FrameworkMetadata = {
  name: string;
  version: string;
}
```

다음 테이블에는 `FrameworkMetadata` 객체의 속성이 설명되어 있습니다.

키	유형	필수	설명
이름	String	예	프레임워크의 이름입니다.
version	String	예	프레임워크의 버전입니다. 유효한 의미 체계 버전 관리(semver) 문자열이어야 합니다.

라우팅 규칙 구성 모범 사례

라우팅 규칙에서는 수신되는 요청 경로를 배포 번들의 특정 대상으로 라우팅하는 메커니즘이 제공됩니다. 배포 번들에서 프레임워크 작성자는 다음과 같은 대상 중 하나에 배포되는 파일을 빌드 출력에 내보낼 수 있습니다.

- 정적 자산 기본 요소 – 파일이 `.amplify-hosting/static` 디렉터리에 포함되어 있습니다.
- 컴퓨팅 기본 요소 – 파일이 `.amplify-hosting/compute/default` 디렉터리에 포함되어 있습니다.

프레임워크 작성자는 라우팅 규칙 배열도 배포 매니페스트 파일로 제공합니다. 배열의 각 규칙은 일치 항목이 있을 때까지 수신되는 요청과 순차적인 순회 순서로 대조됩니다. 일치하는 규칙이 있으면 일치

하는 규칙에 지정된 대상에 요청이 라우팅됩니다. 규칙마다 대체 대상을 지정할 수도 있습니다. 원래 대상에서 404 오류를 반환하면 요청이 대체 대상으로 라우팅됩니다.

배포 사양에서는 순회 순서의 마지막 규칙이 catch-all 규칙이 되어야 합니다. catch-all 규칙은 /* 경로와 함께 지정됩니다. 수신되는 요청이 라우팅 규칙 배열의 이전 경로와 전혀 일치하지 않으면 요청이 catch-all 규칙 대상으로 라우팅됩니다.

SSR 프레임워크(예: Nuxt.js)의 경우 catch-all 규칙 대상이 컴퓨팅 기본 요소여야 합니다. SSR 애플리케이션에는 빌드 시 예측할 수 없는 경로로 렌더링된 서버 측 페이지가 있기 때문입니다. 예를 들어 /blog/[slug]에 Nuxt.js 애플리케이션의 페이지가 있으면 [slug]가 동적 경로 파라미터입니다. catch-all 규칙 대상은 요청을 이러한 페이지에 라우팅하는 유일한 방법입니다.

이와 달리 특정 경로 패턴을 사용하여 빌드 시 알려진 경로를 대상으로 지정할 수 있습니다. 예를 들면 /_nuxt에서는 정적 자산이 Nuxt.js 경로에서 제공됩니다. 따라서 요청을 정적 자산 기본 요소로 라우팅하는 특정 라우팅 규칙에 따라 /_nuxt/* 경로를 대상으로 지정할 수 있습니다.

퍼블릭 폴더 라우팅

대다수 SSR 프레임워크는 public 폴더에 있는 변경 가능한 정적 자산을 사용하는 기능이 제공됩니다. favicon.ico 및 robots.txt와 같은 파일은 일반적으로 public 내부에 유지되며 애플리케이션의 루트 URL에서 제공됩니다. 예를 들면 favicon.ico 파일은 https://example.com/favicon.ico에서 제공됩니다. 참고로, 이러한 파일에는 예측 가능한 경로 패턴이 없습니다. 거의 전적으로 파일 이름에 따라 결정됩니다. public 폴더 내부의 파일을 대상으로 지정하는 유일한 방법은 catch-all 라우팅을 사용하는 것입니다. 그러나 catch-all 라우팅 대상은 컴퓨팅 기본 요소여야 합니다.

public 폴더 관리에는 다음과 같은 접근 방식 중 하나를 따르는 것이 좋습니다.

1. 경로 패턴을 사용하여 파일 확장명이 있는 요청 경로를 대상으로 지정합니다. 예를 들면 /*.*를 사용하여 파일 확장명이 있는 모든 요청 경로를 대상으로 지정할 수 있습니다.

   참고로, 이 접근 방식은 신뢰할 수 없습니다. 예를 들면 public 폴더에 속한 파일에 파일 확장명이 없다면 해당 파일은 이 규칙에 따라 대상으로 지정되지 않습니다. 이 접근 방식에서 유의할 다른 문제는 이름에 마침표가 있는 페이지가 애플리케이션에 있을 수 있다는 점입니다. 예를 들면 /blog/2021/01/01/hello.world의 페이지가 /*.* 규칙에 따라 대상으로 지정됩니다. 페이지는 정적 자산이 아니므로 이는 바람직하지 않습니다. 그러나 정적 기본 요소에서 404 오류가 발생하는 경우 요청이 컴퓨팅 기본 요소로 대체되도록 이 규칙에 대체 대상을 추가할 수 있습니다.

```
{
    "path": "/*.*",
    "target": {
```

```
        "kind": "Static"
    },
    "fallback": {
        "kind": "Compute",
        "src": "default"
    }
}
```

2. 빌드 시 public 폴더의 파일을 식별하고 각 파일에 대한 라우팅 규칙을 내보냅니다. 배포 사양에 따라 규칙이 25개로 제한되므로 이 접근 방식은 확장할 수 없습니다.

```
{
    "path": "/favicon.ico",
    "target": {
        "kind": "Static"
    }
},
{
    "path": "/robots.txt",
    "target": {
        "kind": "Static"
    }
}
```

3. 프레임워크 사용자는 변경 가능한 모든 정적 자산을 public 폴더의 하위 폴더에 저장하는 것이 좋습니다.

   다음 예시에서는 사용자가 변경 가능한 모든 정적 자산을 public/assets 폴더에 저장할 수 있습니다. 그런 다음 경로 패턴이 /assets/*인 라우팅 규칙을 사용하여 public/assets 폴더의 모든 변경 가능한 정적 자산을 대상으로 지정할 수 있습니다.

```
{
    "path": "/assets/*",
    "target": {
        "kind": "Static"
    }
}
```

4. catch-all 라우팅에 대한 정적 대체를 지정합니다. 이 접근 방식에는 단점이 있으며 다음 catch-all 대체 라우팅 섹션에 자세히 설명되어 있습니다.

catch-all 대체 라우팅

컴퓨팅 기본 요소 대상에 대해 catch-all 라우팅이 지정된 SSR 프레임워크(예: Nuxt.js)의 경우 프레임워크 작성자가 `public` 폴더 라우팅 문제를 해결하려면 catch-all 라우팅에 대한 정적 대체를 지정하는 것이 좋습니다. 그러나 이 라우팅 규칙 유형은 서버 측에서 렌더링한 404 페이지를 중단시킵니다. 예를 들어 최종 사용자가 존재하지 않는 페이지를 방문하면 애플리케이션에서는 상태 코드가 404인 404 페이지를 렌더링합니다. 그러나 catch-all 라우팅에 정적 대체가 있으면 404 페이지가 렌더링되지 않습니다. 대신에 요청은 정적 기본 요소로 대체되고 여전히 404 상태 코드로 끝나지만, 404 페이지는 렌더링되지 않습니다.

```
{
    "path": "/*",
    "target": {
        "kind": "Compute",
        "src": "default"
    },
    "fallback": {
        "kind": "Static"
    }
}
```

기본 경로 라우팅

애플리케이션의 기본 경로를 수정하는 기능이 제공되는 프레임워크에서는 `.amplify-hosting/static` 디렉터리 내부의 정적 자산 앞에 기본 경로를 추가할 것으로 예상됩니다. 예를 들어 기본 경로가 `/folder1/folder2`인 경우에는 main.css라는 정적 자산의 빌드 출력이 `.amplify-hosting/static/folder1/folder2/main.css`가 됩니다.

따라서 기본 경로가 반영되도록 라우팅 규칙도 업데이트해야 합니다. 예를 들어 기본 경로가 `/folder1/folder2`인 경우에는 `public` 폴더의 정적 자산에 대한 라우팅 규칙은 다음과 같습니다.

```
{
    "path": "/folder1/folder2/*.*",
    "target": {
        "kind": "Static"
    }
}
```

마찬가지로 서버 측 경로도 앞에 기본 경로를 추가해야 합니다. 예를 들어 기본 경로가 `/folder1/folder2`인 경우에는 `/api` 경로에 대한 라우팅 규칙은 다음과 같습니다.

```
{
    "path": "/folder1/folder2/api/*",
    "target": {
        "kind": "Compute",
        "src": "default"
    }
}
```

그러나 catch-all 라우팅 앞에는 기본 경로를 추가하면 안 됩니다. 예를 들어 기본 경로가 `/folder1/folder2`인 경우에는 catch-all 라우팅이 다음과 같이 유지됩니다.

```
{
    "path": "/*",
    "target": {
        "kind": "Compute",
        "src": "default"
    }
}
```

Nuxt.js 경로 예시

다음은 라우팅 규칙을 지정하는 방법을 보여주는 Nuxt 애플리케이션의 예시 `deploy-manifest.json` 파일입니다.

```
{
  "version": 1,
  "routes": [
    {
      "path": "/_nuxt/image",
      "target": {
        "kind": "ImageOptimization",
        "cacheControl": "public, max-age=3600, immutable"
      }
    },
    {
      "path": "/_nuxt/builds/meta/*",
      "target": {
        "cacheControl": "public, max-age=31536000, immutable",
        "kind": "Static"
      }
    },
    {
```

```
      "path": "/_nuxt/builds/*",
      "target": {
        "cacheControl": "public, max-age=1, immutable",
        "kind": "Static"
      }
    },
    {
      "path": "/_nuxt/*",
      "target": {
        "cacheControl": "public, max-age=31536000, immutable",
        "kind": "Static"
      }
    },
    {
      "path": "/*.*",
      "target": {
        "kind": "Static"
      },
      "fallback": {
        "kind": "Compute",
        "src": "default"
      }
    },
    {
      "path": "/*",
      "target": {
        "kind": "Compute",
        "src": "default"
      }
    }
  ],
  "computeResources": [
    {
      "name": "default",
      "entrypoint": "server.js",
      "runtime": "nodejs18.x"
    }
  ],
  "framework": {
    "name": "nuxt",
    "version": "3.8.1"
  }
}
```

다음은 기본 경로가 포함된 라우팅 규칙을 지정하는 방법을 보여주는 Nuxt의 예시 `deploy-manifest.json` 파일입니다.

```
{
  "version": 1,
  "routes": [
    {
      "path": "/base-path/_nuxt/image",
      "target": {
        "kind": "ImageOptimization",
        "cacheControl": "public, max-age=3600, immutable"
      }
    },
    {
      "path": "/base-path/_nuxt/builds/meta/*",
      "target": {
        "cacheControl": "public, max-age=31536000, immutable",
        "kind": "Static"
      }
    },
    {
      "path": "/base-path/_nuxt/builds/*",
      "target": {
        "cacheControl": "public, max-age=1, immutable",
        "kind": "Static"
      }
    },
    {
      "path": "/base-path/_nuxt/*",
      "target": {
        "cacheControl": "public, max-age=31536000, immutable",
        "kind": "Static"
      }
    },
    {
      "path": "/base-path/*.*",
      "target": {
        "kind": "Static"
      },
      "fallback": {
        "kind": "Compute",
        "src": "default"
      }
```

```
    },
    {
      "path": "/*",
      "target": {
        "kind": "Compute",
        "src": "default"
      }
    }
  ],
  "computeResources": [
    {
      "name": "default",
      "entrypoint": "server.js",
      "runtime": "nodejs18.x"
    }
  ],
  "framework": {
    "name": "nuxt",
    "version": "3.8.1"
  }
}
```

`routes` 속성에 대한 자세한 내용은 routes 속성 사용 섹션을 참조하세요.

배포 매니페스트를 사용하여 Express 서버 배포

이 예시에서는 Amplify Hosting 배포 사양을 참조하여 기본 Express 서버를 배포하는 방법을 설명합니다. 제공된 배포 매니페스트를 활용하여 라우팅, 컴퓨팅 리소스 및 기타 구성을 지정할 수 있습니다.

Amplify Hosting에 배포하기 전에 로컬로 Express 서버 설정

1. 프로젝트의 새 디렉터리를 만들고 Express와 Typescript를 설치합니다.

```
mkdir express-app
cd express-app

# The following command will prompt you for information about your project
npm init

# Install express, typescript and types
npm install express --save
npm install typescript ts-node @types/node @types/express --save-dev
```

2. 프로젝트의 루트에 다음과 같은 콘텐츠가 포함된 `tsconfig.json` 파일을 추가합니다.

```
{
  "compilerOptions": {
    "target": "es6",
    "module": "commonjs",
    "outDir": "./dist",
    "strict": true,
    "esModuleInterop": true,
    "skipLibCheck": true,
    "forceConsistentCasingInFileNames": true
  },
  "include": ["src/**/*.ts"],
  "exclude": ["node_modules"]
}
```

3. 프로젝트 루트에 `src`라는 디렉터리를 만듭니다.

4. `src` 디렉터리에 `index.ts` 파일을 만듭니다. 이 파일이 애플리케이션에서 Express 서버가 시작되는 진입점이 됩니다. 포트 3000에서 수신 대기하도록 서버를 구성해야 합니다.

```
// src/index.ts
import express from 'express';

const app: express.Application = express();
const port = 3000;

app.use(express.text());

app.listen(port, () => {
  console.log(`server is listening on ${port}`);
});

// Homepage
app.get('/', (req: express.Request, res: express.Response) => {
  res.status(200).send("Hello World!");
});

// GET
app.get('/get', (req: express.Request, res: express.Response) => {
  res.status(200).header("x-get-header", "get-header-value").send("get-response-
from-compute");
```

```
});

//POST
app.post('/post', (req: express.Request, res: express.Response) => {
  res.status(200).header("x-post-header", "post-header-
value").send(req.body.toString());
});

//PUT
app.put('/put', (req: express.Request, res: express.Response) => {
  res.status(200).header("x-put-header", "put-header-
value").send(req.body.toString());
});

//PATCH
app.patch('/patch', (req: express.Request, res: express.Response) => {
  res.status(200).header("x-patch-header", "patch-header-
value").send(req.body.toString());
});

// Delete
app.delete('/delete', (req: express.Request, res: express.Response) => {
  res.status(200).header("x-delete-header", "delete-header-value").send();
});
```

5. 다음과 같은 스크립트를 package.json 파일에 추가합니다.

```
"scripts": {
  "start": "ts-node src/index.ts",
  "build": "tsc",
  "serve": "node dist/index.js"
}
```

6. 프로젝트의 루트에 public이라는 디렉터리를 만듭니다. 그런 다음에 다음과 같은 콘텐츠가 포함된 hello-world.txt라는 파일을 만듭니다.

```
Hello world!
```

7. 프로젝트 루트에 다음과 같은 콘텐츠가 포함된 .gitignore 파일을 추가합니다.

```
.amplify-hosting
dist
```

```
node_modules
```

Amplify 배포 매니페스트 설정

1. 프로젝트의 루트 디렉터리에 `deploy-manifest.json`이라는 파일을 만듭니다.
2. 다음 매니페스트를 복사하여 `deploy-manifest.json` 파일에 붙여넣습니다.

```
{
  "version": 1,
  "framework": { "name": "express", "version": "4.18.2" },
  "imageSettings": {
    "sizes": [
      100,
      200,
      1920
    ],
    "domains": [],
    "remotePatterns": [],
    "formats": [],
    "minimumCacheTTL": 60,
    "dangerouslyAllowSVG": false
  },
  "routes": [
    {
      "path": "/_amplify/image",
      "target": {
        "kind": "ImageOptimization",
        "cacheControl": "public, max-age=3600, immutable"
      }
    },
    {
      "path": "/*.*",
      "target": {
        "kind": "Static",
        "cacheControl": "public, max-age=2"
      },
      "fallback": {
        "kind": "Compute",
        "src": "default"
      }
    },
    {
```

```
      "path": "/*",
      "target": {
        "kind": "Compute",
        "src": "default"
      }
    }
  ],
  "computeResources": [
    {
      "name": "default",
      "runtime": "nodejs18.x",
      "entrypoint": "index.js"
    }
  ]
}
```

매니페스트는 Amplify Hosting에서 애플리케이션 배포를 처리하는 방식을 설명합니다. 기본 설정은 다음과 같습니다.

- version – 사용 중인 배포 사양의 버전을 나타냅니다.
- framework – 이를 조정하여 Express 서버 설정을 지정합니다.
- imageSettings – 이미지 최적화를 처리하지 않는다면 이 섹션은 Express 서버에 대한 선택 사항입니다.
- routes – 앱의 적합한 부분으로 트래픽을 유도하는 데 매우 중요합니다. `"kind": "Compute"` 경로에서는 트래픽이 서버 로직으로 유도됩니다.
- computeResources – 이 섹션을 사용하여 Express 서버의 런타임과 진입점을 지정합니다.

다음으로, 빌드된 애플리케이션 아티팩트를 `.amplify-hosting` 배포 번들로 이동하는 빌드 후 스크립트를 설정합니다. 디렉터리 구조는 Amplify Hosting 배포 사양에 부합합니다.

빌드 후 스크립트 설정

1. 프로젝트 루트에 `bin`라는 디렉터리를 만듭니다.
2. `bin` 디렉터리에 `postbuild.sh`라는 파일을 만듭니다. 다음 내용을 `postbuild.sh` 파일에 추가합니다.

```
#!/bin/bash

rm -rf ./.amplify-hosting
```

```
mkdir -p ./.amplify-hosting/compute

cp -r ./dist ./.amplify-hosting/compute/default
cp -r ./node_modules ./.amplify-hosting/compute/default/node_modules

cp -r public ./.amplify-hosting/static

cp deploy-manifest.json ./.amplify-hosting/deploy-manifest.json
```

3. `package.json` 파일에 `postbuild` 스크립트를 추가합니다. 파일이 다음과 같아야 합니다.

```
"scripts": {
  "start": "ts-node src/index.ts",
  "build": "tsc",
  "serve": "node dist/index.js",
  "postbuild": "chmod +x bin/postbuild.sh && ./bin/postbuild.sh"
}
```

4. 다음 명령을 실행하여 애플리케이션을 빌드합니다.

```
npm run build
```

5. (선택 사항) Express의 경로를 조정합니다. Express 서버에 알맞게 배포 매니페스트의 경로를 수정할 수 있습니다. 예를 들어 `public` 디렉터리에 정적 자산이 없으면 Compute로 유도되는 catch-all 라우팅(`"path": "/*"`)만 필요할 수 있습니다. 이는 서버의 설정에 따라 다릅니다.

최종 디렉터리 구조는 다음과 같아야 합니다.

```
express-app/
### .amplify-hosting/
#   ### compute/
#   #   ### default/
#   #       ### node_modules/
#   #       ### index.js
#   ### static/
#   #   ### hello.txt
#   ### deploy-manifest.json
### bin/
#   ### .amplify-hosting/
#   #   ### compute/
#   #   #   ### default/
```

```
#   #   ### static/
#   ### postbuild.sh*
### dist/
#   ### index.js
### node_modules/
### public/
#   ### hello.txt
### src/
#   ### index.ts
### deploy-manifest.json
### package.json
### package-lock.json
### tsconfig.json
```

서버 배포

1. 코드를 Git 리포지토리로 푸시한 다음에 앱을 Amplify Hosting에 배포합니다.
2. 다음과 같이 `baseDirectory`에서 `.amplify-hosting`을 가리키도록 빌드 설정을 업데이트합니다. 빌드 중에 Amplify에서는 `.amplify-hosting` 디렉터리의 매니페스트 파일을 감지하고 Express 서버를 구성된 대로 배포합니다.

```
version: 1
frontend:
  phases:
    preBuild:
      commands:
        - nvm use 18
        - npm install
    build:
      commands:
        - npm run build
  artifacts:
    baseDirectory: .amplify-hosting
    files:
      - '**/*'
```

3. 배포가 성공했고 서버가 올바르게 실행되는지 확인하려면 Amplify Hosting에서 제공되는 기본 URL에서 앱을 방문합니다.

SSR 앱을 위한 이미지 최적화

Amplify Hosting에는 모든 SSR 앱을 지원하도록 기본적으로 제공되는 이미지 최적화 기능이 있습니다. Amplify의 이미지 최적화를 통해 가능한 한 가장 작은 파일 크기를 유지하면서 해당 이미지에 액세스하는 디바이스에 적합한 형식, 크기 및 해상도로 고품질 이미지를 전달할 수 있습니다.

현재 Next.js Image 구성 요소를 사용하여 온디맨드 방식으로 이미지를 최적화하거나 사용자 지정 이미지 로더를 구현할 수 있습니다. Next.js 13 이상을 사용한다면 Amplify의 이미지 최적화 기능을 사용하기 위해 별도의 조치를 취하지 않아도 됩니다. 사용자 지정 로더를 구현하려면 사용자 지정 이미지 로더 사용 섹션을 참조하세요.

사용자 지정 이미지 로더 사용

사용자 지정 이미지 로더를 사용하면 Amplify에서는 애플리케이션의 `next.config.js` 파일에서 로더를 감지하며 기본으로 제공되는 이미지 최적화 기능을 활용하지 않습니다. Next.js에서 지원하는 사용자 지정 로더에 대한 자세한 내용은 Next.js 이미지 설명서를 참조하세요.

프레임워크 작성자를 위한 이미지 최적화 통합

프레임워크 작성자는 Amplify Hosting 배포 사양을 참조하여 Amplify의 이미지 최적화 기능을 통합할 수 있습니다. 이미지 최적화를 활성화하려면 배포 매니페스트에 이미지 최적화 서비스를 대상으로 지정하는 라우팅 규칙이 포함되어야 합니다. 다음 예시에서는 라우팅 규칙을 구성하는 방법을 보여줍니다.

```
// .amplify-hosting/deploy-manifest.json

{
  "routes": [
    {
      "path": "/images/*",
      "target": {
        "kind": "ImageOptimization",
        "cacheControl": "public, max-age=31536000, immutable"
      }
    }
  ]
}
```

배포 사양을 참조하여 이미지 최적화 설정을 구성하는 방법에 대한 자세한 내용은 Amplify Hosting 배포 사양 섹션을 참조하세요.

이미지 최적화 API 이해

라우팅 규칙에 따라 정의된 경로에서 Amplify 앱의 도메인 URL을 통해 런타임에 이미지 최적화를 간접적으로 호출할 수 있습니다.

```
GET https://{appDomainName}/{path}?{queryParams}
```

이미지 최적화에서는 이미지에 다음과 같은 규칙이 적용됩니다.

- Amplify는 GIF, APNG 및 SVG 형식을 최적화하거나 다른 형식으로 변환할 수 없습니다.
- `dangerouslyAllowSVG` 설정을 활성화하지 않으면 SVG 이미지가 제공되지 않습니다.
- 소스 이미지의 너비 또는 높이는 11MB 또는 9,000픽셀을 초과할 수 없습니다.
- 최적화된 이미지의 크기 제한은 4MB입니다.
- HTTP 또는 HTTPS가 원격 URL로 이미지를 소싱하는 데 지원되는 유일한 프로토콜입니다.

HTTP 헤더

Accept 요청 HTTP 헤더는 클라이언트(일반적으로 웹 브라우저)에서 허용되는 이미지 형식(MIME 유형으로 표시됨)을 지정하는 데 사용합니다. 이미지 최적화 서비스에서는 이미지를 지정된 형식으로 변환하려고 시도합니다. 이 헤더에 지정된 값은 형식 쿼리 파라미터보다 우선순위가 높습니다. 예를 들면 Accept 헤더의 유효한 값은 `image/png, image/webp, */*` 입니다. Amplify 배포 매니페스트에 지정된 형식 설정을 통해 목록에 있는 형식으로 제한됩니다. Accept 헤더가 특정 형식을 요청하더라도 해당 형식이 허용 목록에 없으면 요청이 무시됩니다.

URI 요청 파라미터

다음 테이블에서는 이미지 최적화의 URI 요청 파라미터를 설명합니다.

쿼리 파라미터	유형	필수	설명	예
url	String	예	소스 이미지에 대한 상대 경로 또는 절대 URL입니다. 원격 URL의 경우 http 및 https 프로토콜이 지원됩니다. 값은	`?url=https%3A%2F%2Fwww.example.com%2Fbuffalo.png`

쿼리 파라미터	유형	필수	설명	예
			URL로 인코딩해야 합니다.	
width	숫자	예	최적화된 이미지의 너비입니다(픽셀).	`?width=800`
height	숫자	아니요	최적화된 이미지의 높이입니다(픽셀). 지정하지 않으면 이미지가 너비에 일치하도록 자동으로 규모가 조정됩니다.	`?height=600`
fit	열거형 값: `cover`, `contain`, `fill`, `inside`, `outside`	아니요	지정된 너비와 높이에 알맞게 이미지 크기가 조정되는 방식입니다.	`?width=800&height=600&fit=cover`
position	열거형 값: `center`, `top`, `right`, `bottom`, `left`	아니요	배치가 `cover` 또는 `contain`일 때 사용되는 위치입니다.	`?fit=contain&position=centre`
trim	숫자	아니요	왼쪽 위 픽셀의 지정된 배경색과 비슷한 값이 있는 모든 가장자리에서 픽셀을 잘라냅니다.	`?trim=50`

쿼리 파라미터	유형	필수	설명	예
확장	객체	아니요	가장 가까운 가장자리 픽셀에서 나온 색상을 사용하여 이미지 가장자리에 픽셀을 추가합니다. 형식은 `{top}_{right}_{bottom}_{left}` 이며 여기서 각 값은 추가할 픽셀의 수입니다.	`?extend=10_0_5_0`
extract	객체	아니요	위쪽, 왼쪽, 너비 및 높이로 구분된 지정된 직사각형으로 이미지를 자릅니다. 형식은 {left}_{top}_{width}_{right}이며 여기서 각 값은 잘라낼 픽셀의 수입니다.	`?extract=10_0_5_0`
형식	String	아니요	최적화된 이미지에 바람직한 출력 형식입니다.	`?format=webp`
quality	숫자	아니요	이미지 품질입니다(1~100). 이미지 형식을 변환할 때만 사용합니다.	`?quality=50`

쿼리 파라미터	유형	필수	설명	예
rotate	숫자	아니요	지정된 각도(도)만큼 이미지를 회전합니다.	`?rotate=45`
flip	불린(Boolean)	아니요	이미지를 x축에서 세로(위-아래)로 미러링합니다. 회전이 있는 경우 항상 회전 전에 발생합니다.	`?flip`
flop	불린(Boolean)	아니요	이미지를 y축에서 가로(왼쪽-오른쪽)로 미러링합니다. 회전이 있는 경우 항상 회전 전에 발생합니다.	`?flop`
sharpen	숫자	아니요	선명하게 하면 이미지 가장자리의 선명도가 향상됩니다. 유효한 값은 0.000001~10입니다.	`?sharpen=1`
median	숫자	아니요	중앙값 필터를 적용합니다. 그러면 노이즈가 제거되거나 이미지 가장자리가 부드러워집니다.	`?sharpen=3`

쿼리 파라미터	유형	필수	설명	예
blur	숫자	아니요	지정된 시그마의 가우스 블러를 적용합니다. 유효한 값은 0.3~1,000입니다.	`?blur=20`
gamma	숫자	아니요	크기가 조정된 이미지에서 인식되는 밝기를 개선하려면 감마 보정을 적용합니다. 값은 1.0~3.0이어야 합니다.	`?gamma=1`
negate	불린(Boolean)	아니요	이미지의 색상을 반전합니다.	`?negate`
normalize	불린(Boolean)	아니요	전체 동적 범위를 포괄하도록 휘도를 늘려 이미지 대비를 개선합니다.	`?normalize`
threshold	숫자	아니요	지정된 임곗값보다 강도가 낮으면 이미지의 모든 픽셀을 검은색 픽셀로 대체합니다. 또는 임곗값보다 높으면 흰색 픽셀로 대체합니다. 유효한 값은 0~255입니다.	`?threshold=155`

쿼리 파라미터	유형	필수	설명	예
tint	String	아니요	이미지 휘도를 유지하면서 제공된 RGB를 사용하여 이미지에 색조를 추가합니다.	`?tint=#7743CE`
grayscale	불린(Boolean)	아니요	이미지를 회색조(흑백)로 전환합니다.	`?grayscale`

응답 상태 코드

다음 목록에서는 이미지 최적화의 응답 상태 코드를 설명합니다.

Success - HTTP 상태 코드 200

요청이 이행되었습니다.

BadRequest - HTTP 상태 코드 400

- 입력 쿼리 파라미터가 잘못 지정되었습니다.
- 원격 URL이 `remotePatterns` 설정에 허용된 대로 나열되어 있지 않습니다.
- 원격 URL이 이미지로 확인되지 않습니다.
- 요청된 너비 또는 높이가 `sizes` 설정에 허용된 대로 나열되어 있지 않습니다.
- 요청된 이미지가 SVG인데 `dangerouslyAllowSvg` 설정이 비활성화되어 있습니다.

Not Found - HTTP 상태 코드 404

소스 이미지를 찾을 수 없습니다.

Content too large - HTTP 상태 코드 413

소스 이미지 또는 최적화된 이미지가 허용된 최대 크기(바이트)를 초과합니다.

캐싱

Amplify Hosting에서는 동일한 쿼리 파라미터를 통해 동일한 이미지에 대한 후속 요청이 캐시에서 제공되도록 CDN에 최적화된 이미지를 캐시합니다. 캐시 TTL(Time To Live)은 `Cache-Control` 헤더에 따라 제어됩니다. 다음 목록에서는 `Cache-Control` 헤더 지정 옵션을 설명합니다.

- 이미지 최적화를 대상으로 지정하는 라우팅 규칙 내에서 `Cache-Control` 키를 사용합니다.
- Amplify 앱에 정의된 사용자 지정 헤더를 사용합니다.
- 원격 이미지의 경우 원격 이미지에서 반환된 `Cache-Control` 헤더가 적용됩니다.

이미지 최적화 설정에 지정된 `minimumCacheTTL`에서는 cache-control max-age 지시문의 하한을 정의합니다. 예를 들어 원격 이미지 URL에서는 `cache-control s-max-age=10`으로 응답하는데 `minimumCacheTTL` 값이 60이면 60이 사용됩니다.

Next.js 앱에 대한 Node.js 버전 지원

Amplify에서는 Next.js 컴퓨팅 앱을 빌드하고 배포할 때 앱 빌드에 사용된 Node.js의 메이저 버전과 일치하는 Node.js 런타임 버전을 사용합니다.

Amplify 콘솔의 라이브 패키지 재정의 기능에서 사용할 Node.js 버전을 지정할 수 있습니다. 라이브 패키지 업데이트 구성에 대한 자세한 내용은 라이브 패키지 업데이트 섹션을 참조하세요. nvm 명령과 같은 다른 메커니즘을 사용하여 Node.js 버전을 지정할 수도 있습니다. 버전을 지정하지 않으면 Amplify에서는 Amplify 빌드 컨테이너에서 사용되는 현재 버전을 기본적으로 사용합니다.

SSR 배포 문제 해결

Amplify Hosting 컴퓨팅을 사용하여 SSR 앱을 배포할 때 예상치 못한 문제가 발생하는 경우, 다음 문제 해결 항목을 검토하십시오. 여기에서 문제의 해결 방법을 찾을 수 없는 경우 Amplify GitHub Hosting Issue 리포지토리의 SSR 웹 컴퓨팅 문제 해결 가이드를 참조하십시오.

주제

- 프레임워크 어댑터 사용 중
- 엣지 API 라우팅으로 인해 Next.js 빌드가 실패함
- 앱에 온디맨드 증분 정적 재생성이 작동하지 않음
- 앱의 빌드 출력이 최대 허용 크기를 초과했습니다.
- 메모리 부족 오류로 인해 빌드가 실패함

- HTTP 응답 크기가 너무 큼

프레임워크 어댑터 사용 중

프레임워크 어댑터를 사용하는 SSR 앱 배포에서 문제가 발생하면 SSR 프레임워크를 위한 Amplify 지원 섹션을 참조하세요.

엣지 API 라우팅으로 인해 Next.js 빌드가 실패함

현재 Amplify는 Next.js Edge API 라우팅을 지원하지 않습니다. Amplify로 앱을 호스팅할 때는 비엣지 API와 미들웨어를 사용해야 합니다.

앱에 온디맨드 증분 정적 재생성이 작동하지 않음

Next.js 버전 12.2.0부터 ISR(증분 정적 재생성)을 지원하여 특정 페이지의 Next.js 캐시를 수동으로 제거합니다. 그러나 Amplify는 현재 온디맨드 ISR을 지원하지 않습니다. 앱이 Next.js 온디맨드 재검증을 사용하는 경우, 앱을 Amplify에 배포하면 이 기능이 작동하지 않습니다.

앱의 빌드 출력이 최대 허용 크기를 초과했습니다.

현재 Amplify가 SSR 앱에 지원하는 최대 빌드 출력 크기는 220MB입니다. 앱의 빌드 출력 크기가 최대 허용 크기를 초과한다는 오류 메시지가 표시되면 크기를 줄이기 위한 조치를 취해야 합니다.

앱의 빌드 출력 크기를 줄이려면 앱의 빌드 아티팩트를 검사하고 업데이트하거나 제거할 대규모 종속성을 식별할 수 있습니다. 먼저 빌드 아티팩트를 로컬 컴퓨터에 다운로드합니다. 그런 다음 디렉터리 크기를 확인하세요. 예를 들어, `node_modules` 디렉터리에는 Next.js 서버 런타임 파일에서 `@esbuild` 참조하는 `@swc` 및 와 같은 바이너리가 포함될 수 있습니다. 이러한 바이너리는 런타임에 필요하지 않으므로 빌드 후에 삭제할 수 있습니다.

다음 안내에 따라 AWS Command Line Interface (CLI) 를 사용하여 앱의 빌드 출력을 다운로드하고 디렉터리 크기를 검사하세요.

Next.js 앱의 빌드 출력을 다운로드하고 검사하려면

1. 터미널 창을 열고 다음 명령을 실행합니다. 앱 ID, 브랜치 이름, 작업 ID를 사용자 고유의 정보로 변경합니다. 작업 ID에는 조사 중인 실패한 빌드의 빌드 번호를 사용하세요.

```
aws amplify get-job --app-id abcd1234 --branch-name main --job-id 2
```

2. 터미널 출력의,, 섹션에서 사전 서명된 아티팩트 URL을 찾으십시오. `job steps stepName: "BUILD"` 다음 예제 출력에서는 URL이 빨간색으로 강조 표시됩니다.

```
"job": {
    "summary": {
        "jobArn": "arn:aws:amplify:us-west-2:111122223333:apps/abcd1234/main/
jobs/0000000002",
        "jobId": "2",
        "commitId": "HEAD",
        "commitTime": "2024-02-08T21:54:42.398000+00:00",
        "startTime": "2024-02-08T21:54:42.674000+00:00",
        "status": "SUCCEED",
        "endTime": "2024-02-08T22:03:58.071000+00:00"
    },
    "steps": [
        {
            "stepName": "BUILD",
            "startTime": "2024-02-08T21:54:42.693000+00:00",
            "status": "SUCCEED",
            "endTime": "2024-02-08T22:03:30.897000+00:00",
            "logUrl": "https://aws-amplify-prod-us-west-2-artifacts.s3.us-
west-2.amazonaws.com/abcd1234/main/0000000002/BUILD/log.txt?X-Amz-Security-
Token=IQoJb3JpZ2luX2V...Example
```

3. URL을 복사하여 브라우저 창에 붙여넣습니다. `artifacts.zip`파일이 로컬 컴퓨터에 다운로드 됩니다. 이것은 빌드 출력입니다.
4. du디스크 사용량 명령어를 실행하여 디렉터리 크기를 검사합니다. 다음 예제 명령은 `compute` 및 `static` 디렉터리의 크기를 반환합니다.

```
du -csh compute static
```

다음은 `compute` 및 `static` 디렉터리의 크기 정보가 포함된 출력의 예입니다.

```
 29M    compute
3.8M    static
 33M    total
```

5. `compute`디렉터리를 열고 `node_modules` 폴더를 찾습니다. 폴더 크기를 줄이기 위해 업데이트하거나 제거할 수 있는 파일이 있는지 종속성을 검토하십시오.
6. 런타임에 필요하지 않은 바이너리가 앱에 포함되어 있는 경우 앱 파일의 빌드 섹션에 다음 명령을 추가하여 빌드 후에 바이너리를 삭제하세요. `amplify.yml`

```
- rm -f node_modules/@swc/core-linux-x64-gnu/swc.linux-x64-gnu.node
- rm -f node_modules/@swc/core-linux-x64-musl/swc.linux-x64-musl.node
```

다음은 프로덕션 빌드를 실행한 후 이러한 명령이 추가된 `amplify.yml` 파일의 빌드 명령 섹션 예제입니다.

```
frontend:
  phases:
    build:
      commands:
         -npm run build

         // After running a production build, delete the files
         - rm -f node_modules/@swc/core-linux-x64-gnu/swc.linux-x64-gnu.node
         - rm -f node_modules/@swc/core-linux-x64-musl/swc.linux-x64-musl.node
```

메모리 부족 오류로 인해 빌드가 실패함

Next.js를 통해 빌드 아티팩트를 캐시하여 후속 빌드의 성능을 개선할 수 있습니다. 또한 Amplify의 AWS CodeBuild 컨테이너는 사용자를 대신하여 이 캐시를 압축하여 Amazon S3에 업로드하여 후속 빌드 성능을 개선합니다. 이로 인해 메모리 부족 오류가 발생하면 빌드가 실패할 수 있습니다.

빌드 단계에서 앱이 메모리 제한을 초과하지 않도록 하려면 다음 작업을 수행합니다. 먼저 빌드 설정의 cache.paths 섹션에서 `.next/cache/**/*`를 삭제합니다. 그런 다음, 빌드 설정 파일에서 `NODE_OPTIONS` 환경 변수를 제거합니다. 대신 Amplify 콘솔에서 `NODE_OPTIONS` 환경 변수를 설정하여 노드 최대 메모리 제한을 정의합니다. Amplify 콘솔을 사용하여 환경 변수를 설정하는 방법에 대한 자세한 내용은 환경 변수 설정을 참조하십시오.

이러한 변경을 수행한 후 빌드를 다시 시도합니다. 빌드가 성공하면 빌드 설정 파일의 cache.paths 섹션에 `.next/cache/**/*`를 다시 추가합니다.

빌드 성능 개선을 위한 Next.js 캐시 구성에 대한 자세한 내용은 Next.js 웹 CodeBuild 사이트의 AWS를 참조하십시오.

HTTP 응답 크기가 너무 큼

현재 Amplify가 웹 컴퓨트 플랫폼을 사용하는 Next.js 12 이상 앱에 지원하는 최대 응답 크기는 5.72MB입니다. 이 한도를 초과하는 응답은 콘텐츠가 없는 504 오류를 클라이언트에 반환합니다.

Next.js 지원을 Amplify

Amplify는 Next.js 를 사용하여 만든 서버 측 렌더링 (SSR) 웹 앱의 배포 및 호스팅을 지원합니다. Next.js 는 풀스택 웹 애플리케이션을 빌드하기 위한 React 프레임워크입니다. 이미지 최적화 및 미들웨어와 같은 기능을 갖춘 Next.js 14로 빌드된 앱을 배포할 수 있습니다.

개발자는 Next.js를 사용하여 정적 사이트 생성(SSG)과 SSR을 단일 프로젝트에 결합할 수 있습니다. SSG 페이지는 빌드 시 프리렌더링되며, SSR 페이지는 요청 시 프리렌더링됩니다.

프리렌더링은 성능과 검색 엔진 최적화를 개선할 수 있습니다. Next.js는 서버의 모든 페이지를 프리렌더링하므로 각 페이지의 HTML 콘텐츠가 클라이언트의 브라우저에 도달되는 즉시 이용할 수 있습니다. 이러한 콘텐츠는 또한 더 빨리 로드될 수 있습니다. 로드 시간이 빨라지면 최종 사용자의 웹사이트 이용 경험이 향상되고 사이트의 SEO 순위에 긍정적인 영향을 미칩니다. 또한 프리렌더링은 검색 엔진 봇이 웹사이트의 HTML 콘텐츠를 쉽게 찾고 크롤링할 수 있도록 하여 SEO를 개선합니다.

Next.js는 첫 번째 바이트까지의 시간(TTFB)과 첫 번째 콘텐츠를 렌더링하는 데 걸리는 시간(FCP)과 같은 다양한 성능 메트릭을 측정하기 위한 내장된 분석 지원을 제공합니다. Next.js에 관한 자세한 내용은 Next.js 웹사이트의 시작하기를 참조하십시오.

Next.js 기능 지원

Amplify Hosting 컴퓨트는 Next.js 버전 12, 13, 14로 빌드된 앱의 서버 사이드 렌더링 (SSR) 을 완벽하게 관리합니다. Amplify Hosting 컴퓨팅이 출시되기 전에 Amplify에 Next.js 앱을 배포한 경우, 앱은 Amplify의 이전 SSR 공급자인 Classic(Next.js 11만 해당)을 사용합니다. Amplify Hosting 컴퓨팅은 Next.js 11 또는 그 이전 버전을 사용하여 만든 앱을 지원하지 않습니다. Next.js 11 앱을 Amplify Hosting 컴퓨팅 관리형 SSR 공급자로 마이그레이션하는 것이 좋습니다.

다음 목록은 Amplify Hosting 컴퓨팅 SSR 공급자가 지원하는 특정 기능을 설명합니다.

지원되는 기능

- 서버 측 렌더링 페이지(SSR)
- 정적 페이지
- API 라우팅
- 동적 라우팅
- 모든 라우팅 포착
- SSG(정적 생성)
- 증분 정적 재생성(ISR)

- 다국어(i18n) 하위 경로 라우팅
- 다국어(i18n) 도메인 라우팅
- 미들웨어
- 환경 변수
- 이미지 최적화
- Next.js 13 앱 디렉터리

지원되지 않는 기능

- 엣지 API 경로(엣지 미들웨어 미지원)
- 온디맨드 증분 정적 재생성(ISR)
- 다국어(i18n) 자동 로케일 감지
- Next.js 스트리밍
- 정적 자산 및 최적화된 이미지에서 미들웨어 실행

Next.js 이미지

이미지의 최대 출력 크기는 4.3MB를 초과할 수 없습니다. 더 큰 이미지 파일은 다른 곳에 저장해 두고 Next.js Image 구성 요소를 사용하여 Webp 또는 AVIF 형식으로 크기를 조정하고 최적화한 다음, 더 작은 크기로 제공할 수 있습니다.

참고로, Next.js 설명서에서는 프로덕션 환경에서 이미지 최적화가 올바르게 작동할 수 있도록 Sharp 이미지 처리 모듈을 설치할 것을 권장합니다. 그러나 Amplify 배포에는 필요하지 않습니다. Amplify는 Sharp를 자동으로 배포합니다.

Next.js 앱 요금

Next.js 12 또는 그 이후 버전의 SSR 앱 배포 시, Amplify Hosting 컴퓨팅은 SSR 앱을 배포하는 데 필요한 리소스를 관리합니다. Amplify Hosting 컴퓨팅 요금에 대한 자세한 내용은 AWS Amplify 요금을 참조하십시오.

Amplify를 사용한 Next.js 앱 배포하기

기본적으로 Amplify는 Next.js 12, 13, 14를 지원하는 Amplify 호스팅의 컴퓨팅 서비스를 사용하여 새 SSR 앱을 배포합니다. Amplify Hosting 컴퓨팅에서는 SSR 앱을 배포하는 데 필요한 리소스를 완벽하

게 관리합니다. 2022년 11월 17일 이전에 배포한 Amplify 계정의 SSR 앱은 Classic(Next.js 11만 해당) SSR 공급자를 사용합니다.

Classic(Next.js 11만 해당) SSR을 사용하는 앱을 Amplify Hosting 컴퓨팅 SSR 공급자로 마이그레이션하는 것이 좋습니다. Amplify는 자동 마이그레이션을 수행하지 않습니다. 앱을 수동으로 마이그레이션한 다음 새 빌드를 시작하여 업데이트를 완료해야 합니다. 지침은 Next.js 11 앱을 Amplify 호스팅 컴퓨트로 마이그레이션하기 섹션을 참조하십시오.

다음 지침에 따라 새 Next.js 앱을 배포하십시오.

Amplify 호스팅 컴퓨팅 SSR 공급자를 사용하여 Amplify에 Next.js 앱을 배포하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 모든 앱 페이지에서 새 앱 생성을 선택합니다.
3. Amplify로 빌드 시작 페이지에서 Git 리포지토리 공급자를 선택한 후 다음을 선택합니다.
4. 리포지토리 브랜치 추가 페이지에서 다음을 수행합니다.
   a. 연결할 리포지토리의 이름을 선택합니다.
   b. 연결할 리포지토리 브랜치의 이름을 선택합니다.
   c. 다음을 선택합니다.
5. 앱은 Amplify가 사용자를 대신하여 다른 서비스를 호출할 때 맡는 IAM 서비스 역할을 필요로 합니다. Amplify Hosting 컴퓨팅이 자동으로 서비스 역할을 생성하도록 허용하거나 사용자가 생성한 역할을 지정할 수 있습니다.
   - Amplify가 자동으로 역할을 생성하여 앱에 연결하도록 허용하려면:
     - 새 서비스 역할 생성 및 사용을 선택합니다.
   - 이전에 만든 서비스 역할을 연결하려면:
     a. 기존 서비스 역할 사용을 선택합니다.
     b. 목록에서 사용할 역할을 선택합니다.
6. 다음을 선택합니다.
7. 검토 페이지에서 저장 및 배포를 선택합니다.

Package.json 파일 설정

Next.js 앱 배포 시 Amplify는 `package.json` 파일에 있는 앱의 빌드 스크립트를 검사하여 앱이 SSR 또는 SSG 중에 무엇인지 감지합니다.

다음은 Next.js SSR 앱의 빌드 스크립트 예입니다. 빌드 스크립트 "next build"는 앱이 SSG 페이지와 SSR 페이지를 모두 지원함을 나타냅니다.

```
"scripts": {
  "dev": "next dev",
  "build": "next build",
  "start": "next start"
},
```

다음은 Next.js SSG 앱의 빌드 스크립트의 예입니다. 빌드 스크립트 "next build && next export"는 앱이 SSG 페이지만 지원함을 나타냅니다.

```
"scripts": {
  "dev": "next dev",
  "build": "next build && next export",
  "start": "next start"
},
```

Amplify 빌드 설정

앱의 package.json 파일을 검사하여 배포하는 앱이 SSR 또는 SSG 중에 무엇인지 판단한 후, Amplify는 앱의 빌드 설정을 확인합니다. Amplify 콘솔이나 리포지토리 루트의 amplify.yml 파일에 빌드 설정을 저장할 수 있습니다. 자세한 내용은 빌드 설정 구성 섹션을 참조하십시오.

Next.js SSR 앱을 배포하고 있는 것을 감지했으나 amplify.yml 파일이 없는 경우, Amplify는 앱에 대한 buildspec을 생성하고 baseDirectory을(를) .next(으)로 설정합니다. amplify.yml 파일이 있는 곳에 앱을 배포하는 경우, 파일의 빌드 설정이 콘솔의 모든 빌드 설정을 재정의합니다. 따라서 파일에서 baseDirectory를 .next으로 수동 설정해야 합니다.

다음은 baseDirectory가 .next으로 설정된 앱의 빌드 설정 예시입니다. 이는 빌드 아티팩트가 SSG 및 SSR 페이지를 지원하는 Next.js 앱용임을 나타냅니다.

```
version: 1
frontend:
  phases:
    preBuild:
      commands:
        - npm ci
    build:
      commands:
        - npm run build
```

```
  artifacts:
    baseDirectory: .next
    files:
      - '**/*'
  cache:
    paths:
      - node_modules/**/*
```

SSG 앱을 배포하고 있는 것을 Amplify가 감지하면 앱에 대한 buildspec을 생성하고 `baseDirectory`를 `out`으로 설정합니다. `amplify.yml` 파일이 있는 곳에 앱을 배포하는 경우, 파일에서 `baseDirectory`을(를) `out`(으)로 수동으로 설정해야 합니다.

다음은 `baseDirectory`가 `out`으로 설정된 앱의 빌드 설정 예시입니다. 이는 빌드 아티팩트가 SSG 페이지만 지원하는 Next.js 앱용임을 나타냅니다.

```
version: 1
frontend:
  phases:
    preBuild:
      commands:
        - npm ci
    build:
      commands:
        - npm run build
  artifacts:
    baseDirectory: out
    files:
      - '**/*'
  cache:
    paths:
      - node_modules/**/*
```

Next.js 11 앱을 Amplify 호스팅 컴퓨트로 마이그레이션하기

새 Next.js 앱 배포 시 Amplify는 지원되는 가장 최신 버전의 Next.js를 기본으로 사용합니다. 현재 Amplify 호스팅 컴퓨팅 SSR 공급자는 Next.js 버전 14를 지원합니다.

Amplify 콘솔은 Next.js 버전 12, 13, 14를 완벽하게 지원하는 Amplify 호스팅 컴퓨팅 서비스가 출시되기 전에 배포된 앱을 사용자 계정에서 탐지합니다. 이 콘솔은 Amplify의 이전 SSR 공급자인 Classic(Next.js 11만 해당)을 사용하여 배포된 브랜치가 있는 앱을 식별하는 정보 배너를 보여줍니다. Amplify Hosting 컴퓨팅 SSR 공급자로 앱을 마이그레이션하는 것이 좋습니다.

앱과 모든 프로덕션 브랜치를 동시에 수동으로 마이그레이션해야 합니다. 앱에는 클래식 (Next.js 11만 해당) 과 Next.js 12, 13 또는 14개의 브랜치를 모두 포함할 수 없습니다.

다음 지침에 따라 앱을 Amplify Hosting 컴퓨팅 SSR 공급자로 마이그레이션합니다.

앱을 Amplify Hosting 컴퓨팅 SSR 공급자로 마이그레이션하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 마이그레이션하려는 Next.js 앱을 선택합니다.

> **Note**
>
> Amplify 콘솔에서 앱을 마이그레이션하기 전에 먼저 앱의 package.json 파일을 업데이트하여 Next.js 버전 12, 13 또는 14를 사용해야 합니다.

3. 탐색 창에서 앱 설정, 일반을 선택합니다.
4. 앱에 Classic(Next.js 11만 해당) SSR 공급자를 사용하여 배포한 브랜치가 있는 경우, 앱 홈페이지의 콘솔에 배너가 표시됩니다. 배너에서 마이그레이션을 선택합니다.
5. 마이그레이션 확인 창에서 세 개의 명령문을 선택하고 마이그레이션을 선택합니다.
6. Amplify가 앱을 빌드하고 재배포하여 마이그레이션을 완료할 것입니다.

SSR 마이그레이션 되돌리기

Next.js 앱 배포 시 Amplify Hosting은 앱의 설정을 감지하고 앱의 내부 플랫폼 값을 설정합니다. 세 개의 유효한 플랫폼 값이 있습니다. SSG 앱의 플랫폼 값은 `WEB`으로 설정됩니다. Next.js 버전 11을 사용하는 SSR 앱의 플랫폼 값은 `WEB_DYNAMIC`으로 설정됩니다. Next.js 12 또는 그 이후 버전 SSR 앱의 플랫폼 값은 `WEB_COMPUTE`으로 설정됩니다.

이전 섹션의 지침에 따라 앱을 마이그레이션하면 Amplify는 앱의 플랫폼 값을 `WEB_DYNAMIC`에서 `WEB_COMPUTE`으로 변경합니다. Amplify Hosting 컴퓨팅으로 마이그레이션을 완료한 후에는 콘솔에서 마이그레이션을 되돌릴 수 없습니다. 마이그레이션을 되돌리려면 AWS Command Line Interface 을 사용하여 앱의 플랫폼을 `WEB_DYNAMIC`으로 다시 변경해야 합니다. 터미널 창을 열고 다음 명령을 입력하여 사용자의 고유 정보로 앱 ID와 리전을 업데이트합니다.

```
aws amplify update-app --app-id abcd1234 --platform WEB_DYNAMIC --region us-west-2
```

정적 Next.js 앱에 SSR 기능 추가

Amplify를 통해 배포된 기존 정적(SSG) Next.js 앱에 SSR 기능을 추가할 수 있습니다. SSG 앱을 SSR로 변환하는 프로세스를 시작하기 전에 Next.js 버전 12, 13 또는 14를 사용하도록 앱을 업데이트하고 SSR 기능을 추가하십시오. 그런 다음 다음 단계를 수행해야 합니다.

1. 를 AWS Command Line Interface 사용하여 앱의 플랫폼 유형을 변경할 수 있습니다.
2. 앱에 서비스 역할을 추가합니다.
3. 앱의 빌드 설정에서 출력 디렉터리를 업데이트합니다.
4. 앱이 SSR을 사용한다는 것을 나타내도록 앱의 `package.json` 파일을 업데이트합니다.

플랫폼 업데이트

플랫폼 유형에는 세 가지 유효한 값이 있습니다. SSG 앱의 플랫폼 유형은 `WEB`으로 설정됩니다. Next.js 버전 11을 사용하는 SSR 앱의 플랫폼 유형은 `WEB_DYNAMIC`으로 설정됩니다. Amplify Hosting 컴퓨팅에서 관리되는 SSR을 사용하여 Next.js 12 이상에 배포된 앱의 경우 플랫폼 유형이 로 설정됩니다. `WEB_COMPUTE`

앱을 SSG 앱으로 배포한 경우, Amplify는 플랫폼 유형을 `WEB`으로 설정합니다. 를 AWS CLI 사용하여 앱의 플랫폼을 다음으로 변경할 수 있습니다. `WEB_COMPUTE` 터미널 창을 열고 다음 명령을 입력하여 빨간색 텍스트를 사용자의 고유한 앱 ID 및 리전으로 업데이트합니다.

```
aws amplify update-app --app-id abcd1234 --platform WEB_COMPUTE --region us-west-2
```

서비스 역할 추가

서비스 역할은 사용자를 대신하여 다른 서비스를 호출할 때 Amplify가 맡는 AWS Identity and Access Management (IAM) 역할입니다. Amplify를 통해 이미 배포된 SSG 앱에 서비스 역할을 추가하려면 다음 단계를 따릅니다.

서비스 역할을 추가하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. Amplify 계정에 아직 서비스 역할을 생성하지 않은 경우 서비스 역할 추가를 참조하여 이 필수 단계를 완료합니다.
3. 서비스 역할을 추가할 정적 Next.js 앱을 선택합니다.
4. 탐색 창에서 앱 설정, 일반을 선택합니다.

5. 앱 세부 정보 페이지에서 편집을 선택합니다.
6. 서비스 역할에서 기존 서비스 역할의 이름 또는 2단계에서 만든 서비스 역할의 이름을 선택합니다.
7. 저장을 선택합니다.

빌드 설정 업데이트

SSR 기능을 사용하여 앱을 재배포하기 전에 출력 디렉토리가 `.next`으로 설정되도록 앱의 빌드 설정을 업데이트해야 합니다. Amplify 콘솔 또는 리포지토리에 저장된 `amplify.yml` 파일에서 빌드 설정을 편집할 수 있습니다. 자세한 내용은 빌드 설정 구성 섹션을 참조하십시오.

다음은 `baseDirectory`가 `.next`으로 설정된 앱의 빌드 설정 예시입니다.

```
version: 1
frontend:
  phases:
    preBuild:
      commands:
        - npm ci
    build:
      commands:
        - npm run build
  artifacts:
    baseDirectory: .next
    files:
      - '**/*'
  cache:
    paths:
      - node_modules/**/*
```

package.json 파일 업데이트

서비스 역할을 추가하고 빌드 설정을 업데이트한 후 앱의 `package.json` 파일을 업데이트합니다. 다음 예제와 같이 Next.js 앱이 SSG 및 SSR 페이지를 모두 지원한다는 것을 나타내도록 빌드 스크립트를 `"next build"`로 설정합니다.

```
"scripts": {
  "dev": "next dev",
  "build": "next build",
```

```
  "start": "next start"
},
```

Amplify는 리포지토리의 `package.json` 파일 변경을 감지하고 SSR 기능을 사용하여 앱을 재배포합니다.

환경 변수가 서버 측 런타임에 액세스할 수 있도록 만들기

Amplify Hosting은 Amplify 콘솔의 프로젝트 구성에 환경 변수를 설정하여 애플리케이션 빌드에 환경 변수를 추가할 수 있도록 지원합니다. 하지만 Next.js 서버 구성 요소는 기본적으로 이러한 환경 변수에 액세스할 수 없습니다. 이는 애플리케이션이 빌드 단계에서 사용하는 환경 변수에 저장된 모든 암호를 보호하기 위한 것입니다.

특정 환경 변수가 Next.js에 액세스할 수 있도록 하려면 Next.js가 인식하는 환경 파일에 해당 변수를 설정하도록 Amplify 빌드 사양 파일을 수정하면 됩니다. 이를 통해 Amplify는 애플리케이션을 빌드하기 전에 이러한 환경 변수를 로드할 수 있습니다. 다음 빌드 사양 예제는 빌드 명령 섹션에 환경 변수를 추가하는 방법을 보여줍니다.

```
version: 1
frontend:
  phases:
    preBuild:
      commands:
        - npm ci
    build:
      commands:
        - env | grep -e DB_HOST -e DB_USER -e DB_PASS >> .env.production
        - env | grep -e NEXT_PUBLIC_ >> .env.production
        - npm run build
  artifacts:
    baseDirectory: .next
    files:
      - '**/*'
  cache:
    paths:
      - node_modules/**/*
      - .next/cache/**/*
```

이 예제의 빌드 명령 섹션에는 애플리케이션 빌드가 실행되기 전에 `.env.production` 파일에 환경 변수를 쓰는 두 개의 명령이 포함되어 있습니다. Amplify Hosting은 애플리케이션이 트래픽을 수신할 때 애플리케이션이 이러한 변수에 액세스할 수 있도록 합니다.

이전 예제에서 빌드 명령 섹션의 다음 줄은 빌드 환경에서 특정 변수를 가져와 .env.production 파일에 추가하는 방법을 설명합니다.

```
- env | grep -e DB_HOST -e DB_USER -e DB_PASS >> .env.production
```

변수가 빌드 환경에 있는 경우, .env.production 파일에는 다음과 같은 환경 변수가 포함됩니다.

```
DB_HOST=localhost
DB_USER=myuser
DB_PASS=mypassword
```

이전 예제에서 빌드 명령 섹션의 다음 줄은 특정 접두사가 있는 환경 변수를 .env.production 파일에 추가하는 방법을 설명합니다. 이 예제에서는 접두사 NEXT_PUBLIC_이 있는 모든 변수를 추가합니다.

```
- env | grep -e NEXT_PUBLIC_ >> .env.production
```

빌드 환경에 접두사 NEXT_PUBLIC_이 있는 변수가 여러 개 있는 경우 .env.production 파일은 다음과 유사하게 표시됩니다.

```
NEXT_PUBLIC_ANALYTICS_ID=abcdefghijk
NEXT_PUBLIC_GRAPHQL_ENDPOINT=uowelalsmlsadf
NEXT_PUBLIC_SEARCH_KEY=asdfiojslf
NEXT_PUBLIC_SEARCH_ENDPOINT=https://search-url
```

모노리포지토리를 위한 SSR 환경 변수

모노레포에 SSR 앱을 배포하고 특정 환경 변수를 Next.js 에 액세스할 수 있게 하려면 파일 앞에 애플리케이션 루트를 붙여야 합니다. .env.production Nx monorepo 내 Next.js 앱을 위한 다음 예제 빌드 사양은 빌드 명령 섹션에서 환경 변수를 추가하는 방법을 보여줍니다.

```
version: 1
applications:
  - frontend:
      phases:
        preBuild:
          commands:
            - npm ci
        build:
          commands:
```

```
            - env | grep -e DB_HOST -e DB_USER -e DB_PASS >> apps/app/.env.production
            - env | grep -e NEXT_PUBLIC_ >> apps/app/.env.production
            - npx nx build app
      artifacts:
        baseDirectory: dist/apps/app/.next
        files:
          - '**/*'
      cache:
        paths:
          - node_modules/**/*
      buildPath: /
    appRoot: apps/app
```

위 예제의 빌드 명령 섹션의 다음 줄은 빌드 환경에서 특정 변수를 가져와 애플리케이션 루트를 사용하여 모노리포지토리의 앱 `.env.production` 파일에 추가하는 방법을 보여줍니다. `apps/app`

```
- env | grep -e DB_HOST -e DB_USER -e DB_PASS >> apps/app/.env.production
- env | grep -e NEXT_PUBLIC_ >> apps/app/.env.production
```

모노레포 Next.js 앱 배포

Amplify는 일반 모노레포 앱뿐만 아니라 npm 워크스페이스, pnpm 워크스페이스, Yarn 워크스페이스, Nx 및 Turborepo를 사용하여 생성된 모노레포 앱을 지원합니다. 앱 배포 시 Amplify는 사용 중인 모노레포 빌드 프레임워크를 자동으로 감지합니다. Amplify는 npm 워크스페이스, Yarn 워크스페이스 또는 Nx의 앱에 대한 빌드 설정을 자동으로 적용합니다. 참고로 pnpm 및 Turborepo 앱에는 추가 구성이 필요합니다. 자세한 정보는 모노레포 빌드 설정을 참조하세요.

Nx에 대한 자세한 예제는 AWS Amplify Hosting을 통해 Nx를 사용하는 Next.js 앱 간 코드 공유 블로그 게시물을 참조하십시오.

SSR CloudWatch 앱용 아마존 로그

Amplify는 Next.js 런타임에 대한 정보를 사용자의 아마존 CloudWatch 로그에 전송합니다. AWS 계정 SSR 앱을 배포할 때 Amplify가 사용자를 대신하여 다른 서비스를 호출할 때 맡는 IAM 서비스 역할이 앱에 필요합니다. Amplify Hosting 컴퓨팅이 자동으로 서비스 역할을 생성하도록 허용하거나 사용자가 생성한 역할을 지정할 수 있습니다.

Amplify에서 IAM 역할을 생성하도록 허용하면 해당 역할에는 이미 로그를 생성할 권한이 있습니다. CloudWatch IAM 역할을 직접 생성하는 경우 Amplify가 Amazon CloudWatch Logs에 액세스할 수 있도록 하려면 정책에 다음 권한을 추가해야 합니다.

```
logs:CreateLogStream
logs:CreateLogGroup
logs:DescribeLogGroups
logs:PutLogEvents
```

서비스 역할에 대한 자세한 내용은 서비스 역할 추가을 참조하십시오.

Amplify Next.js 11 지원

2022년 11월 17일에 Amplify Hosting 컴퓨팅이 릴리스되기 전에 Amplify에 Next.js 앱을 배포한 경우, 앱은 Amplify의 이전 SSR 공급자인 Classic(Next.js 11만 해당)을 사용합니다. 이 섹션의 설명서는 Classic(Next.js 11만 해당) SSR 공급자를 사용하여 배포한 앱에만 적용됩니다.

> **Note**
>
> Next.js 11 앱을 Amplify Hosting 컴퓨팅 관리형 SSR 공급자로 마이그레이션하는 것이 좋습니다. 자세한 정보는 Next.js 11 앱을 Amplify 호스팅 컴퓨트로 마이그레이션하기을 참조하세요.

다음 목록은 Amplify Classic(Next.js 11만 해당) SSR 공급자가 지원하는 특정 기능을 설명합니다.

지원되는 기능

- 서버 측 렌더링 페이지(SSR)
- 정적 페이지
- API 라우팅
- 동적 라우팅
- 모든 라우팅 포착
- SSG(정적 생성)
- 증분 정적 재생성(ISR)
- 다국어(i18n) 하위 경로 라우팅
- 환경 변수

지원되지 않는 기능

- 이미지 최적화

- 온디맨드 증분 정적 재생성(ISR)
- 다국어(i18n) 도메인 라우팅
- 다국어(i18n) 자동 로케일 감지
- 미들웨어
- 엣지 미들웨어
- 엣지 API 라우팅

Next.js 11 앱 가격

Next.js 11 SSR 앱을 배포할 때 Amplify는 계정에 다음과 같은 추가 백엔드 리소스를 생성합니다. AWS

- 앱의 정적 자산에 대한 리소스를 저장하는 Amazon Simple Storage Service(S3) 버킷. Amazon S3 요금에 대한 자세한 내용은 Amazon S3 요금을 참조하십시오.
- 앱을 제공하기 위한 Amazon CloudFront 배포판입니다. CloudFront 요금에 대한 자세한 내용은 Amazon CloudFront 요금을 참조하십시오.
- 제공하는 콘텐츠를 사용자 지정하는 네 개의 Lambda @Edge 함수 CloudFront

AWS Identity and Access Management Next.js 11 SSR 앱에 대한 권한

Amplify는 SSR 앱을 배포하려면 AWS Identity and Access Management (IAM) 권한이 필요합니다. 필요한 최소 권한이 없으면 SSR 앱 배포를 시도할 때 오류가 발생합니다. Amplify에 필요한 권한을 제공하려면 서비스 역할을 지정해야 합니다.

Amplify가 사용자를 대신하여 다른 서비스를 호출할 때 맡는 IAM 서비스 역할을 생성하려면 서비스 역할 추가 섹션을 참조하십시오. 이 지침은 `AdministratorAccess-Amplify` 관리형 정책을 연결하는 역할을 생성하는 방법을 설명합니다.

`AdministratorAccess-Amplify`관리형 정책은 IAM 작업을 비롯한 여러 AWS 서비스에 대한 액세스를 제공합니다. 정책만큼이나 강력하다고 간주해야 합니다. `AdministratorAccess` 이 정책은 SSR 앱을 배포하는 데 필요한 것보다 더 많은 권한을 제공합니다.

최소 권한을 부여하는 모범 사례를 따르고 서비스 역할에 부여되는 권한을 줄이는 것이 좋습니다. 관리자에게 서비스 역할에 대한 액세스 권한을 부여하는 대신, SSR 앱을 배포하는 데 필요한 권한만 부여하는 자체 고객 관리형 IAM 정책을 만들 수 있습니다. 고객 관리형 정책을 만드는 방법에 대한 지침은 IAM 사용 설명서의 IAM 정책 생성 섹션을 참조하십시오.

자체 정책을 생성하는 경우, SSR 앱을 배포하는 데 필요한 다음의 최소 권한 목록을 참조하십시오.

```
acm:DescribeCertificate
acm:ListCertificates
acm:RequestCertificate
cloudfront:CreateCloudFrontOriginAccessIdentity
cloudfront:CreateDistribution
cloudfront:CreateInvalidation
cloudfront:GetDistribution
cloudfront:GetDistributionConfig
cloudfront:ListCloudFrontOriginAccessIdentities
cloudfront:ListDistributions
cloudfront:ListDistributionsByLambdaFunction
cloudfront:ListDistributionsByWebACLId
cloudfront:ListFieldLevelEncryptionConfigs
cloudfront:ListFieldLevelEncryptionProfiles
cloudfront:ListInvalidations
cloudfront:ListPublicKeys
cloudfront:ListStreamingDistributions
cloudfront:UpdateDistribution
cloudfront:TagResource
cloudfront:UntagResource
cloudfront:ListTagsForResource
cloudfront:DeleteDistribution
iam:AttachRolePolicy
iam:CreateRole
iam:CreateServiceLinkedRole
iam:GetRole
iam:PutRolePolicy
iam:PassRole
iam:UpdateAssumeRolePolicy
iam:DeleteRolePolicy
lambda:CreateFunction
lambda:EnableReplication
lambda:DeleteFunction
lambda:GetFunction
lambda:GetFunctionConfiguration
lambda:PublishVersion
lambda:UpdateFunctionCode
lambda:UpdateFunctionConfiguration
lambda:ListTags
lambda:TagResource
lambda:UntagResource
lambda:ListEventSourceMappings
```

```
lambda:CreateEventSourceMapping
route53:ChangeResourceRecordSets
route53:ListHostedZonesByName
route53:ListResourceRecordSets
s3:CreateBucket
s3:GetAccelerateConfiguration
s3:GetObject
s3:ListBucket
s3:PutAccelerateConfiguration
s3:PutBucketPolicy
s3:PutObject
s3:PutBucketTagging
s3:GetBucketTagging
sqs:CreateQueue
sqs:DeleteQueue
sqs:GetQueueAttributes
sqs:SetQueueAttributes
amplify:GetApp
amplify:GetBranch
amplify:UpdateApp
amplify:UpdateBranch
```

Next.js 11 배포 문제 해결

Amplify로 Classic(Next.js 11만 해당) SSR 앱을 배포할 때 예상치 못한 문제가 발생하는 경우, 다음 문제 해결 항목을 검토하십시오.

주제

- 출력 디렉터리가 재정의됨
- SSR 사이트를 배포한 후 404 오류가 발생함
- 앱에 SSR 배포에 대한 재작성 규칙이 누락되었습니다. CloudFront
- 앱이 너무 커서 배포할 수 없음
- 메모리 부족 오류로 인해 빌드가 실패함
- 앱에 SSR 브랜치와 SSG 브랜치가 모두 있음
- 앱은 예약된 경로가 있는 폴더에 정적 파일을 저장합니다.
- 앱이 CloudFront 한도에 도달했습니다.
- 환경 변수가 Lambda 함수로 전달되지 않음
- Lambda@Edge 함수가 미국 동부(버지니아 북부) 리전에서 생성됨

- Next.js 앱이 지원되지 않는 기능을 사용함
- Next.js 앱의 이미지가 로드되지 않음
- 지원되지 않는 리전

출력 디렉터리가 재정의됨

Amplify로 배포된 Next.js 앱의 출력 디렉토리는 `.next`으로 설정되어야 합니다. 앱의 출력 디렉토리가 재정의되는 경우 `next.config.js` 파일을 확인합니다. 빌드 출력 디렉터리의 기본값을 `.next`으로 설정하려면 파일에서 다음 줄을 삭제합니다.

```
distDir: 'build'
```

빌드 설정에서 출력 디렉터리가 `.next`으로 설정되어 있는지 확인합니다. 앱의 빌드 설정을 보는 방법에 대한 자세한 내용은 빌드 설정 구성 섹션을 참조하십시오.

다음은 `baseDirectory`가 `.next`으로 설정된 앱의 빌드 설정 예시입니다.

```
version: 1
frontend:
  phases:
    preBuild:
      commands:
        - npm ci
    build:
      commands:
        - npm run build
  artifacts:
    baseDirectory: .next
    files:
      - '**/*'
  cache:
    paths:
      - node_modules/**/*
```

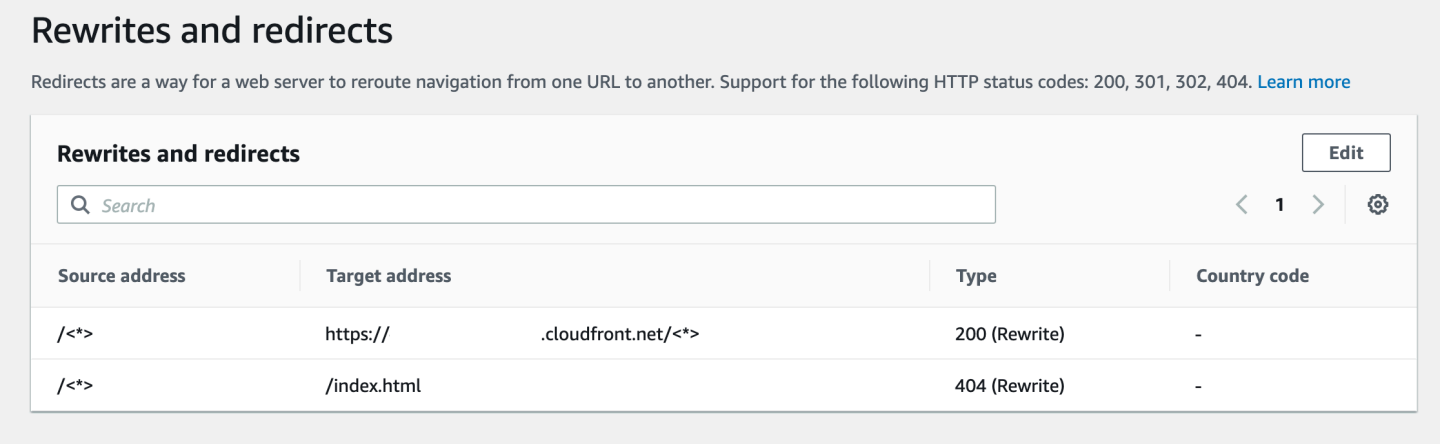
SSR 사이트를 배포한 후 404 오류가 발생함

사이트를 배포한 후 404 오류가 발생하는 경우, 출력 디렉터리가 재정의되어 문제가 발생한 것일 수 있습니다. `next.config.js` 파일을 확인하고 앱 빌드 사양의 빌드 출력 디렉터리가 올바른지 확인하려면 이전 출력 디렉터리가 재정의됨 주제의 단계를 따릅니다.

앱에 SSR 배포에 대한 재작성 규칙이 누락되었습니다. CloudFront

SSR 앱을 배포할 때 Amplify는 SSR 배포를 위한 CloudFront 재작성 규칙을 생성합니다. 웹 브라우저에서 앱에 액세스할 수 없는 경우 Amplify 콘솔에 앱에 대한 CloudFront 재작성 규칙이 있는지 확인하십시오. 규칙이 없는 경우 수동으로 추가하거나 앱을 재배포할 수 있습니다.

Amplify 콘솔에서 앱의 다시 쓰기 및 리디렉션 규칙을 보거나 편집하려면, 탐색 창에서 앱 설정을 선택한 다음 다시 쓰기 및 리디렉션을 선택합니다. 다음 스크린샷은 SSR 앱을 배포할 때 Amplify가 생성하는 다시 쓰기 규칙의 예시를 보여줍니다. 이 예제에는 CloudFront 재작성 규칙이 있다는 것을 알 수 있습니다.



앱이 너무 커서 배포할 수 없음

Amplify는 SSR 배포 크기를 50MB로 제한합니다. Next.js SSR 앱을 Amplify에 배포하려고 할 때 `RequestEntityTooLargeException` 오류가 발생한다면 앱이 너무 커서 배포할 수 없다는 의미입니다. `next.config.js` 파일에 캐시 정리 코드를 추가하여 이 문제를 해결할 수 있습니다.

다음은 캐시 정리를 수행하는 `next.config.js` 파일 내 코드의 예입니다.

```
module.exports = {
    webpack: (config, { buildId, dev, isServer, defaultLoaders, webpack }) => {
        config.optimization.splitChunks.cacheGroups = { }
        config.optimization.minimize = true;
        return config
      },
}
```

메모리 부족 오류로 인해 빌드가 실패함

Next.js를 통해 빌드 아티팩트를 캐시하여 후속 빌드의 성능을 개선할 수 있습니다. 또한 Amplify의 AWS CodeBuild 컨테이너는 사용자를 대신하여 이 캐시를 압축하여 Amazon S3에 업로드하여 후속 빌드 성능을 개선합니다. 이로 인해 메모리 부족 오류가 발생하면 빌드가 실패할 수 있습니다.

빌드 단계에서 앱이 메모리 제한을 초과하지 않도록 하려면 다음 작업을 수행합니다. 먼저 빌드 설정의 cache.paths 섹션에서 `.next/cache/**/*`를 삭제합니다. 그런 다음, 빌드 설정 파일에서 `NODE_OPTIONS` 환경 변수를 제거합니다. 대신 Amplify 콘솔에서 `NODE_OPTIONS` 환경 변수를 설정하여 노드 최대 메모리 제한을 정의합니다. Amplify 콘솔을 사용하여 환경 변수를 설정하는 방법에 대한 자세한 내용은 환경 변수 설정을 참조하십시오.

이러한 변경을 수행한 후 빌드를 다시 시도합니다. 빌드가 성공하면 빌드 설정 파일의 cache.paths 섹션에 `.next/cache/**/*`를 다시 추가합니다.

빌드 성능 개선을 위한 Next.js 캐시 구성에 대한 자세한 내용은 Next.js 웹 CodeBuild 사이트의 AWS를 참조하십시오.

앱에 SSR 브랜치와 SSG 브랜치가 모두 있음

SSR 브랜치와 SSG 브랜치가 모두 있는 앱은 배포할 수 없습니다. SSR 브랜치와 SSG 브랜치를 모두 배포해야 하는 경우, SSR 브랜치만 사용하는 하나의 앱과 SSG 브랜치만 사용하는 다른 앱을 배포해야 합니다.

앱은 예약된 경로가 있는 폴더에 정적 파일을 저장합니다.

Next.js는 프로젝트의 루트 디렉터리에 이름이 `public`으로 지정되어 저장된 폴더의 정적 파일을 제공할 수 있습니다. Amplify를 사용하여 Next.js 앱을 배포하고 호스팅하는 경우 프로젝트에 `public/static` 경로가 있는 폴더를 포함할 수 없습니다. Amplify는 앱을 배포할 때 사용할 `public/static` 경로를 예약합니다. 앱에 이 경로가 포함된 경우, Amplify로 배포하기 전에 `static` 폴더 이름을 변경해야 합니다.

앱이 CloudFront 한도에 도달했습니다.

CloudFront 서비스 할당량은 Lambda @Edge 함수가 연결된 25개의 배포로 AWS 계정을 제한합니다. 이 할당량을 초과하는 경우 계정에서 사용하지 않는 CloudFront 배포를 삭제하거나 할당량 증가를 요청할 수 있습니다. 자세한 내용은 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하십시오.

환경 변수가 Lambda 함수로 전달되지 않음

SSR 앱의 Amplify 콘솔에서 지정하는 환경 변수는 앱 기능에 전달되지 않습니다. AWS Lambda Lambda 함수에서 참조할 수 있는 환경 변수를 추가하는 방법에 대한 자세한 지침은 환경 변수가 서버 측 런타임에 액세스할 수 있도록 만들기 섹션을 참조하십시오.

Lambda@Edge 함수가 미국 동부(버지니아 북부) 리전에서 생성됨

Next.js 앱을 배포하면 Amplify는 Lambda @Edge 함수를 생성하여 제공하는 콘텐츠를 사용자 지정합니다. CloudFront Lambda@Edge 함수는 앱이 배포된 리전이 아닌 미국 동부(버지니아 북부) 리전에서 생성됩니다. 이는 Lambda@Edge의 제한 사항입니다. Lambda @Edge 함수에 대한 자세한 내용은 Amazon CloudFront 개발자 안내서의 에지 함수에 대한 제한을 참조하십시오.

Next.js 앱이 지원되지 않는 기능을 사용함

Amplify로 배포된 앱은 버전 11까지의 Next.js 메이저 버전을 지원합니다. Amplify에서 지원되거나 지원되지 않는 Next.js 기능의 상세 목록은 supported features 섹션을 참조하십시오.

새 Next.js 앱 배포 시 Amplify는 지원되는 가장 최신 버전의 Next.js를 기본적으로 사용합니다. 이전 버전의 Next.js 버전으로 Amplify에 배포한 기존 Next.js 앱이 있는 경우, 이 앱을 Amplify 호스팅 컴퓨팅 SSR 공급자로 마이그레이션할 수 있습니다. 지침은 Next.js 11 앱을 Amplify 호스팅 컴퓨트로 마이그레이션하기 섹션을 참조하십시오.

Next.js 앱의 이미지가 로드되지 않음

`next/image` 구성 요소를 사용하여 Next.js 앱에 이미지를 추가할 때, 이미지 크기는 1MB를 초과할 수 없습니다. Amplify에 앱을 배포할 때 이미지가 1MB보다 큰 경우 503 오류를 반환합니다. 이는 헤더 및 본문을 포함하여 Lambda 함수가 생성하는 응답의 크기를 1MB로 제한하는 Lambda@Edge 제한 때문입니다.

1MB 제한은 PDF, 문서 파일 등 앱의 다른 아티팩트에 적용됩니다.

지원되지 않는 리전

Amplify는 Amplify를 사용할 수 있는 모든 AWS 리전에서 Classic(Next.js 11만 해당) SSR 앱 배포를 지원하지 않습니다. Classic(Next.js 11만 해당) SSR은 유럽(밀라노) eu-south-1, 중동(바레인) me-south-1, 아시아 태평양(홍콩) ap-east-1 리전에서 지원되지 않습니다.

사용자 지정 도메인 설정

Amplify Hosting으로 배포한 앱을 사용자 지정 도메인에 연결할 수 있습니다. Amplify를 사용하여 웹 앱을 배포하는 경우 Amplify는 다음과 같은 URL을 사용하여 기본 `amplifyapp.com` 도메인에서 웹 앱을 호스팅합니다. `https://branch-name.d1m7bkiki6tdw1.amplifyapp.com` 앱을 사용자 지정 도메인에 연결하면 사용자는 앱이 `https://www.example.com`과 같은 사용자 지정 URL에서 호스팅되는 것을 볼 수 있습니다.

Amazon Route 53 또는 같은 공인 도메인 등록 기관을 통해 사용자 지정 도메인을 구입할 수 있습니다. GoDaddy Route 53는 아마존의 DNS (도메인 이름 시스템) 웹 서비스입니다. Route 53의 사용에 대한 자세한 내용은 Amazon Route 53이란을 참조하십시오. 타사 공인 도메인 등록 기관 목록은 ICANN 웹 사이트의 공인 등록 기관 디렉토리를 참조하십시오.

사용자 지정 도메인을 설정할 때 Amplify에서 제공하는 기본 관리 인증서를 사용하거나 자체 사용자 지정 인증서를 사용할 수 있습니다. 도메인에 사용 중인 인증서를 언제든지 변경할 수 있습니다. 인증서 관리에 대한 자세한 내용은 을 참조하십시오SSL/TLS 인증서 사용.

사용자 지정 도메인 설정을 진행하기 전에 다음 사전 요구 사항을 충족했는지 확인하세요.

- 등록된 도메인 이름을 소유하고 있습니다.
- 에서 발급했거나 가져온 인증서가 AWS Certificate Manager있습니다.
- Amplify 호스팅에 앱을 배포했습니다.

  이 단계를 완료하는 방법에 대한 자세한 내용은 을 참조하십시오Amplify Hosting 시작하기.
- 도메인과 DNS 용어에 대한 기본 지식이 있어야 합니다.

  도메인 및 DNS에 대한 자세한 내용은 DNS 용어 및 개념 이해을 참조하십시오.

주제

- DNS 용어 및 개념 이해
- SSL/TLS 인증서 사용
- Amazon Route 53에서 관리되는 사용자 지정 도메인 추가
- 타사 DNS 공급자가 관리하는 사용자 지정 도메인 추가
- 에서 관리하는 도메인의 DNS 레코드 업데이트 GoDaddy
- Google 도메인에서 관리하는 도메인의 DNS 레코드 업데이트

- 도메인의 SSL/TLS 인증서를 업데이트하세요.
- 하위 도메인 관리
- Wildcard 하위 도메인
- Amazon Route 53 사용자 지정 도메인을 위한 자동 하위 도메인을 설정합니다.
- 사용자 지정 도메인 문제 해결

DNS 용어 및 개념 이해

도메인 이름 시스템(DNS)과 관련된 용어 및 개념에 익숙하지 않은 경우, 다음 항목을 참조하여 사용자 지정 도메인을 추가하는 절차를 이해하는 데 도움이 될 수 있습니다.

DNS 용어

다음은 DNS에서 흔히 사용되는 용어 목록입니다. 사용자 지정 도메인을 추가하는 절차를 이해하는 데 도움이 될 수 있습니다.

CNAME

정식 레코드 이름(CNAME)은 웹페이지 세트에 대해 도메인을 숨기고 다른 곳에 위치해 있는 것처럼 표시할 수 있게 해주는 DNS 레코드의 유형입니다. CNAME은 정규화된 도메인 이름(FQDN)에 대한 하위 도메인을 가리킵니다. 예를 들어, 새 CNAME 레코드를 생성하여 하위 도메인 www.example.com(여기서 www는 하위 도메인임)을 Amplify 콘솔에서 앱에 할당된 FQDN 도메인 branch-name.d1m7bkiki6tdw1.cloudfront.net에 매핑할 수 있습니다.

ANAME

ANAME 레코드는 CNAME 레코드와 같지만 루트 수준에 해당합니다. ANAME는 FQDN에 대한 도메인의 루트를 가리킵니다. 해당 FQDN은 IP 주소를 가리킵니다.

이름 서버

이름 서버는 도메인 이름의 다양한 서비스의 위치에 관한 쿼리를 전문적으로 처리하는 인터넷상의 서버입니다. Amazon Route 53에서 도메인을 설정하면 도메인에 이름 서버 목록이 이미 할당되어 있습니다.

NS 레코드

NS 레코드는 도메인 세부 정보를 조회하는 네임 서버를 가리킵니다.

DNS 확인

도메인 이름 시스템(DNS)은 사람이 읽을 수 있는 도메인 이름을 컴퓨터 친화적인 IP 주소로 변환하는 전화번호부와 같습니다. **`https://google.com`**을(를) 브라우저에 입력하면 DNS 공급자에서 웹 사이트를 호스팅하는 서버의 IP 주소를 찾기 위한 조회 작업이 수행됩니다.

DNS 공급자는 도메인 레코드와 해당 IP 주소를 포함합니다. 가장 일반적으로 사용되는 DNS 레코드는 CNAME, ANAME, NS 레코드입니다.

Amplify는 CNAME 레코드를 사용하여 사용자가 자체 사용자 지정 도메인을 소유하고 있는지 확인합니다. Route 53을 사용하여 도메인을 호스팅하는 경우, 자동으로 사용자를 대신하여 확인이 이루어집니다. 그러나 타사 제공업체 (예:) 를 통해 도메인을 호스팅하는 경우 도메인의 DNS 설정을 수동으로 업데이트하고 Amplify에서 제공하는 새 CNAME 레코드를 추가해야 합니다. GoDaddy

Amplify 호스팅 사용자 지정 도메인 활성화 프로세스

Amplify Hosting으로 사용자 지정 도메인을 추가하는 경우, 사용자 지정 도메인을 사용하여 앱을 보려면 먼저 여러 단계를 완료해야 합니다. 다음 목록은 도메인 설정 프로세스의 각 단계를 설명합니다.

SSL/TLS 생성

관리형 인증서를 사용하는 경우 안전한 사용자 지정 도메인을 AWS Amplify 설정하기 위한 SSL/TLS 인증서를 발급합니다.

SSL/TLS 구성 및 확인

Amplify는 관리형 인증서를 발급하기 전에 사용자가 도메인 소유자인지 확인합니다. Amazon Route 53에서 관리하는 도메인의 경우, Amplify에서 DNS 확인 레코드를 자동으로 업데이트합니다. Route 53 외부에서 관리되는 도메인의 경우, Amplify 콘솔에서 제공하는 DNS 확인 레코드를 타사 DNS 공급자를 통해 도메인에 수동으로 추가해야 합니다.

사용자 지정 인증서를 사용하는 경우 도메인 소유권을 검증할 책임은 사용자에게 있습니다.

도메인 활성화

도메인이 성공적으로 확인되었습니다. Route 53 외부에서 관리되는 도메인의 경우, Amplify 콘솔에서 제공하는 CNAME 레코드를 타사 DNS 공급자를 통해 도메인에 수동으로 추가해야 합니다.

SSL/TLS 인증서 사용

SSL/TLS 인증서는 웹 브라우저가 보안 SSL/TLS 프로토콜을 사용하여 웹 사이트에 대한 암호화된 네트워크 연결을 식별하고 설정할 수 있도록 하는 디지털 문서입니다. 사용자 지정 도메인을 설정할 때 Amplify에서 제공하는 기본 관리 인증서를 사용하거나 자체 사용자 지정 인증서를 사용할 수 있습니다.

Amplify는 관리형 인증서를 사용하여 앱에 연결된 모든 도메인에 대해 SSL/TLS 인증서를 발급하므로 HTTPS/2를 통해 모든 트래픽이 보호됩니다. AWS Certificate Manager (ACM) 에서 생성한 기본 인증서는 13개월 동안 유효하며 Amplify에서 앱을 호스팅하는 한 자동으로 갱신됩니다.

> **Warning**
>
> 도메인 공급자의 DNS 설정에서 CNAME 확인 레코드가 수정 또는 삭제된 경우 Amplify는 인증서를 갱신할 수 없습니다. Amplify 콘솔에서 도메인을 삭제하고 다시 추가해야 합니다.

사용자 지정 인증서를 사용하려면 선택한 타사 인증 기관으로부터 인증서를 받아야 합니다. 다음으로 인증서를 로 가져옵니다 AWS Certificate Manager. ACM은 내부 연결 리소스와 함께 AWS 서비스 사용할 공개 및 사설 SSL/TLS 인증서를 쉽게 프로비저닝, 관리 및 배포할 수 있게 해주는 서비스입니다. 미국 동부 (버지니아 북부) (us-east-1) 지역에서 인증서를 요청하거나 가져와야 합니다.

사용자 지정 인증서가 추가하려는 모든 하위 도메인을 포함하는지 확인하세요. 도메인 이름 앞에 와일드카드를 사용하여 여러 하위 도메인을 포함할 수 있습니다. 예를 들어 도메인이 인 경우 와일드카드 도메인을 포함할 수 있습니다. `example.com` `*.example.com` 여기에는 및 와 같은 하위 도메인도 포함됩니다. `product.example.com` `api.example.com`

ACM에서 사용자 지정 인증서를 사용할 수 있게 되면 도메인 설정 과정에서 해당 인증서를 선택할 수 있습니다. 인증서를 가져오는 방법에 대한 지침은 사용 설명서의 인증서 AWS Certificate Manager가져오기를 참조하십시오. AWS Certificate ManagerAWS Certificate Manager

ACM에서 사용자 지정 인증서를 갱신하거나 다시 가져오는 경우 Amplify는 사용자 지정 도메인과 연결된 인증서 데이터를 새로 고칩니다. 가져온 인증서의 경우 ACM은 갱신을 자동으로 관리하지 않습니다. 사용자 지정 인증서를 갱신하고 다시 가져오는 것은 사용자의 책임입니다.

도메인에 사용 중인 인증서를 언제든지 변경할 수 있습니다. 예를 들어 기본 관리형 인증서를 사용자 지정 인증서로 전환하거나 사용자 지정 인증서에서 관리형 인증서로 변경할 수 있습니다. 또한 사용 중인 사용자 지정 인증서를 다른 사용자 지정 인증서로 변경할 수 있습니다. 인증서 업데이트에 대한 지침은 도메인의 SSL/TLS 인증서 업데이트를 참조하십시오.

Amazon Route 53에서 관리되는 사용자 지정 도메인 추가

Route 53에서 관리하는 사용자 지정 도메인을 추가하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 사용자 지정 도메인에 연결할 앱을 선택합니다.
3. 탐색 창에서 호스팅, 사용자 지정 도메인을 선택합니다.
4. 사용자 지정 도메인 페이지에서 도메인 추가를 선택합니다.
5. 루트 도메인의 이름을 입력합니다. 예를 들어, 도메인 이름이 https://example.com인 경우, **`example.com`**을(를) 입력합니다.

   입력을 시작하면 Route 53에서 이미 관리하고 있는 모든 루트 도메인이 목록에 나타납니다. 목록에서 사용하려는 도메인을 선택할 수 있습니다. 아직 도메인을 소유하고 있지 않고 사용 가능한 경우, Amazon Route 53에서 도메인을 구매할 수 있습니다.
6. 도메인 이름을 입력한 후 도메인 구성을 선택합니다.
7. 기본적으로 Amplify는 도메인에 대해 두 개의 하위 도메인 항목을 자동으로 생성합니다. 예를 들어 도메인 이름이 example.com인 경우, 루트 도메인에서 www 하위 도메인으로 리디렉션이 설정된 하위 도메인 https://www.example.com 및 https://example.com이 표시됩니다.

   (선택 사항) 하위 도메인만을 추가하려는 경우, 기본 구성을 수정할 수 있습니다. 하위 도메인 연결을 참조하십시오. 기본 구성을 변경하려면 탐색 창에서 재작성 및 리디렉션을 선택한 다음 도메인을 구성합니다.
8. 사용할 SSL/TLS 인증서를 선택합니다. Amplify에서 제공하는 기본 관리 인증서를 사용하거나 가져온 사용자 지정 타사 인증서를 사용할 수 있습니다. AWS Certificate Manager
   - 기본 Amplify 관리 인증서를 사용합니다.
     - Amplify 관리 인증서를 선택합니다.
   - 사용자 지정 타사 인증서를 사용하세요.
     a. 사용자 지정 SSL 인증서를 선택합니다.
     b. 목록에서 사용할 인증서를 선택합니다.
9. 도메인 추가를 선택합니다.

> **Note**
>
> DNS 전파와 인증서 발급에 최대 24시간이 소요될 수 있습니다. 발생한 오류를 해결하는 데 도움이 필요하면 사용자 지정 도메인 문제 해결 단원을 참조하십시오.

타사 DNS 공급자가 관리하는 사용자 지정 도메인 추가

Amazon Route 53을 사용하여 도메인을 관리하지 않는 경우, Amplify로 배포한 앱에 타사 DNS 공급자가 관리하는 사용자 지정 도메인을 추가할 수 있습니다.

Google 도메인을 사용하는 GoDaddy 경우 해당 제공업체와 관련된 절차는 the section called “에서 관리하는 도메인의 DNS 레코드 업데이트 GoDaddy” 또는 the section called “Google 도메인에서 관리하는 도메인의 DNS 레코드 업데이트” 를 참조하십시오.

타사 DNS 공급자가 관리하는 사용자 지정 도메인 추가

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 사용자 지정 도메인을 추가할 앱을 선택합니다.
3. 탐색 창에서 호스팅, 사용자 지정 도메인을 선택합니다.
4. 사용자 지정 도메인 페이지에서 도메인 추가를 선택합니다.
5. 루트 도메인의 이름을 입력합니다. 예를 들어, 도메인 이름이 https://example.com인 경우, **`example.com`**을(를) 입력합니다.
6. Amplify는 사용자가 Route 53 도메인을 사용하고 있지 않음을 감지하고 Route 53에 호스팅 영역을 생성할 수 있는 옵션을 제공합니다.
   - Route 53에 호스팅 영역을 생성하려면
     a. Route 53에서 호스팅 영역 생성을 선택합니다.
     b. 도메인 구성을 선택합니다.
     c. 호스팅 영역 이름 서버가 콘솔에 표시됩니다. DNS 공급자의 웹사이트로 이동하여 DNS 설정에 이름 서버를 추가합니다.
     d. 위의 네임 서버를 도메인 레지스트리에 추가했습니다. 를 선택합니다.
     e. 7단계로 진행하세요.
   - 수동 구성을 계속하려면

a. 수동 구성을 선택합니다.

b. 도메인 구성을 선택합니다.

c. 7단계로 진행합니다.

7. 기본적으로 Amplify는 도메인에 대해 두 개의 하위 도메인 항목을 자동으로 생성합니다. 예를 들어 도메인 이름이 example.com인 경우, 루트 도메인에서 www 하위 도메인으로 리디렉션이 설정된 하위 도메인 https://www.example.com 및 https://example.com이 표시됩니다.

   (선택 사항) 하위 도메인만을 추가하려는 경우, 기본 구성을 수정할 수 있습니다. 하위 도메인 연결을 참조하십시오. 기본 구성을 변경하려면 탐색 창에서 재작성 및 리디렉션을 선택하고 도메인을 구성합니다.

8. 사용할 SSL/TLS 인증서를 선택합니다. Amplify에서 제공하는 기본 관리 인증서를 사용하거나 가져온 사용자 지정 타사 인증서를 사용할 수 있습니다. AWS Certificate Manager

   - 기본 Amplify 관리 인증서를 사용합니다.

     - Amplify 관리 인증서를 선택합니다.

   - 사용자 지정 타사 인증서를 사용하세요.

     a. 사용자 지정 SSL 인증서를 선택합니다.

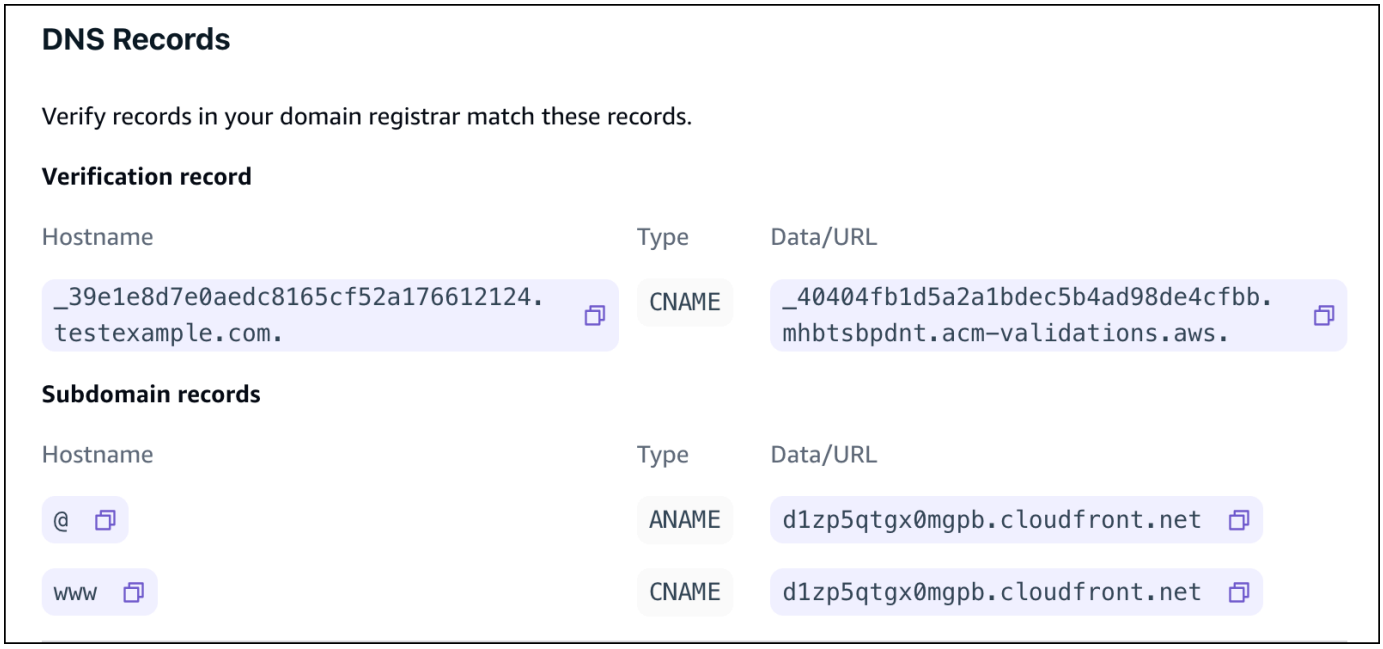
     b. 목록에서 사용할 인증서를 선택합니다.

9. 도메인 추가를 선택합니다.

10. 6단계에서 Route 53에 호스팅 영역 생성을 선택한 경우 15단계로 진행하십시오.

    수동 구성을 선택한 경우 6단계에서 타사 도메인 공급자를 통해 DNS 레코드를 업데이트해야 합니다.

    작업 메뉴에서 DNS 레코드 보기를 선택합니다. 다음 스크린샷은 콘솔에 표시된 DNS 레코드를 보여줍니다.



11. 다음 중 하나를 수행하십시오.

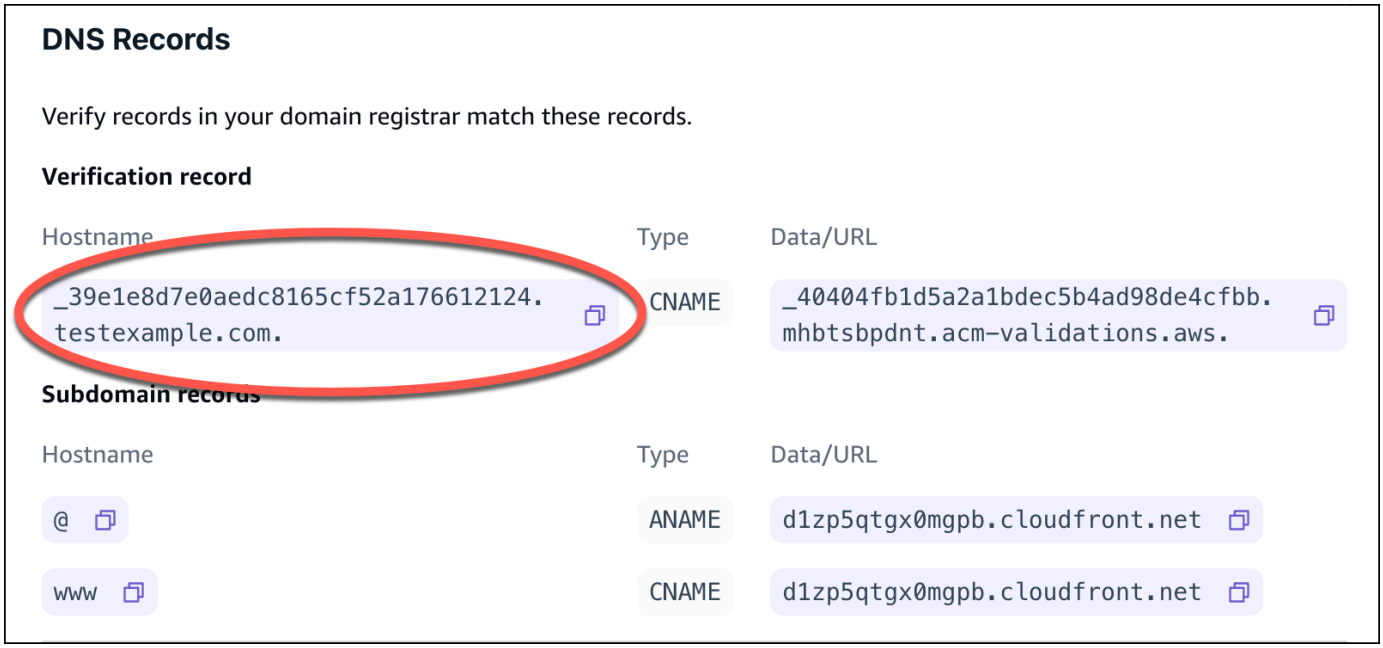
    - 사용 중인 GoDaddy 경우 으로 이동하십시오. 에서 관리하는 도메인의 DNS 레코드 업데이트 GoDaddy
    - Google 도메인을 사용하는 경우, Google 도메인에서 관리하는 도메인의 DNS 레코드 업데이트로 이동하십시오.
    - 다른 타사 DNS 공급자를 사용하는 경우, 이 절차의 다음 단계로 이동하십시오.

12. DNS 공급자의 웹사이트로 이동하여 계정에 로그인한 다음 도메인의 DNS 관리 설정을 찾으십시오. 두 개의 CNAME 레코드를 구성하게 됩니다.

13. 첫 번째 CNAME 레코드가 하위 도메인이 유효성 검사 서버를 가리키도록 구성합니다. AWS

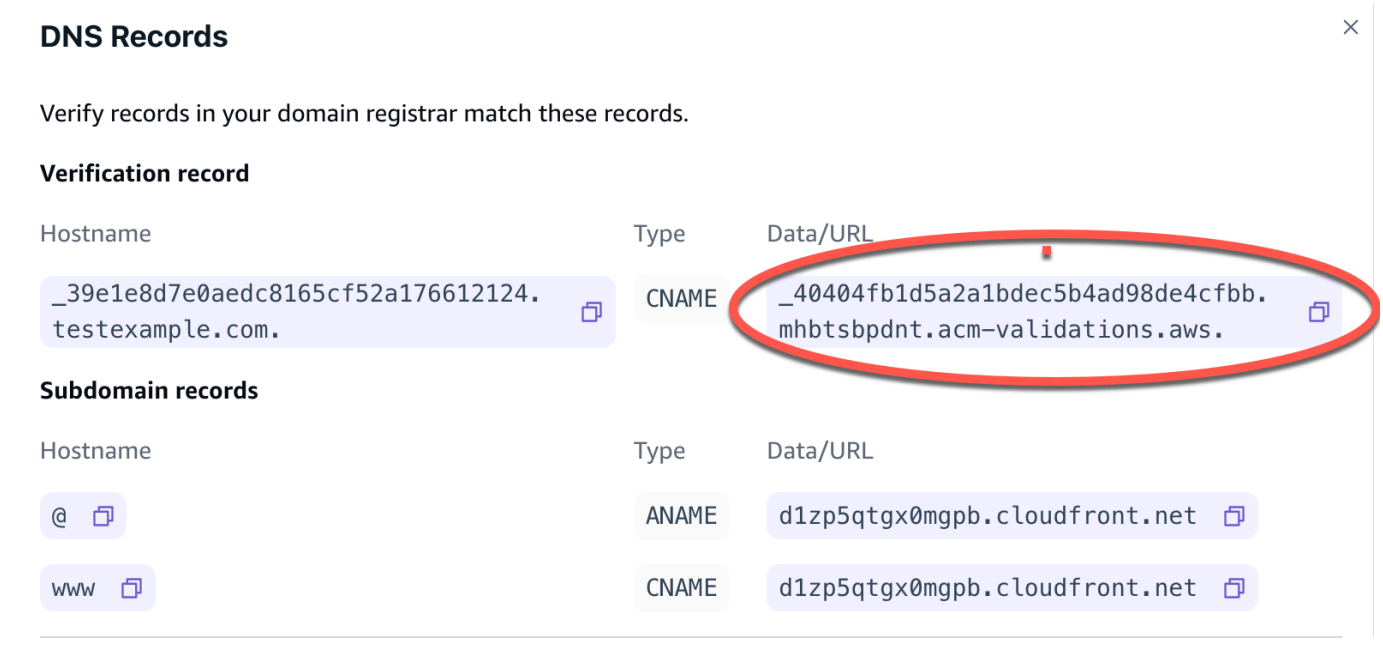
    Amplify 콘솔에 _c3e2d7eaf1eaf1e656b73f46cd6980fdc0e.example.com과 같은 하위 도메인의 소유권을 확인하기 위한 DNS 레코드가 표시되는 경우 CNAME 레코드 하위 도메인 이름에만 입력하십시오. **`_c3e2d7eaf1e656b73f46cd6980fdc0e`**

    다음 스크린샷은 사용할 확인 레코드의 위치를 보여줍니다.



Amplify 콘솔에 _cjhwou20vhu2exampleuw20vuyb2ovb9.j9s73ucn9vy.acm-validations.aws 와 같은 ACM 검증 서버 레코드가 표시되는 경우 CNAME 레코드 값으로 입력하십시오. **`_cjhwou20vhu2exampleuw20vuyb2ovb9.j9s73ucn9vy.acm-validations.aws`**

다음 스크린샷은 사용할 ACM 검증 레코드의 위치를 보여줍니다.



Amplify는 이 정보를 사용하여 도메인 소유권을 확인하고 도메인의 SSL/TLS 인증서를 생성합니다. Amplify이 도메인의 소유권을 확인하면 모든 트래픽이 HTTPS/2를 통해 제공됩니다.

> **Note**
>
> AWS Certificate Manager (ACM) 에서 생성한 기본 Amplify 인증서는 13개월 동안 유효하며 Amplify에서 앱을 호스팅하는 한 자동으로 갱신됩니다. CNAME 확인 레코드가 수정 또는 삭제된 경우, Amplify는 인증서를 갱신할 수 없습니다. Amplify 콘솔에서 도메인을 삭제하고 다시 추가해야 합니다.

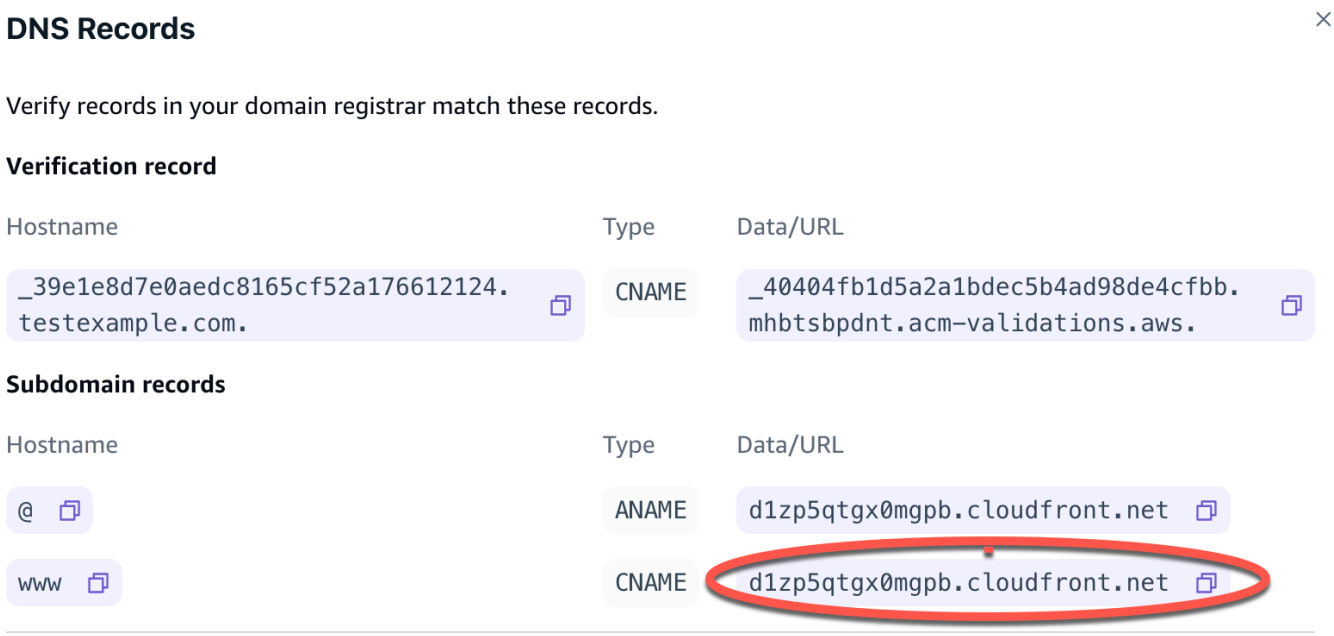
> **Important**
>
> Amplify 콘솔에서 사용자 지정 도메인을 추가한 후 바로 이 단계를 수행하는 것이 중요합니다. AWS Certificate Manager (ACM) 은 즉시 소유권 확인을 시도하기 시작합니다. 시간이 지나면 검사 빈도가 줄어듭니다. 앱을 만든 후 몇 시간 후에 CNAME 레코드를 추가하거나 업데이트하면 앱이 확인 보류 중 상태에서 멈출 수 있습니다.

14. 하위 도메인이 Amplify 도메인을 가리키도록 두 번째 CNAME 레코드를 구성합니다. 예를 들어, 하위 도메인이 www.example.com인 경우 하위 도메인 이름으로 www를 입력합니다.

    Amplify 콘솔에 앱의 도메인이 d111111abcdef8.cloudfront.net으로 표시되는 경우 Amplify 도메인을 입력하십시오. **`d111111abcdef8.cloudfront.net`**

    프로덕션 트래픽이 있는 경우, 도메인 상태가 Amplify 콘솔에서 AVAILABLE을 표시한 후 CNAME 레코드를 업데이트하는 것이 좋습니다.

    다음 스크린샷은 사용할 도메인 이름 레코드의 위치를 보여줍니다.



15. 앱의 루트 도메인 (예: https://example.com) 을 가리키도록 ANAME/ALIAS 레코드를 구성합니다. ANAME 레코드는 도메인의 루트가 호스트 이름을 가리킬 수 있습니다. 프로덕션 트래픽이 있는 경우, 도메인 상태가 콘솔에서 AVAILABLE을 표시한 후 ANAME 레코드를 업데이트하는 것이 좋습니다.* ANAME/ALIAS 지원 기능이 없는 DNS 공급자의 경우, DNS를 Route 53으로 마이그레이션하는 것이 좋습니다. 자세한 내용은 Amazon Route 53을 DNS 서비스로 구성을 참조하십시오.

> **Note**
>
> 타사 도메인에 대한 도메인 소유권 및 DNS 전파 확인에는 최대 48시간이 소요될 수 있습니다. 발생하는 오류를 해결하는 데 도움이 필요하면 사용자 지정 도메인 문제 해결을 참조하십시오.

에서 관리하는 도메인의 DNS 레코드 업데이트 GoDaddy

에서 관리하는 사용자 지정 도메인을 추가하려면 GoDaddy

1. 로 GoDaddy DNS 레코드를 업데이트하려면 먼저 절차의 1~9단계를 the section called “타사 DNS 공급자가 관리하는 사용자 지정 도메인 추가” 완료하십시오.
2. GoDaddy 계정에 로그인합니다.
3. 도메인 목록에서 추가할 도메인을 찾아 DNS 관리를 선택합니다.
4. DNS 페이지의 DNS 레코드 섹션에 도메인의 레코드 목록이 GoDaddy 표시됩니다. 새 CNAME 레코드 두 개를 추가해야 합니다.

5. 첫 번째 CNAME 레코드를 생성하여 하위 도메인이 Amplify 도메인을 가리키도록 합니다.

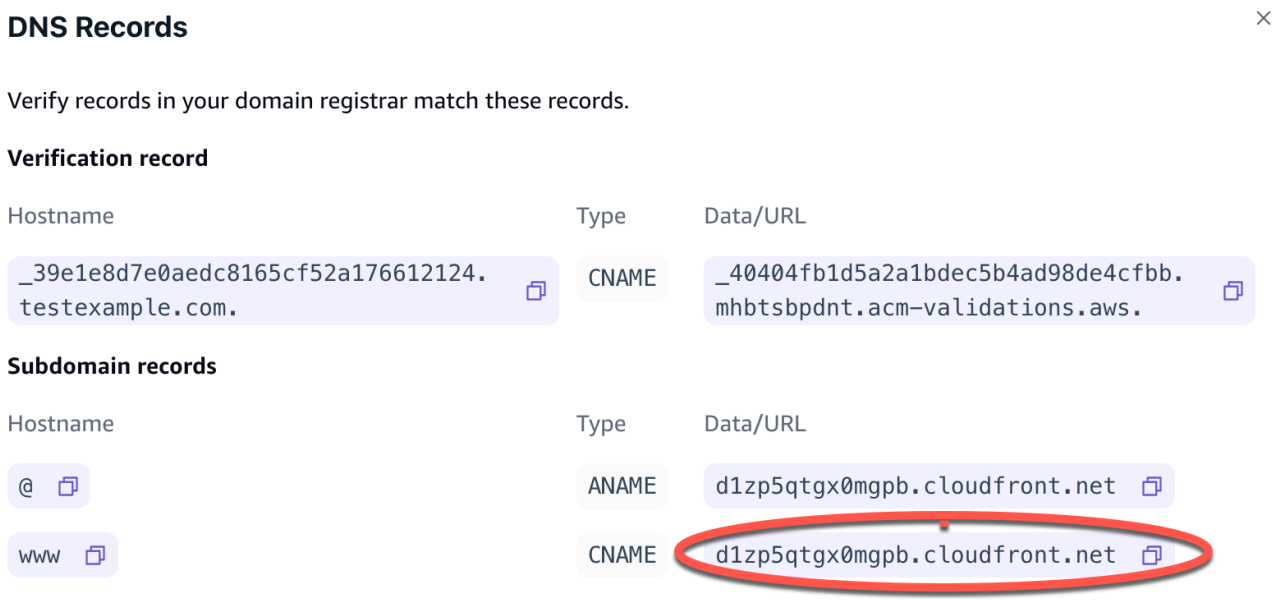
   a. DNS 레코드 섹션에서 새 레코드 추가를 선택합니다.

   b. 유형에서 CNAME을 선택합니다.

   c. 이름에는 하위 도메인만 입력합니다. 예를 들어, 하위 도메인이 www.example.com인 경우, 이름에 www를 입력합니다.

   d. 값의 경우, Amplify 콘솔에서 DNS 레코드를 확인한 다음 값을 입력합니다. Amplify 콘솔에 앱의 도메인이 d111111abcdef8.cloudfront.net으로 표시되는 경우 값에 입력하십시오.
   `d111111abcdef8.cloudfront.net`

   다음 스크린샷은 사용할 도메인 이름 레코드의 위치를 보여줍니다.



   e. 저장을 선택합니다.

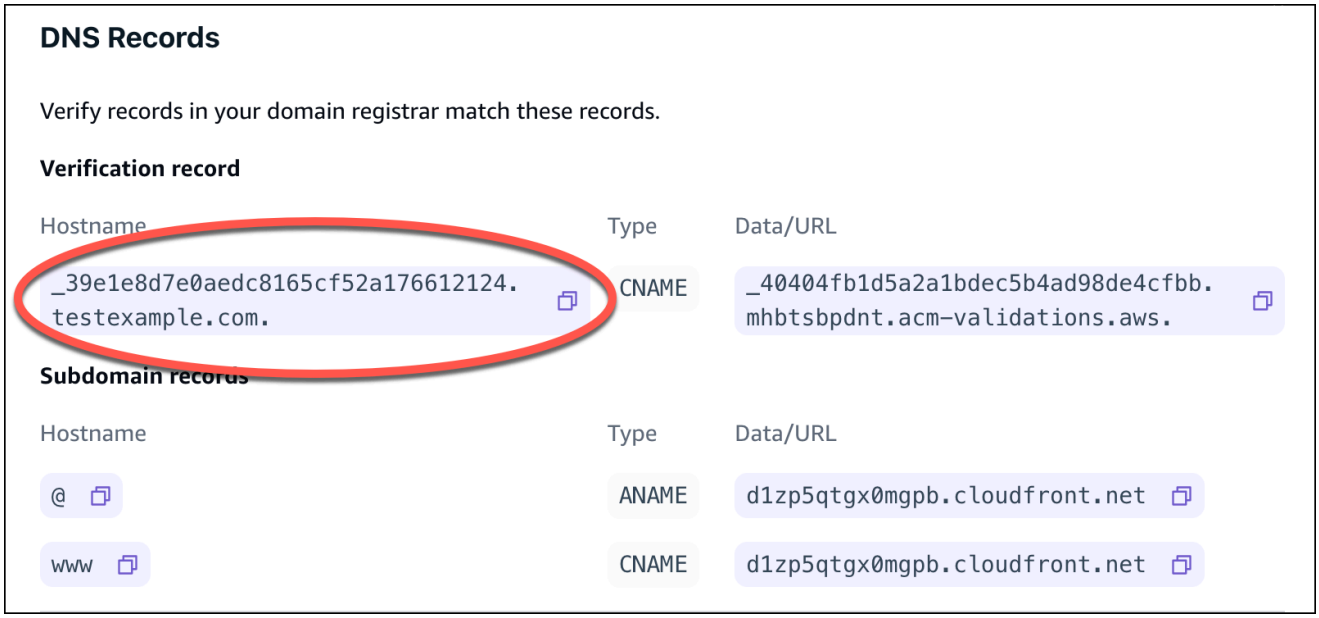
6. AWS Certificate Manager (ACM) 검증 서버를 가리키도록 두 번째 CNAME 레코드를 생성합니다. 확인된 단일 ACM이 도메인의 SSL/TLS 인증서를 생성합니다.

   a. 유형에서 CNAME을 선택합니다.

   b. 이름에 하위 도메인을 입력합니다.

   예를 들어, 하위 도메인의 소유권을 확인하기 위한 Amplify 콘솔의 DNS 레코드가 _c3e2d7eaf1e656b73f46cd6980fdc0e.example.com인 경우 이름에만 입력하십시오.
   `_c3e2d7eaf1e656b73f46cd6980fdc0e`

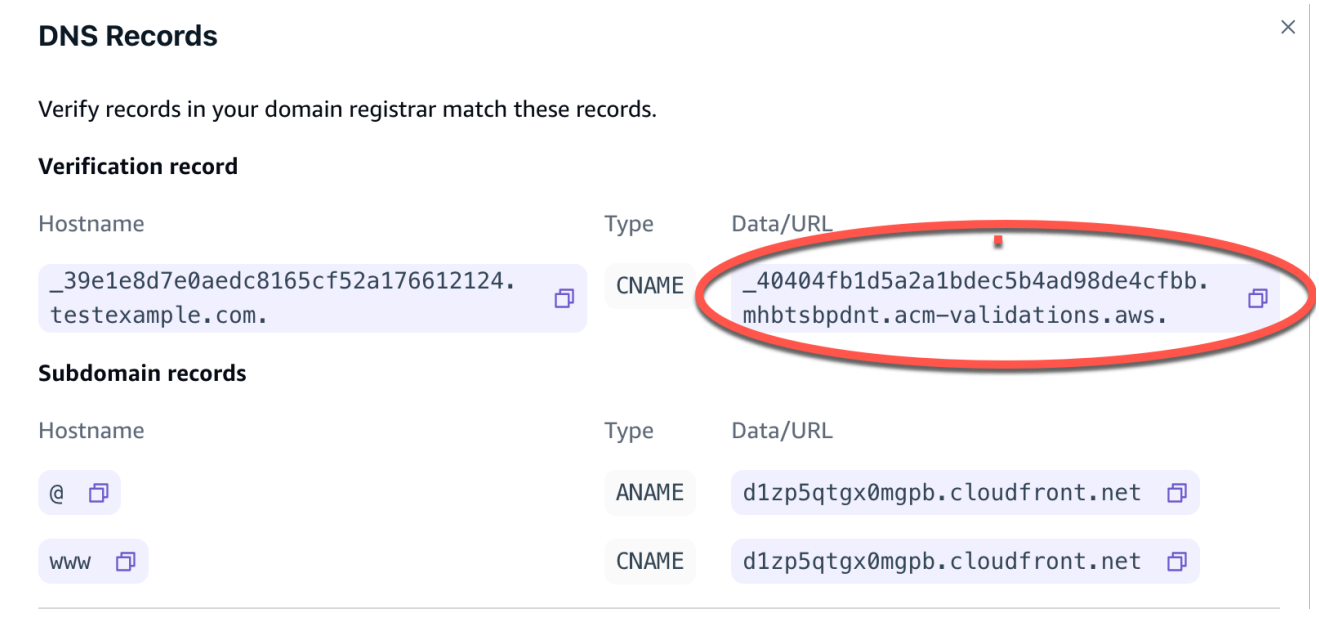
   다음 스크린샷은 사용할 확인 레코드의 위치를 보여줍니다.



c. 값에는 ACM 검증 인증서를 입력하십시오.

예를 들어 검증 서버가 _cjhwou20vhu2exampleuw20vuyb2ovb9.j9s73ucn9vy.acm-validations.aws인 경우, 값에 _cjhwou20vhu2exampleuw20vuyb2ovb9.j9s73ucn9vy.acm-validations.aws를 입력합니다.

다음 스크린샷은 사용할 ACM 확인 레코드의 위치를 보여줍니다.



d. 저장을 선택합니다.

> **Note**
>
> AWS Certificate Manager (ACM) 에서 생성한 기본 Amplify 인증서는 13개월 동안 유효하며 Amplify에서 앱을 호스팅하는 한 자동으로 갱신됩니다. CNAME 확인 레코드가 수정 또는 삭제된 경우, Amplify는 인증서를 갱신할 수 없습니다. Amplify 콘솔에서 도메인을 삭제하고 다시 추가해야 합니다.

7. 하위 도메인에는 이 단계가 필요하지 않습니다. GoDaddy ANAME/ALIAS 레코드는 지원하지 않습니다. ANAME/ALIAS 지원 기능이 없는 DNS 공급자의 경우, DNS를 Amazon Route 53으로 마이그레이션하는 것이 좋습니다. 자세한 내용은 Amazon Route 53을 DNS 서비스로 구성을 참조하십시오.

   GoDaddy 공급자로 유지하고 루트 도메인을 업데이트하려면 전달을 추가하고 도메인 포워딩을 설정하세요.

   a. DNS 페이지에서 페이지 상단의 메뉴를 찾아 전달을 선택합니다.
   b. 도메인 섹션에서 전달 추가를 선택합니다.
   c. http://를 선택한 다음 대상 URL로 전달할 하위 도메인의 이름 (예: www.example.com) 을 입력합니다.
   d. 전송 유형에서는 임시(302)를 선택합니다.
   e. 저장을 선택합니다.

Google 도메인에서 관리하는 도메인의 DNS 레코드 업데이트

Google 도메인에서 관리하는 맞춤 도메인을 추가하려면

1. Google 도메인으로 DNS 레코드를 업데이트하려면 먼저 타사 DNS 공급자가 관리하는 사용자 지정 도메인을 추가하려면 절차의 1~9단계를 완료하세요.
2. https://domains.google.com에서 계정에 로그인하고 왼쪽 탐색 창에서 내 도메인을 선택합니다.
3. 도메인 목록에서 추가할 도메인을 찾아 관리를 선택합니다.
4. 왼쪽 탐색 창에서 DNS를 선택합니다. Google은 도메인의 리소스 레코드를 표시합니다. 새 CNAME 레코드 두 개를 추가해야 합니다.
5. 다음과 같이 첫 번째 CNAME 레코드를 생성하여 모든 하위 도메인이 Amplify 도메인을 가리키도록 합니다.

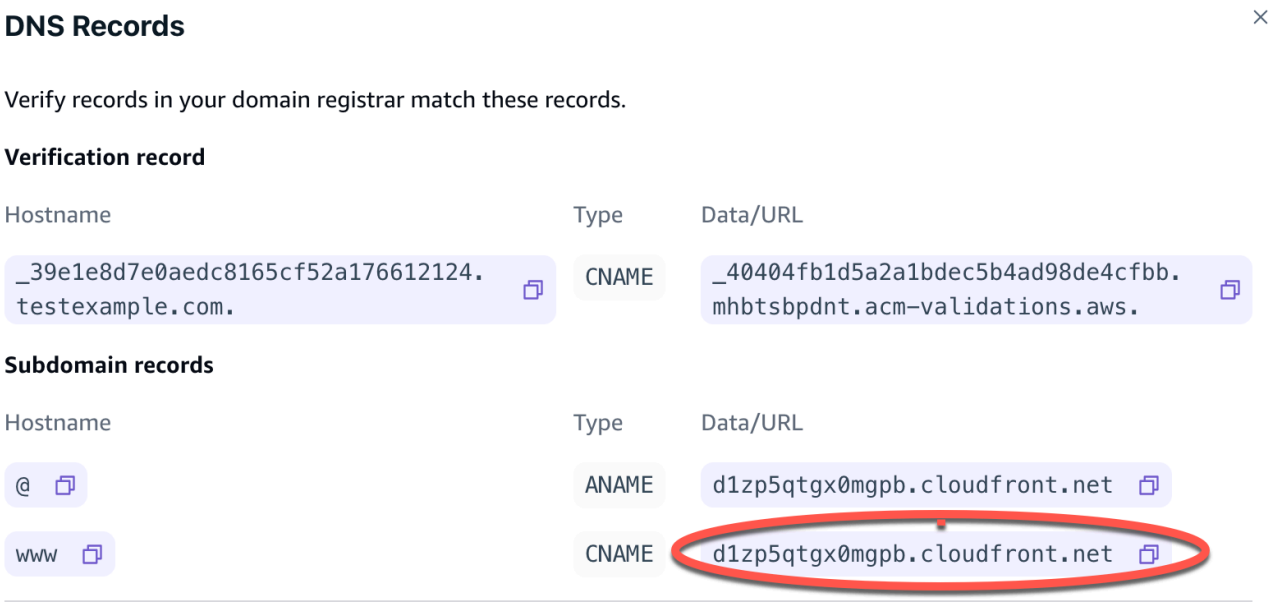
a. 호스트 이름에는 하위 도메인 이름만 입력합니다. 예를 들어, 하위 도메인이 www.example.com인 경우, 호스트 이름에 www를 입력합니다.

b. 유형에서 CNAME을 선택합니다.

c. 데이터에 Amplify 콘솔에서 사용할 수 있는 값을 입력합니다.

Amplify 콘솔에 앱의 도메인이 d111111abcdef8.cloudfront.net으로 표시되는 경우, 데이터에 d111111abcdef8.cloudfront.net을 입력하십시오.

다음 스크린샷은 사용할 도메인 이름 레코드의 위치를 보여줍니다.

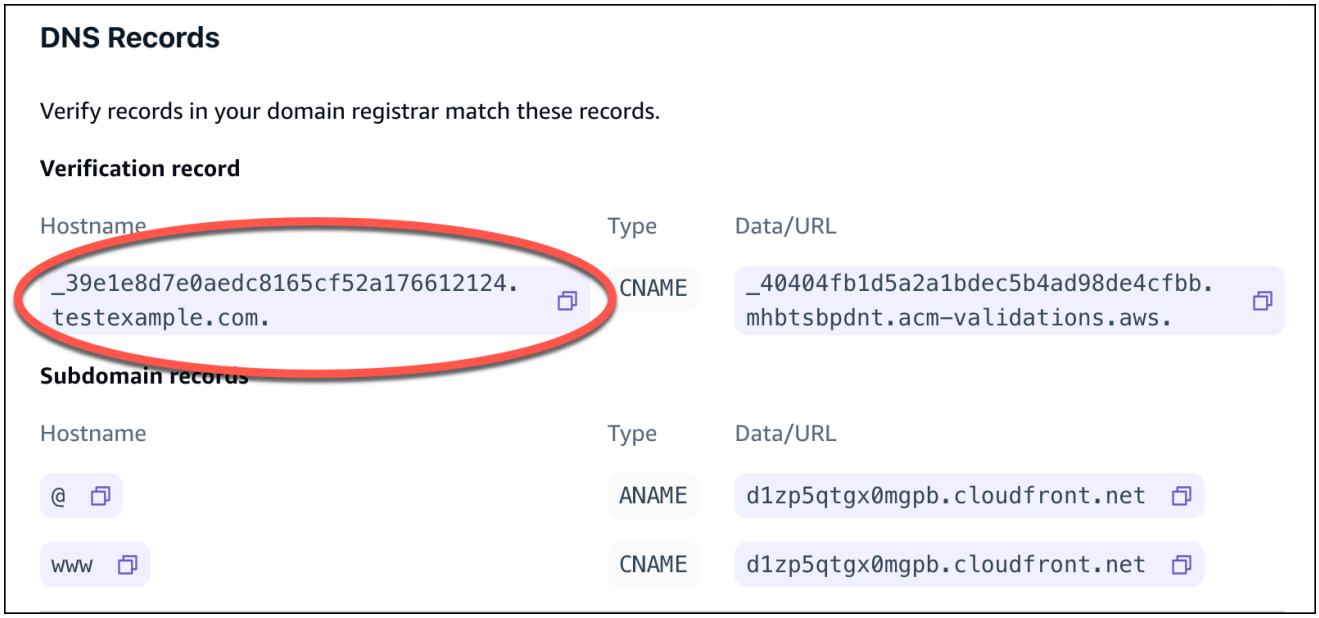


6. AWS Certificate Manager (ACM) 검증 서버를 가리키도록 두 번째 CNAME 레코드를 생성합니다. 확인된 단일 ACM이 도메인의 SSL/TLS 인증서를 생성합니다.

a. 호스트 이름에는 하위 도메인을 입력합니다.

예를 들어, 하위 도메인의 소유권을 확인하기 위한 Amplify 콘솔의 DNS 레코드가 _c3e2d7eaf1e656b73f46cd6980fdc0e.example.com인 경우, 호스트 이름으로 _c3e2d7eaf1e656b73f46cd6980fdc0e만 입력하십시오.

다음 스크린샷은 사용할 확인 레코드의 위치를 보여줍니다.

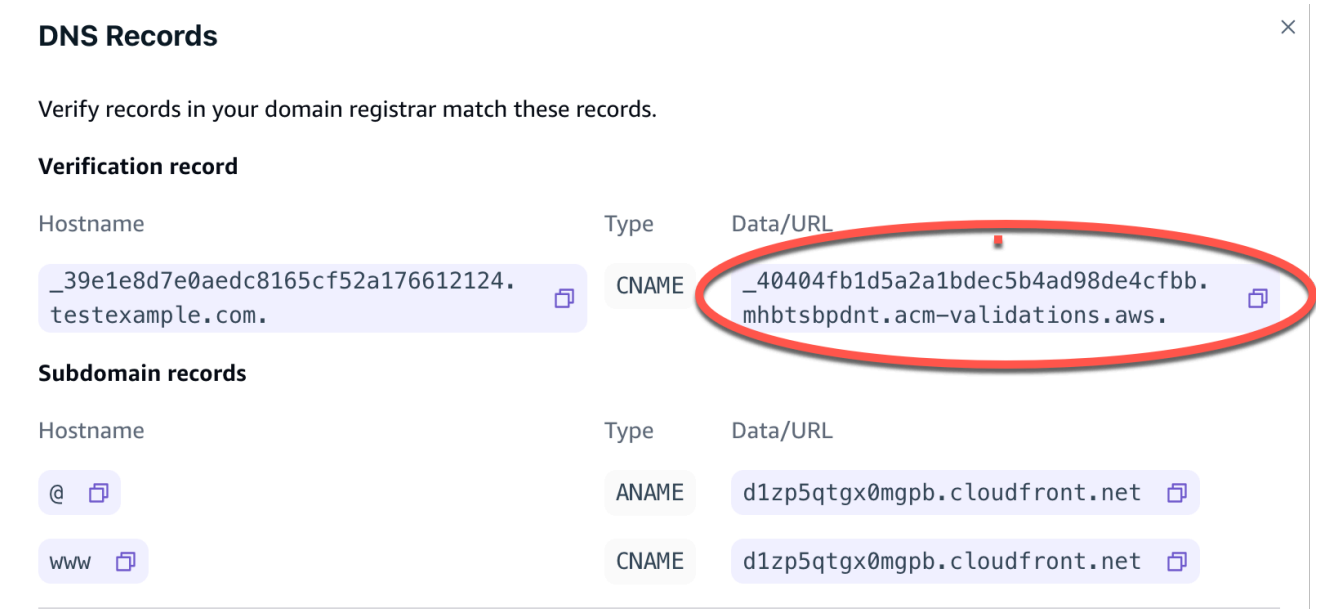


b. 유형에서 CNAME을 선택합니다.

c. 데이터에는 ACM 검증 인증서를 입력하십시오.

예를 들어 검증 서버가 _cf1z2npwt9vzexample93c1j4xzc92wl.2te3iym6kzr.acm-validations.aws인 경우, 데이터로 _cf1z2npwt9vzexample93c1j4xzc92wl.2te3iym6kzr.acm-validations.aws를 입력하십시오.

다음 스크린샷은 사용할 ACM 확인 레코드의 위치를 보여줍니다.



7. 저장을 선택합니다.

> **Note**
>
> AWS Certificate Manager (ACM) 에서 생성한 기본 Amplify; 인증서는 13개월 동안 유효하며 Amplify에서 앱을 호스팅하는 한 자동으로 갱신됩니다. CNAME 확인 레코드가 수정 또는 삭제된 경우, Amplify는 인증서를 갱신할 수 없습니다. Amplify 콘솔에서 도메인을 삭제하고 다시 추가해야 합니다.

8. ANAME/ALIAS 레코드에 대한 Google 도메인 지원이 미리 보기로 제공됩니다. ANAME/ALIAS 지원 기능이 없는 DNS 공급자의 경우, DNS를 Amazon Route 53으로 마이그레이션하는 것이 좋습니다. 자세한 내용은 Amazon Route 53을 DNS 서비스로 구성을 참조하십시오. Google 도메인을 공급자로 유지하고 루트 도메인을 업데이트하려면 하위 도메인을 전송으로 설정하십시오. Google 도메인의 웹 사이트 페이지를 찾습니다. 그런 다음 도메인 전송을 선택하고 웹 전송 페이지에서 전송을 구성합니다.

> **Note**
>
> Google 도메인에 대한 DNS 설정 업데이트가 적용되려면 최대 48시간이 걸립니다. 발생한 오류를 해결하는 데 도움이 필요하면 사용자 지정 도메인 문제 해결을 참조하십시오.

도메인의 SSL/TLS 인증서를 업데이트하세요.

도메인에 사용 중인 SSL/TLS 인증서는 언제든지 변경할 수 있습니다. 예를 들어 관리형 인증서 사용에서 사용자 지정 인증서 사용으로 변경할 수 있습니다. 도메인에 사용 중인 사용자 지정 인증서를 변경할 수도 있습니다. 인증서에 대한 자세한 내용은 SSL/TLS 인증서 사용을 참조하십시오.

다음 절차를 사용하여 도메인에 사용 중인 사용자 지정 인증서 또는 인증서 유형을 업데이트하십시오.

도메인의 인증서를 업데이트하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 업데이트하려는 앱을 선택합니다.
3. 탐색 창에서 호스팅, 사용자 지정 도메인을 선택합니다.
4. 사용자 지정 도메인 페이지에서 도메인 구성을 선택합니다.
5. 도메인의 세부 정보 페이지에서 사용자 지정 SSL 인증서 섹션을 찾으십시오. 인증서 업데이트 절차는 변경하려는 유형에 따라 다릅니다.

- 사용자 지정 인증서를 기본 Amplify 관리 인증서로 변경하려면
  - Amplify 관리 인증서를 선택합니다.
- 관리형 인증서에서 사용자 지정 인증서로 변경하려면
  a. 사용자 지정 SSL 인증서를 선택합니다.
  b. 목록에서 사용할 인증서를 선택합니다.
- 사용자 지정 인증서를 다른 사용자 지정 인증서로 변경하려면
  - 사용자 지정 SSL 인증서의 경우 목록에서 사용할 새 인증서를 선택합니다.

6. 저장을 선택합니다. 도메인의 상태 세부 정보는 Amplify가 관리 인증서에 대한 SSL 생성 프로세스 또는 사용자 지정 인증서에 대한 구성 프로세스를 시작했음을 나타냅니다.

하위 도메인 관리

하위 도메인은 도메인 이름 앞에 나타나는 URL의 일부입니다. 예를 들어 www는 www.amazon.com의 하위 도메인이고 aws는 aws.amazon.com의 하위 도메인입니다. 이미 프로덕션 웹사이트가 있는 경우, 하위 도메인만 연결하는 것이 좋습니다. 하위 도메인은 다중 수준일 수도 있습니다. 예를 들어 beta.alpha.example.com에는 다중 수준 하위 도메인 beta.alpha가 있습니다.

하위 도메인만 추가하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 하위 도메인을 추가할 앱을 선택합니다.
3. 탐색 창에서 호스팅을 선택한 다음 사용자 지정 도메인을 선택합니다.
4. 사용자 지정 도메인 페이지에서 도메인 추가를 선택합니다.
5. 루트 도메인의 이름을 입력한 다음 도메인 구성을 선택합니다. 예를 들어 도메인 이름이 https://example.com 인 경우 example.com을 입력합니다.
6. 루트 제외를 선택하고 하위 도메인의 이름을 수정합니다. 예를 들어 도메인이 example.com인 경우, 하위 도메인 알파만 추가하도록 수정할 수 있습니다.
7. 도메인 추가를 선택합니다.

다단계 하위 도메인을 추가하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.

2. 다단계 하위 도메인을 추가할 앱을 선택합니다.
3. 탐색 창에서 호스팅을 선택한 다음 사용자 지정 도메인을 선택합니다.
4. 사용자 지정 도메인 페이지에서 도메인 추가를 선택합니다.
5. 하위 도메인이 있는 도메인의 이름을 입력하고 루트 제외를 선택한 다음 하위 도메인을 수정하여 새 수준을 추가합니다.

   예를 들어 alpha.example.com이라는 도메인이 있고 다단계 하위 도메인 beta.alpha.example.com을 만들려면 하위 도메인 값으로 베타를 입력합니다.
6. 도메인 추가를 선택합니다.

하위 도메인을 추가 또는 편집하려면

앱에 사용자 지정 도메인을 추가한 후 기존 하위 도메인을 편집하거나 새 하위 도메인을 추가할 수 있습니다.

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 하위 도메인을 관리할 앱을 선택합니다.
3. 탐색 창에서 호스팅을 선택한 다음 사용자 지정 도메인을 선택합니다.
4. 사용자 지정 도메인 페이지에서 도메인 구성을 선택합니다.
5. 하위 도메인 섹션에서 필요에 따라 기존 하위 도메인을 편집할 수 있습니다.
6. (선택 사항) 새 하위 도메인을 추가하려면 새로 추가를 선택합니다.
7. 저장을 선택합니다.

Wildcard 하위 도메인

Amplify 호스팅은 이제 와일드카드 하위 도메인을 지원합니다. 와일드카드 하위 도메인은 기존 하위 도메인과 존재하지 않는 하위 도메인을 애플리케이션의 특정 브랜치로 가리킬 수 있는 포괄적인 하위 도메인입니다. 와일드카드를 사용하여 앱의 모든 하위 도메인을 특정 브랜치에 연결하면 모든 하위 도메인의 앱 사용자에게 동일한 콘텐츠를 제공할 수 있으므로 각 하위 도메인을 개별적으로 구성하지 않아도 됩니다.

와일드카드 하위 도메인을 만들려면 하위 도메인 이름으로 별표(*) 를 지정하십시오. 예를 들어 앱의 특정 브랜치에 와일드카드 하위 도메인을 `*.example.com` 지정하는 경우, example.com으로 끝나는 모든 URL은 브랜치로 라우팅됩니다. 이 경우, `dev.example.com` 및 에 대한 요청은 하위 도메인으로 `prod.example.com` 라우팅됩니다. `*.example.com`

Amplify는 사용자 지정 도메인에 대해서만 와일드카드 하위 도메인을 지원합니다. 기본 `amplifyapp.com` 도메인에서는 이 기능을 사용할 수 없습니다.

Wildcard 하위 도메인에 적용되는 요구 사항은 다음과 같습니다.

- 하위 도메인 이름은 별표(*) 로만 지정해야 합니다.
- 와일드카드를 사용하여 하위 도메인 이름의 일부를 대체할 수 없습니다(예: *domain.example.com).
- 도메인 이름의 중간에 있는 하위 도메인은 바꿀 수 없습니다(예: subdomain.*.example.com).
- 기본적으로 모든 Amplify 프로비저닝 인증서는 사용자 지정 도메인의 모든 하위 도메인을 포함합니다.

와일드카드 하위 도메인을 추가 또는 삭제하려면

앱에 커스텀 도메인을 추가한 후 앱 브랜치에 와일드카드 하위 도메인을 추가할 수 있습니다.

1. AWS Management Console 로그인하고 Amplify 호스팅 콘솔을 엽니다.
2. 와일드카드 하위 도메인을 관리할 앱을 선택합니다.
3. 탐색 창에서 호스팅을 선택한 다음 사용자 지정 도메인을 선택합니다.
4. 사용자 지정 도메인 페이지에서 도메인 구성을 선택합니다.
5. 하위 도메인 섹션에서 와일드카드 하위 도메인을 추가하거나 삭제할 수 있습니다.
   - 새 Wildcard 하위 도메인을 추가하려면
     a. 새로 추가를 선택합니다.
     b. 하위 도메인에 대해 *****을 입력합니다.
     c. 앱 브랜치의 경우, 목록에서 브랜치 이름을 선택합니다.
     d. 저장을 선택합니다.
   - 와일드카드 하위 도메인을 삭제하려면
     a. 하위 도메인 이름 옆의 제거를 선택합니다. 명시적으로 구성되지 않은 하위 도메인으로의 트래픽이 중지되고 Amplify Hosting은 해당 요청에 404 상태 코드를 반환합니다.
     b. 저장을 선택합니다.

Amazon Route 53 사용자 지정 도메인을 위한 자동 하위 도메인을 설정합니다.

앱이 Route 53의 사용자 지정 도메인에 연결되면 Amplify를 사용하면 새로 연결된 브랜치의 하위 도메인을 자동으로 생성할 수 있습니다. 예를 들어 dev 브랜치를 연결하면 Amplify는 dev.exampledomain.com을 자동으로 생성할 수 있습니다. 브랜치를 삭제하면 연결된 모든 하위 도메인이 자동으로 삭제됩니다.

새로 연결된 브랜치에 자동 하위 도메인 생성을 설정하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. Route 53에서 관리되는 사용자 지정 도메인에 연결된 앱을 선택합니다.
3. 탐색 창에서 호스팅을 선택한 다음 사용자 지정 도메인을 선택합니다.
4. 사용자 지정 도메인 페이지에서 도메인 구성을 선택합니다.
5. 자동 하위 도메인 생성 섹션에서 기능을 켜십시오.

> **Note**
>
> 이 기능은 루트 도메인(예: exampledomain.com)에서만 사용할 수 있습니다. 도메인이 이미 dev.exampledomain.com과 같은 하위 도메인인 경우에는 Amplify 콘솔에 이 확인란이 표시되지 않습니다.

하위 도메인이 포함된 웹 미리 보기

위 지침에 따라 자동 하위 도메인 생성을 활성화하면 자동으로 생성된 하위 도메인을 통해 앱의 풀 리퀘스트 웹 미리보기에도 액세스할 수 있습니다. pull 요청가 종료되면 연결된 브랜치 및 하위 도메인이 자동으로 삭제됩니다. pull 요청의 웹 미리 보기 설정에 대한 자세한 내용은 pull 요청를 위한 웹 미리 보기 단원을 참조하십시오.

사용자 지정 도메인 문제 해결

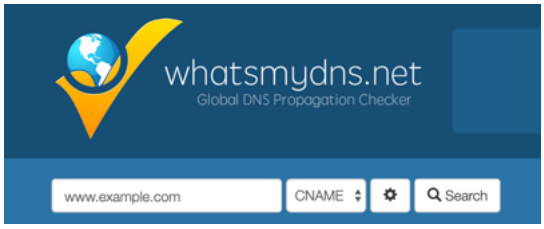
AWS Amplify 콘솔에서 앱에 사용자 지정 도메인을 추가할 때 문제가 발생하는 경우, 이 섹션의 다음 항목에서 문제 해결 도움말을 참조하십시오.

여기에서 문제 해결 방법을 찾을 수 없다면 AWS Support에 문의하세요. 자세한 내용을 알아보려면 AWS Support 사용 설명서의 지원 사례 만들기를 참조하세요.

주제

CNAME 리졸빙이 되는지 어떻게 확인합니까?

1. 타사 도메인 공급자와 함께 DNS 레코드를 업데이트한 후에는 dig와 같은 도구나 https://www.whatsmydns.net/과 같은 무료 웹사이트를 사용하여 CNAME 레코드가 제대로 해결되고 있는지 확인할 수 있습니다. 다음 스크린샷은 whatsmydns.net을 사용하여 www.example.com 도메인의 CNAME 레코드를 확인하는 방법을 보여줍니다.



2. 검색을 선택하면 whatsmydns.net에 CNAME에 대한 결과가 표시됩니다. 다음 스크린샷은 CNAME이 cloudfront.net URL로 올바르게 확인되는지 확인하는 결과 목록의 예입니다.

타사에서 호스팅하는 도메인이 확인 보류 상태로 고착된 경우,

1. 커스텀 도메인이 확인 보류 중 상태에서 멈춘 경우, CNAME 레코드가 해결되고 있는지 확인하십시오. 이 작업을 수행하는 방법에 대한 지침은 이전 문제 해결 항목인 CNAME 문제가 해결되었는지 확인하는 방법을 참조하십시오.
2. CNAME 레코드가 확인되지 않는 경우, 도메인 공급자의 DNS 설정에 해당 CNAME 항목이 있는지 확인하십시오.

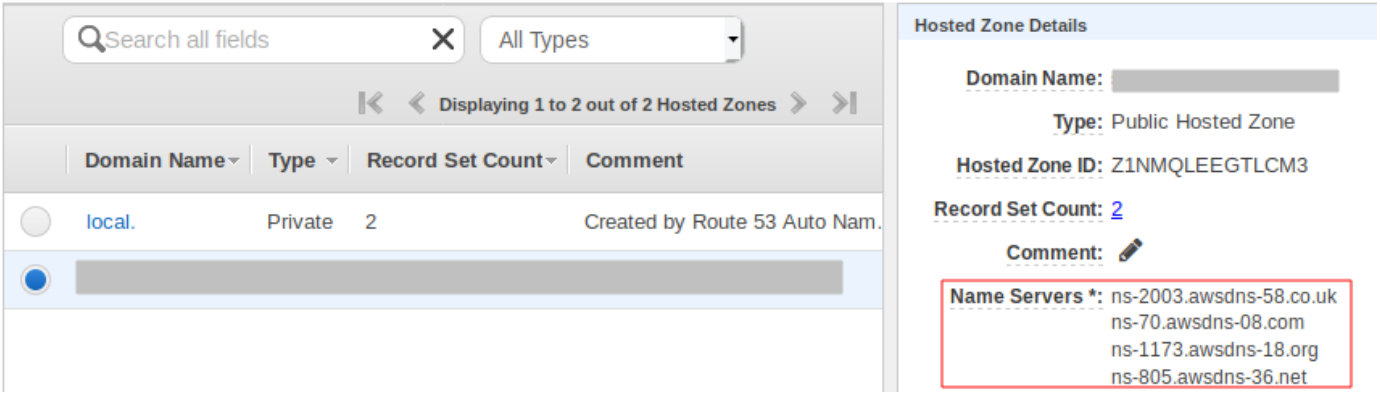
> **Important**
>
> 사용자 지정 도메인을 생성하는 즉시 CNAME 레코드를 업데이트하는 것이 중요합니다. 앱이 Amplify 콘솔에 생성되면 몇 분마다 CNAME 레코드의 리졸빙 여부를 확인해야 합니다. 1시간 후에 리졸빙이 되지 않는 경우, 몇 시간마다 확인을 해야 하므로 도메인의 사용 준비 완료에 지연이 초래될 수 있습니다. 앱을 만든 후 몇 시간 후에 CNAME 레코드를 추가하거나 업데이트한 경우, 이로 인해 앱이 확인 보류 중 상태에서 멈출 가능성이 높습니다.

3. CNAME 레코드가 존재하는지 확인한 경우, DNS 공급자에 문제가 있을 수 있습니다. DNS 공급자에게 연락하여 DNS 확인 CNAME 리졸빙이 되지 않는 이유를 진단하거나 DNS를 Route 53로 마이그레이션할 수 있습니다. 자세한 내용은 Amazon Route 53을 기존 도메인의 DNS 서비스로 지정 단원을 참조하십시오.

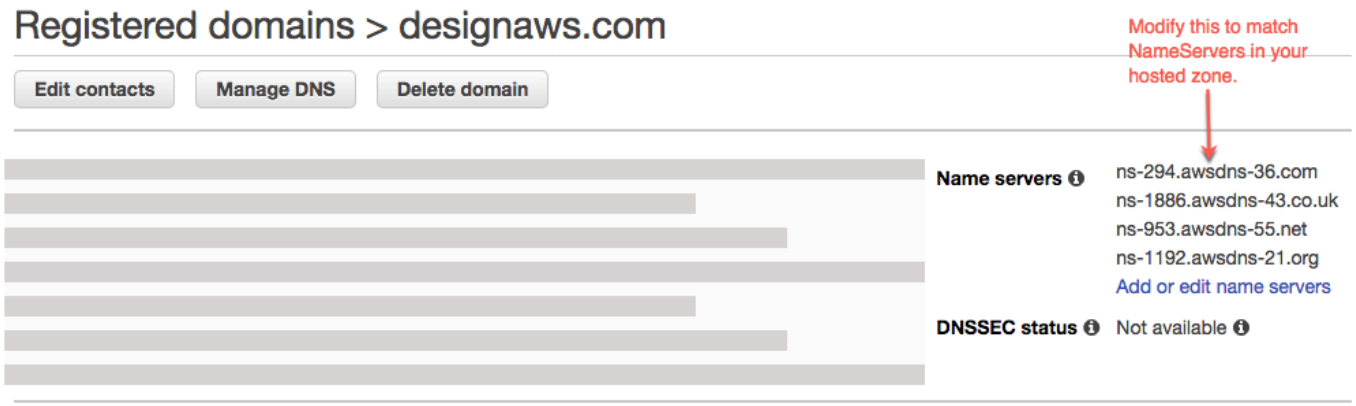
Amazon Route 53으로 호스팅된 도메인이 확인 보류 상태로 고착된 경우,

도메인을 Amazon Route 53으로 이전한 경우, 도메인은 앱 생성 시 Amplify에서 발급한 것과 다른 이름 서버를 가질 수 있습니다. 오류의 원인을 진단하려면 다음 단계를 수행하십시오.

1. Amazon Route 53 콘솔에 로그인합니다.
2. 탐색 창에서 호스팅 영역을 선택한 다음 연결 중인 도메인의 이름을 선택합니다.
3. 호스팅 영역 세부 정보 섹션에서 이름 서버 값을 기록합니다. 다음 단계를 완료하려면 이 값이 모두 필요합니다. Route 53 콘솔의 다음 스크린샷은 오른쪽 하단에 이름 서버 값의 위치를 표시합니다.



4. 탐색 창에서 등록된 도메인을 선택합니다. 등록된 도메인 섹션에 표시된 이름 서버가 호스팅 영역 세부 정보 섹션의 이전 단계에서 기록한 이름 서버 값과 일치하는지 확인하십시오. 일치하지 않는 경우, 이름 서버 값을 호스팅 영역의 값과 일치하도록 편집하십시오. Route 53 콘솔의 다음 스크린샷은 오른쪽에 이름 서버 값의 위치를 표시합니다.



5. 이렇게 해도 문제가 해결되지 않으면 AWS Support에 문의하세요. 자세한 내용을 알아보려면 AWS Support 사용 설명서의 지원 사례 만들기를 참조하세요.

CNAME 오류가 발생합니다. AlreadyExistsException

CNAME AlreadyExistsException 오류가 발생하면 연결하려고 시도한 호스트 이름 중 하나 (하위 도메인 또는 apex 도메인) 가 이미 다른 Amazon 배포에 배포되었음을 의미합니다. CloudFront 오류의 원인을 진단하려면 다음 단계를 수행하십시오.

1. Amazon CloudFront 콘솔에 로그인하여 이 도메인을 다른 배포에 배포하지 않았는지 확인합니다. 한 번에 하나의 CloudFront 배포에 단일 CNAME 레코드를 첨부할 수 있습니다.
2. 이전에 도메인을 배포에 CloudFront 배포한 경우 해당 도메인을 제거해야 합니다.
   a. 왼쪽 탐색 창에서 배포를 선택합니다.
   b. 편집할 배포판 이름을 선택합니다.

c. 일반 탭을 선택합니다. 설정 섹션에서 편집을 선택합니다.

d. 대체 도메인 이름(CNAME)에서 도메인 이름을 제거합니다. 그런 다음 변경 사항 저장을 선택합니다.

3. 이 도메인이 사용자가 소유하는 다른 Amplify 앱에 연결되어 있는지 확인하십시오. 그렇다면 호스트 이름 중 하나를 재사용하려고 하지 마십시오. www.example.com을 다른 앱에 사용하는 경우, 현재 연결 중인 앱에서는 www.example.com을 사용할 수 없습니다. blog.example.com과 같은 다른 하위 도메인을 사용할 수 있습니다.
4. 이 도메인이 다른 앱에 성공적으로 연결되었다가 최근 1시간 내에 삭제된 경우, 최소 1시간이 지난 후에 다시 시도하십시오. 6시간이 지난 후에도 이 예외가 계속 표시되면 문의하세요 AWS Support. 자세한 내용을 알아보려면 AWS Support 사용 설명서의 지원 사례 만들기를 참조하세요.

추가 확인 필요 오류가 발생합니다.

추가 확인 필요 오류가 발생하는 경우, 이는 AWS Certificate Manager (ACM) 에서 이 인증서 요청을 처리하기 위해 추가 정보가 필요함을 의미합니다. 이는 예를 들어 도메인이 Alexa Top 1000 웹 사이트 순위에 든 경우, 사기 방지 조치로 이루어질 수 있습니다. 필요한 정보를 제공하려면 지원 센터를 사용하여 AWS Support에 문의하십시오. 지원 계획이 없는 경우, ACM 토론 포럼에서 새 스레드를 게시할 수 있습니다.

> **Note**
>
> amazonaws.com, cloudfront.net 또는 elasticbeanstalk.com으로 끝나는 이름과 같이 Amazon 소유 도메인 이름에 대한 인증서를 요청할 수 없습니다.

URL에 404 오류가 나타납니다. CloudFront

트래픽을 처리하기 위해 Amplify 호스팅은 CNAME 레코드를 통해 CloudFront URL을 가리킵니다. 앱을 사용자 지정 도메인에 연결하는 과정에서 Amplify 콘솔은 앱의 CloudFront URL을 표시합니다. 하지만 이 CloudFront URL을 사용하여 애플리케이션에 직접 액세스할 수는 없습니다. 404 오류가 반환됩니다. 애플리케이션은 Amplify 앱 URL(예: `https://main.d5udybEXAMPLE.amplifyapp.com`)또는 사용자 지정 도메인(예 `www.example.com`)을 사용해서만 리졸빙됩니다.

Amplify는 요청을 올바른 배포된 브랜치로 라우팅해야 하며 호스트 이름을 사용하여 이 작업을 수행합니다. 예를 들어 앱의 기본라인 브랜치를 가리키는 도메인 `www.example.com`을 구성할 수 있지만 동일한 앱의 dev 브랜치를 가리키도록 `dev.example.com`을 구성할 수도 있습니다. 따라서 Amplify가

요청을 적절하게 라우팅할 수 있도록 구성된 하위 도메인을 기반으로 애플리케이션을 방문해야 합니다.

내 도메인을 방문할 때 SSL 인증서 또는 HTTPS 오류가 발생합니다.

타사 DNS 공급자와 함께 CAA (인증 기관 권한 부여) DNS 레코드를 구성한 경우, ACM AWS Certificate Manager (ACM) 이 사용자 지정 도메인 SSL 인증서에 대한 중간 인증서를 업데이트하거나 재발급하지 못할 수 있습니다. 이 문제를 해결하려면 Amazon 인증 기관 도메인 중 하나 이상을 신뢰하는 CAA 레코드를 추가해야 합니다. 다음 절차는 수행해야 하는 단계를 설명합니다.

Amazon 인증 기관을 신뢰할 수 있는 CAA 레코드를 추가하려면

1. Amazon 인증 기관 도메인 중 하나 이상을 신뢰하도록 도메인 공급자와 함께 CAA 레코드를 구성하십시오. CAA 레코드 구성에 대한 자세한 내용은AWS Certificate Manager 사용 설명서의 CAA(인증 기관 승인) 문제를 참조하십시오.
2. 다음 방법 중 하나를 사용하여 SSL 인증서를 업데이트합니다.
   - Amplify 콘솔을 사용하여 수동으로 업데이트합니다.

     > **Note**
     >
     > 이렇게 하면 사용자 지정 도메인이 다운될 수 있습니다.

     a. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
     b. CAA 레코드를 추가할 앱을 선택합니다.
     c. 탐색 창에서 앱 설정, 도메인 관리를 선택합니다.
     d. 도메인 관리 페이지에서 커스텀 도메인을 삭제합니다.
     e. 앱을 사용자 지정 도메인에 다시 연결합니다. 이 프로세스는 새 SSL 인증서를 발급하며, 이제 ACM에서 해당 중간 인증서를 관리할 수 있습니다.

        앱을 사용자 지정 도메인에 다시 연결하려면 사용 중인 도메인 공급자에 해당하는 다음 절차 중 하나를 사용하십시오.

        - Amazon Route 53에서 관리되는 사용자 지정 도메인 추가.
        - 타사 DNS 공급자가 관리하는 사용자 지정 도메인 추가.
        - 에서 관리하는 도메인의 DNS 레코드 업데이트 GoDaddy.
        - Google 도메인에서 관리하는 도메인의 DNS 레코드 업데이트.

- SSL 인증서를 AWS Support 재발급받으려면 문의하십시오.

빌드 설정 구성

Amplify Hosting으로 앱을 배포하면 리포지토리의 `package.json` 파일을 검사하여 프런트엔드 프레임워크 및 관련 빌드 설정을 자동으로 탐지합니다. 앱의 빌드 설정을 저장하는 옵션은 다음과 같습니다.

- Amplify 콘솔에 빌드 설정 저장 - Amplify 콘솔은 빌드 설정을 자동 감지하여 Amplify 콘솔을 통해 액세스할 수 있도록 저장합니다. Amplify는 리포지토리에 저장된 `amplify.yml` 파일이 없는 한 모든 브랜치에 이러한 설정을 적용합니다.
- 리포지토리에 빌드 설정 저장 - `amplify.yml` 파일을 다운로드하여 리포지토리의 루트에 추가합니다.

Amplify 콘솔에서 호스팅을 선택한 다음 탐색 창에서 빌드 설정을 선택하여 앱의 빌드 설정을 편집할 수 있습니다. 이러한 빌드 설정은 리포지토리에 `amplify.yml` 파일이 저장된 브랜치를 제외하고 앱의 모든 브랜치에 적용됩니다.

> **Note**
>
> 빌드 설정은 앱이 지속적 배포를 위해 설정되고 git 리포지토리에 연결된 경우에만 Amplify 콘솔의 호스팅 메뉴에 표시됩니다. 이러한 유형의 배포에 대한 지침은 시작하기를 참조하십시오.

빌드 사양 명령 및 설정

빌드 사양 YAML에는 Amplify에서 빌드를 실행하는 데 사용할 빌드 명령 및 관련 설정 모음이 포함되어 있습니다. 다음 목록은 이러한 설정과 사용 방법을 설명합니다.

version

Amplify YAML 버전 번호입니다.

appRoot

이 애플리케이션이 있는 리포지토리 내 경로입니다. 여러 개의 애플리케이션이 정의되어 있지 않으면 무시됩니다.

env

이 섹션에 환경 변수를 추가합니다. 콘솔을 사용하여 환경 변수를 추가할 수도 있습니다.

백엔드

Amplify CLI 명령을 실행하여 백엔드 프로비저닝, Lambda 함수 업데이트 또는 GraphQL 스키마를 연속 배포의 일환으로 수행합니다.

프런트엔드

프런트엔드 빌드 명령을 실행합니다.

테스트

테스트 단계에서 명령을 실행합니다. 앱에 테스트를 추가하는 방법에 대해 알아보십시오.

빌드 단계

프런트엔드와 백엔드, 테스트에는 빌드의 각 시퀀스 동안 실행되는 명령을 나타내는 세 가지 단계가 있습니다.

- preBuild - preBuild 스크립트는 실제 빌드가 시작되기 전에 실행되지만 Amplify가 종속성을 설치한 후에 실행됩니다.
- build - 사용자의 빌드 명령입니다.
- postBuild - 사후 빌드 스크립트는 빌드가 종료되고 Amplify가 필요한 모든 결과물을 출력 디렉터리에 복사한 후 실행됩니다.

buildpath

빌드를 실행하는 데 사용할 경로입니다. Amplify는 이 경로를 사용하여 빌드 아티팩트를 찾습니다. 경로를 지정하지 않으면 Amplify는 모노레포 앱 루트를 사용합니다(예: `apps/app`).

artifacts>base-directory

빌드 아티팩트가 있는 디렉터리입니다.

artifacts>files

배포하려는 아티팩트의 파일을 지정합니다. 모든 파일을 포함하려면 `**/*`를 입력합니다.

cache

buildspec의 캐시 필드는 node_modules 폴더와 같은 빌드 시간 종속성을 캐시하는 데 사용되며, 고객 앱이 내장된 패키지 관리자 및 프레임워크를 기반으로 자동으로 제안됩니다. 첫 번째 빌드에서는 여기에 있는 모든 경로가 캐시되며, 이후 빌드에서는 캐시를 다시 확장하고 캐시된 종속성을 최대한 활용하여 빌드 시간을 단축합니다.

다음의 빌드 사양 예제는 기본 YAML 구문을 나타냅니다.

빌드 사양 YAML 구문

```
version: 1
env:
  variables:
    key: value
backend:
  phases:
    preBuild:
      commands:
        - *enter command*
    build:
      commands:
        - *enter command*
    postBuild:
        commands:
        - *enter command*
frontend:
  buildpath:
  phases:
    preBuild:
      commands:
        - cd react-app
        - npm ci
    build:
      commands:
        - npm run build
  artifacts:
    files:
        - location
        - location
    discard-paths: yes
    baseDirectory: location
  cache:
    paths:
        - path
        - path
test:
  phases:
    preTest:
      commands:
        - *enter command*
    test:
```

```
      commands:
        - *enter command*
    postTest:
      commands:
        - *enter command*
  artifacts:
    files:
        - location
        - location
    configFilePath: *location*
    baseDirectory: *location*
```

브랜치별 빌드 설정

배시 쉘 스크립팅을 사용하여 브랜치별 빌드 설정을 지정할 수 있습니다. 예를 들어 다음 스크립트는 시스템 환경 변수 $AWS_BRANCH를 사용하여 브랜치 이름이 main인 경우 한 세트의 명령을 실행하고, 브랜치 이름이 dev인 경우 다른 세트의 명령을 실행합니다.

```
frontend:
  phases:
    build:
      commands:
        - if [ "${AWS_BRANCH}" = "main" ]; then echo "main branch"; fi
        - if [ "${AWS_BRANCH}" = "dev" ]; then echo "dev branch"; fi
```

하위 폴더로 이동

모노레포의 경우 사용자는 빌드를 실행하기 위해 폴더로 연속적으로 cd할 수 있기를 원합니다. cd 명령을 실행한 후에는 빌드의 모든 스테이지에 적용되므로 별도의 단계에서 명령을 반복하지 않아도 됩니다.

```
version: 1
env:
  variables:
    key: value
frontend:
  phases:
    preBuild:
      commands:
```

```
        - cd react-app
        - npm ci
    build:
      commands:
        - npm run build
```

1세대 앱용 프런트 엔드를 사용한 백엔드 배포

> **Note**
>
> 이 섹션은 Amplify 1세대 애플리케이션에만 적용됩니다. 1세대 백엔드는 Amplify 스튜디오와 Amplify 명령줄 인터페이스 (CLI) 를 사용하여 생성됩니다.

`amplifyPush` 명령은 백엔드 배포에 도움을 제공하는 도우미 스크립트입니다. 아래의 빌드 설정은 현재 브랜치에 대해 배포할 올바른 백엔드 환경을 자동으로 결정합니다.

```
version: 1
env:
  variables:
    key: value
backend:
  phases:
    build:
      commands:
        - amplifyPush --simple
```

출력 폴더 설정

다음 빌드 설정에서는 출력 디렉터리를 퍼블릭 폴더로 설정합니다.

```
frontend:
  phases:
    commands:
      build:
        - yarn run build
  artifacts:
    baseDirectory: public
```

빌드의 일부로 패키지 설치

빌드하는 동안 npm 또는 yarn 명령을 사용하여 패키지를 설치할 수 있습니다.

```
frontend:
  phases:
    build:
      commands:
        - npm install -g <package>
        - <package> deploy
        - yarn run build
  artifacts:
    baseDirectory: public
```

프라이빗 npm 레지스트리 사용

빌드 설정에서 프라이빗 레지스트리에 대한 참조를 추가하거나 환경 변수로 추가할 수 있습니다.

```
build:
  phases:
    preBuild:
      commands:
        - npm config set <key> <value>
        - npm config set registry https://registry.npmjs.org
        - npm config set always-auth true
        - npm config set email hello@amplifyapp.com
        - yarn install
```

OS 패키지 설치

Amplify의 AL2023 이미지는 권한이 없는 사용자라는 이름으로 코드를 실행합니다. amplify Amplify는 이 사용자에게 Linux sudo 명령을 사용하여 OS 명령을 실행할 수 있는 권한을 부여합니다. 누락된 종속성을 위한 OS 패키지를 설치하려는 경우 yum 및 with와 rpm 같은 명령을 사용할 수 있습니다. sudo

다음 예제 빌드 섹션에서는 명령을 사용하여 OS 패키지를 설치하는 구문을 보여줍니다. sudo

```
build:
  phases:
    preBuild:
```

```
      commands:
        - sudo yum install -y <package>
```

모든 빌드에 대한 키-값 스토리지

envCache은(는) 빌드 시 키-값 스토리지를 제공합니다 envCache에 저장된 값은 빌드 중에만 수정할 수 있으며 다음 빌드에서 재사용할 수 있습니다. envCache을(를) 사용하여 배포된 환경에 정보를 저장하고 연속 빌드에서 빌드 컨테이너에 사용할 수 있습니다. envCache에 저장된 값과 달리, 빌드 중 환경 변수의 변경 사항은 미래 빌드에 지속되지 않습니다.

사용 예:

```
envCache --set <key> <value>
envCache --get <key>
```

커밋에서 빌드 건너뛰기

특정 커밋에서 자동 빌드를 건너뛰려면 커밋 메시지 끝에 [skip-cd] 텍스트를 포함합니다.

자동 빌드 비활성화

모든 코드 커밋에 대해 자동 빌드를 비활성화도록 Amplify를 구성할 수 있습니다. 설정하려면 앱 설정, Branch 설정을 선택한 다음 연결된 브랜치가 나열된 Branch 섹션을 찾으십시오. 브랜치를 선택한 다음 작업, 자동 빌드 비활성화를 선택합니다. 해당 브랜치를 새로 커밋해도 더 이상 새 빌드가 시작되지 않습니다.

diff 기반 프런트엔드 빌드 및 배포 활성화 또는 비활성화

diff 기반 프런트엔드 빌드를 사용하도록 Amplify를 구성할 수 있습니다. 활성화 시 각 빌드를 시작할 때 Amplify가 기본적으로 사용자의 appRoot 또는 /src/ 폴더에서 diff 실행을 시도합니다. Amplify가 차이점을 발견하지 못하면 프런트엔드 빌드, 테스트(구성된 경우) 및 배포 단계를 건너뛰고 호스팅된 앱을 업데이트하지 않습니다.

diff 기반 프런트엔드 빌드 및 배포를 구성하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. diff 기반 프런트엔드 빌드를 구성하고 배포할 앱을 선택합니다.

3. 탐색 창에서 호스팅, 환경 변수를 선택합니다.
4. 환경 변수 섹션에서 변수 관리를 선택합니다.
5. 환경 변수를 구성하는 절차는 diff 기반 프런트엔드 빌드 및 배포의 활성화 여부에 따라 달라집니다.
   - diff 기반 프런트엔드 빌드 및 배포를 활성화하려면
     a. 변수 관리 섹션의 변수에 AMPLIFY_DIFF_DEPLOY를 입력합니다.
     b. 값에 true를 입력합니다.
   - diff 기반 프런트엔드 빌드 및 배포를 비활성화하려면
     - 다음 중 하나를 수행하십시오.
       - 변수 관리 섹션에서 AMPLIFY_DIFF_DEPLOY을(를) 찾습니다. 값에 false를 입력합니다.
       - AMPLIFY_DIFF_DEPLOY 환경 변수를 제거합니다.
6. 저장을 선택합니다.

선택적으로 AMPLIFY_DIFF_DEPLOY_ROOT 환경 변수를 설정하여 기본 경로를 리포지토리의 루트와 관련된 경로(예: dist)로 재정의할 수 있습니다.

1세대 앱의 diff 기반 백엔드 빌드를 활성화 또는 비활성화합니다.

> **Note**
>
> 이 섹션은 Amplify 1세대 애플리케이션에만 적용됩니다. 1세대 백엔드는 Amplify 스튜디오와 Amplify 명령줄 인터페이스 (CLI) 를 사용하여 생성됩니다.

AMPLIFY_DIFF_BACKEND 환경 변수를 사용하여 diff 기반 백엔드 빌드를 사용하도록 Amplify Hosting을 구성할 수 있습니다. diff 기반 백엔드 빌드를 활성화하면 각 빌드를 시작할 때 Amplify가 리포지토리의 amplify 폴더에서 diff 실행을 시도합니다. Amplify에서 차이점을 발견하지 못하면 백엔드 빌드 단계를 건너뛰고 백엔드 리소스를 업데이트하지 않습니다. 프로젝트의 리포지토리에 amplify 폴더가 없는 경우 Amplify는 AMPLIFY_DIFF_BACKEND 환경 변수 값을 무시합니다.

현재 백엔드 단계의 빌드 설정에 사용자 지정 명령이 지정되어 있는 경우, 조건부 백엔드 빌드는 작동하지 않습니다. 이러한 사용자 지정 명령을 실행하려면 앱의 amplify.yml 파일에 있는 빌드 설정의 프런트엔드 단계로 해당 명령을 이동해야 합니다.

diff 기반 백엔드 빌드를 구성하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. diff 기반 백엔드 빌드를 구성할 앱을 선택합니다.
3. 탐색 창에서 호스팅, 환경 변수를 선택합니다.
4. 환경 변수 섹션에서 변수 관리를 선택합니다.
5. 환경 변수를 구성하는 절차는 diff 기반 백엔드 빌드의 활성화 여부에 따라 달라집니다.
   - diff 기반 백엔드 빌드를 활성화하려면
     a. 변수 관리 섹션의 변수에 `AMPLIFY_DIFF_BACKEND`를 입력합니다.
     b. 값에 `true`를 입력합니다.
   - diff 기반 백엔드 빌드를 비활성화하려면
     - 다음 중 하나를 수행하십시오.
       - 변수 관리 섹션에서 `AMPLIFY_DIFF_BACKEND`을(를) 찾습니다. 값에 `false`를 입력합니다.
       - `AMPLIFY_DIFF_BACKEND` 환경 변수를 제거합니다.
6. 저장을 선택합니다.

모노레포 빌드 설정

단일 리포지토리에 여러 프로젝트 또는 마이크로서비스를 저장하는 것을 모노레포라고 합니다. Amplify Hosting을 사용하면 여러 빌드 구성 또는 브랜치 구성을 만들지 않고도 애플리케이션을 모노레포로 배포할 수 있습니다.

Amplify는 일반 모노레포 앱뿐만 아니라 npm 워크스페이스, pnpm 워크스페이스, Yarn 워크스페이스, Nx 및 Turborepo를 사용하여 생성된 모노레포 앱을 지원합니다. 앱 배포 시 Amplify는 사용 중인 모노레포 빌드 도구를 자동으로 감지합니다. Amplify는 npm 워크스페이스, Yarn 워크스페이스 또는 Nx의 앱에 대한 빌드 설정을 자동으로 적용합니다. Turborepo와 pnpm 앱에는 추가 구성이 필요합니다. 자세한 정보는 Turborepo 및 pnpm 모노레포 앱 구성을 참조하세요.

Amplify 콘솔에서 모노레포에 대한 빌드 설정을 저장하거나 `amplify.yml` 파일을 다운로드하여 리포지토리의 루트에 추가할 수 있습니다. Amplify는 리포지토리에서 `amplify.yml` 파일을 찾지 않는 한, 콘솔에 저장된 설정을 모든 브랜치에 적용합니다. `amplify.yml` 파일이 있는 경우 해당 설정은 Amplify 콘솔에 저장된 모든 빌드 설정을 재정의합니다.

모노레포 빌드 사양 YAML 구문

모노레포 빌드 사양의 YAML 구문은 단일 애플리케이션이 포함된 리포지토리의 YAML 구문과 다릅니다. 모노레포의 경우 애플리케이션 목록에서 각 프로젝트를 선언합니다. 모노레포 빌드 사양에 선언하는 각 애플리케이션에 대해 다음과 같은 추가 appRoot 키를 제공해야 합니다.

appRoot

애플리케이션이 시작되는 리포지토리 내의 루트입니다. 이 키는 반드시 존재해야 하며 AMPLIFY_MONOREPO_APP_ROOT 환경 변수와 동일한 값을 가져야 합니다. 이 환경 변수 설정에 대한 지침은 AMPLIFY_MONOREPO_APP_ROOT 환경 변수 설정 섹션을 참조하십시오.

다음 모노레포 빌드 사양 예제는 동일한 리포지토리에서 여러 Amplify 애플리케이션을 선언하는 방법을 설명합니다. 두 앱 react-app, angular-app은 applications 목록에 선언되어 있습니다. 각 앱의 appRoot 키는 앱이 리포지토리의 apps 루트 폴더에 있음을 나타냅니다.

buildpath 속성은 모노레포 프로젝트 루트에서 앱을 실행하고 빌드하도록 /로 설정되어 있습니다.

모노레포 빌드 사양 YAML 구문

```
version: 1
applications:
  - appRoot: apps/react-app
    env:
      variables:
        key: value
    backend:
      phases:
        preBuild:
          commands:
            - *enter command*
        build:
          commands:
            - *enter command*
        postBuild:
            commands:
            - *enter command*
    frontend:
      buildPath: / # Run install and build from the monorepo project root
      phases:
        preBuild:
          commands:
```

```
            - *enter command*
            - *enter command*
        build:
          commands:
            - *enter command*
      artifacts:
        files:
            - location
            - location
        discard-paths: yes
        baseDirectory: location
      cache:
        paths:
            - path
            - path
    test:
      phases:
        preTest:
          commands:
            - *enter command*
        test:
          commands:
            - *enter command*
        postTest:
          commands:
            - *enter command*
      artifacts:
        files:
            - location
            - location
        configFilePath: *location*
        baseDirectory: *location*
  - appRoot: apps/angular-app
    env:
      variables:
        key: value
    backend:
      phases:
        preBuild:
          commands:
            - *enter command*
        build:
          commands:
            - *enter command*
```

```
        postBuild:
            commands:
            - *enter command*
    frontend:
      phases:
        preBuild:
          commands:
            - *enter command*
            - *enter command*
        build:
          commands:
            - *enter command*
      artifacts:
        files:
            - location
            - location
        discard-paths: yes
        baseDirectory: location
      cache:
        paths:
            - path
            - path
    test:
      phases:
        preTest:
          commands:
            - *enter command*
        test:
          commands:
            - *enter command*
        postTest:
          commands:
            - *enter command*
      artifacts:
        files:
            - location
            - location
        configFilePath: *location*
        baseDirectory: *location*
```

AMPLIFY_MONOREPO_APP_ROOT 환경 변수 설정

모노레포에 저장된 앱을 배포하는 경우, 앱의 AMPLIFY_MONOREPO_APP_ROOT 환경 변수는 리포지토리의 루트를 기준으로 앱 루트 경로와 동일한 값을 가져야 합니다. 예를 들어, 이름이 apps으로 지정된 루트 폴더가 있고 app1, app2, app3을 포함하는 ExampleMonorepo라는 이름의 모노레포는 다음 디렉터리 구조를 가집니다.

```
ExampleMonorepo
  apps
    app1
    app2
    app3
```

이 예제에서 app1에 대한 AMPLIFY_MONOREPO_APP_ROOT 환경 변수의 값은 apps/app1입니다.

Amplify 콘솔을 사용하여 모노레포 앱을 배포하면 콘솔은 앱의 루트 경로에 지정한 값을 사용하여 AMPLIFY_MONOREPO_APP_ROOT 환경 변수를 자동으로 설정합니다. 그러나 monorepo 앱이 이미 Amplify에 존재하거나 를 사용하여 AWS CloudFormation배포된 경우 Amplify 콘솔의 AMPLIFY_MONOREPO_APP_ROOT 환경 변수 섹션에서 환경 변수를 수동으로 설정해야 합니다.

배포 중 AMPLIFY_MONOREPO_APP_ROOT 환경 변수 자동 설정

다음 지침은 Amplify 콘솔을 사용하여 모노레포 앱을 배포하는 방법을 설명합니다. Amplify는 콘솔에 지정한 앱의 루트 폴더를 사용하여 AMPLIFY_MONOREPO_APP_ROOT 환경 변수를 자동으로 설정합니다.

Amplify 콘솔을 사용하여 모노레포 앱을 배포하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 오른쪽 상단에서 새 앱 만들기를 선택합니다.
3. Amplify로 빌드 시작 페이지에서 Git 공급자를 선택한 후 다음을 선택합니다.
4. 리포지토리 브랜치 추가 페이지에서 다음을 수행합니다.
   a. 목록에서 리포지토리 이름을 선택합니다.
   b. 사용할 브랜치 이름을 선택합니다.
   c. '내 앱은 모노레포입니다. '를 선택합니다.
   d. 모노레포에 앱 경로를 입력합니다(예: **apps/app1**).
   e. 다음을 선택합니다.

5. 앱 설정 페이지에서 기본 설정을 사용하거나 앱의 빌드 설정을 사용자 지정할 수 있습니다. 환경 변수 섹션에서 Amplify는 AMPLIFY_MONOREPO_APP_ROOT 4d단계에서 지정한 경로를 설정합니다.
6. 다음을 선택합니다.
7. 검토 페이지에서 저장 및 배포를 선택합니다.

기존 앱에 AMPLIFY_MONOREPO_APP_ROOT 환경 변수 설정

다음 지침에 따라 Amplify에 이미 배포되었거나 를 사용하여 만든 앱의 AMPLIFY_MONOREPO_APP_ROOT 환경 변수를 수동으로 설정하십시오. CloudFormation

기존 앱에 AMPLIFY_MONOREPO_APP_ROOT 환경 변수를 설정하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 환경 변수를 설정할 앱 이름을 선택합니다.
3. 탐색 창에서 호스팅을 선택한 다음 환경 변수를 선택합니다.
4. 환경 변수 페이지에서 변수 관리를 선택합니다.
5. 변수 관리 섹션에서 다음을 수행합니다.
   a. 새로 추가를 선택합니다.
   b. 변수에 키 AMPLIFY_MONOREPO_APP_ROOT을(를) 입력합니다.
   c. 값에는 앱 경로를 입력합니다(예: **apps/app1**).
   d. 브랜치의 경우 Amplify가 기본적으로 환경 변수를 모든 브랜치에 적용합니다.
6. 저장을 선택합니다.

Turborepo 및 pnpm 모노레포 앱 구성

Turborepo와 pnpm 워크스페이스 모노레포 빌드 도구는 `.npmrc` 파일에서 구성 정보를 가져옵니다. 이러한 도구 중 하나로 만든 모노레포 앱을 배포할 때는 프로젝트 루트 디렉터리에 `.npmrc` 파일이 있어야 합니다.

`.npmrc` 파일에서 Node 패키지 설치를 위한 링커를 `hoisted`로 설정합니다. 파일에 다음 줄을 복사할 수 있습니다.

```
node-linker=hoisted
```

`.npmrc` 파일 및 설정에 대한 자세한 내용은 pnpm 설명서의 pnpm .npmrc를 참조하십시오.

Pnpm은 Amplify 기본 빌드 컨테이너에 포함되지 않습니다. pnpm 워크스페이스 및 Turborepo 앱의 경우 앱의 빌드 설정 `preBuild` 단계에서 pnpm을 설치하는 명령을 추가해야 합니다.

빌드 사양에서 발췌한 다음 예시는 pnpm 설치 명령이 포함된 `preBuild` 단계를 보여줍니다.

```
version: 1
applications:
  - frontend:
      phases:
        preBuild:
          commands:
            - npm install -g pnpm
```

기능 브랜치 배포 및 팀 워크플로우

Amplify 호스팅은 기능 브랜치 및 GitFlow 워크플로와 함께 작동하도록 설계되었습니다. Amplify는 저장소에서 새 브랜치를 연결할 때마다 Git 브랜치를 사용하여 새 배포를 생성합니다. 첫 번째 브랜치를 연결한 후 추가 기능 브랜치를 생성합니다.

앱에 브랜치를 추가하려면

1. 브랜치를 추가하려는 앱을 선택합니다.
2. 앱 설정을 선택한 다음 Branch 설정을 선택합니다.
3. 브랜치 설정 페이지에서 브랜치 추가를 선택합니다.
4. 리포지토리에서 브랜치를 선택합니다.
5. 브랜치 추가를 선택합니다.
6. 앱을 재배포하세요.

브랜치를 추가하면 Amplify 기본 도메인에서 https://main.appid.amplifyapp.com 및 https://dev.appid.amplifyapp.com 과 같은 두 가지 배포를 사용할 수 있습니다. 이는 다음과 다를 수 team-to-team 있지만 일반적으로 기본 브랜치는 릴리스 코드를 추적하며 프로덕션 브랜치입니다. 개발 브랜치는 새 기능을 테스트하는 데 통합 브랜치로 사용됩니다. 이러한 방식으로 베타 테스터는 기본 브랜치 배포와 관련하여 어떠한 프로덕션 최종 사용자에게도 영향을 주지 않고, 개발 브랜치 배포와 관련하여 릴리스되지 않은 기능을 테스트할 수 있습니다.

주제

- 풀스택 Amplify 2세대 앱을 사용한 팀 워크플로
- 풀스택 Amplify 1세대 앱을 사용한 팀 워크플로
- 패턴 기반 기능 브랜치 배포
- Amplify 구성의 자동 빌드 타임 생성 (1세대 앱만 해당)
- 조건부 백엔드 빌드 (1세대 앱만 해당)
- 여러 앱에서 Amplify 백엔드 사용 (1세대 앱만 해당)

풀스택 Amplify 2세대 앱을 사용한 팀 워크플로

AWS Amplify Gen 2는 백엔드를 정의하기 TypeScript 위한 코드 우선 기반의 개발자 환경을 도입합니다. Amplify Gen 2 애플리케이션을 사용한 풀스택 워크플로에 대해 알아보려면 Amplify 문서에서 풀스택 워크플로를 참조하십시오.

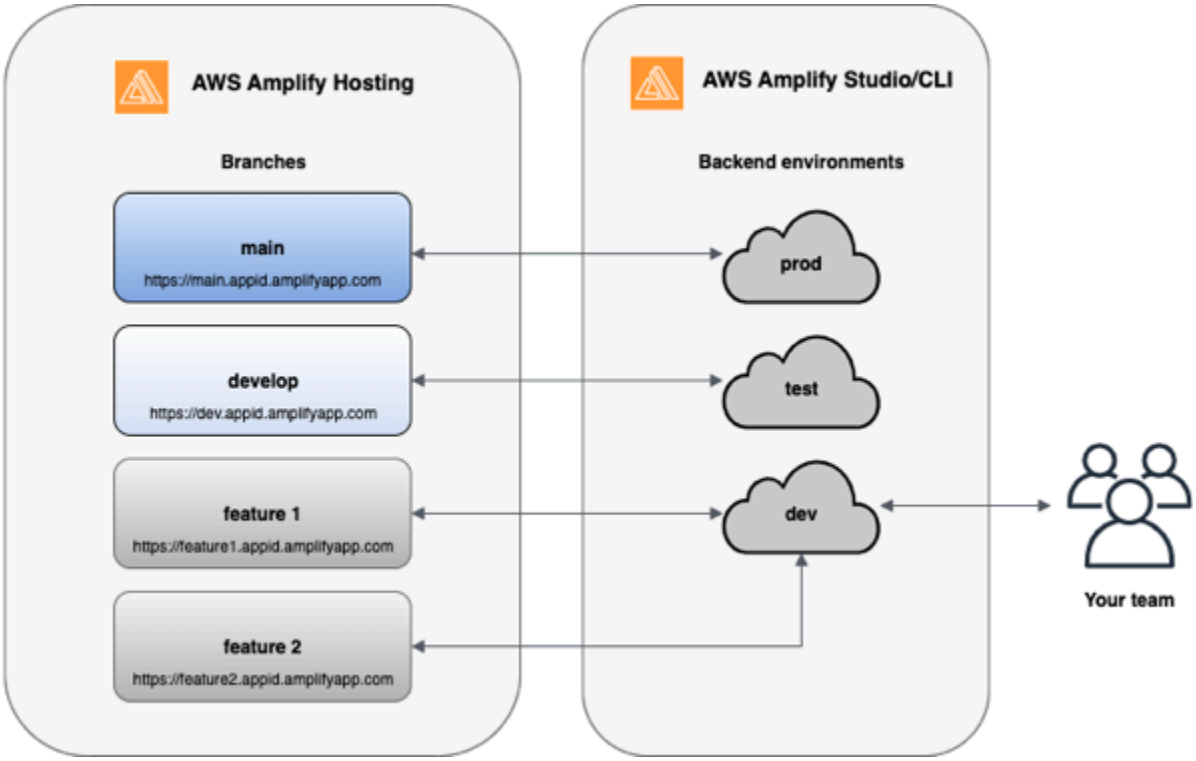
풀스택 Amplify 1세대 앱을 사용한 팀 워크플로

기능 브랜치 배포는 프런트엔드와 선택적 백엔드 환경으로 구성됩니다. 프런트엔드는 빌드된 후 글로벌 콘텐츠 배포 네트워크(CDN)에 배포되지만, 백엔드는 Amplify Studio 또는 Amplify CLI에 의해 AWS에 배포됩니다. 이 배포 시나리오를 설정하는 방법을 알아보려면 을 참조하십시오애플리케이션을 위한 백엔드 구축.

Amplify Hosting은 기능 브랜치 배포와 함께 GraphQL API 및 Lambda 함수와 같은 백엔드 리소스를 지속적으로 배포할 수 있습니다. 다음 브랜칭 모델을 사용하여 Amplify Hosting으로 백엔드 및 프런트엔드를 배포할 수 있습니다.

기능 브랜치 워크플로

- Amplify Studio 또는 Amplify CLI로 prod, 테스트 및 dev 백엔드 환경을 생성합니다.
- prod 백엔드를 기본 브랜치에 매핑하십시오.
- 테스트 백엔드를 개발 브랜치에 매핑합니다.
- 팀 구성원은 dev 백엔드 환경을 사용하여 개별 기능 브랜치를 테스트할 수 있습니다.



1. Amplify CLI를 설치하여 새 Amplify 프로젝트를 초기화합니다.

```
npm install -g @aws-amplify/cli
```

2. 프로젝트에 대해 prod 백엔드 환경을 초기화합니다. 프로젝트가 없는 경우, create-react-app 또는 Gatsby와 같은 부트스트랩 도구를 사용하여 프로젝트를 만드세요.

```
create-react-app next-unicorn
cd next-unicorn
amplify init
 ? Do you want to use an existing environment? (Y/n): n
 ? Enter a name for the environment: prod
...
amplify push
```

3. 테스트 및 dev 백엔드 환경을 추가합니다.

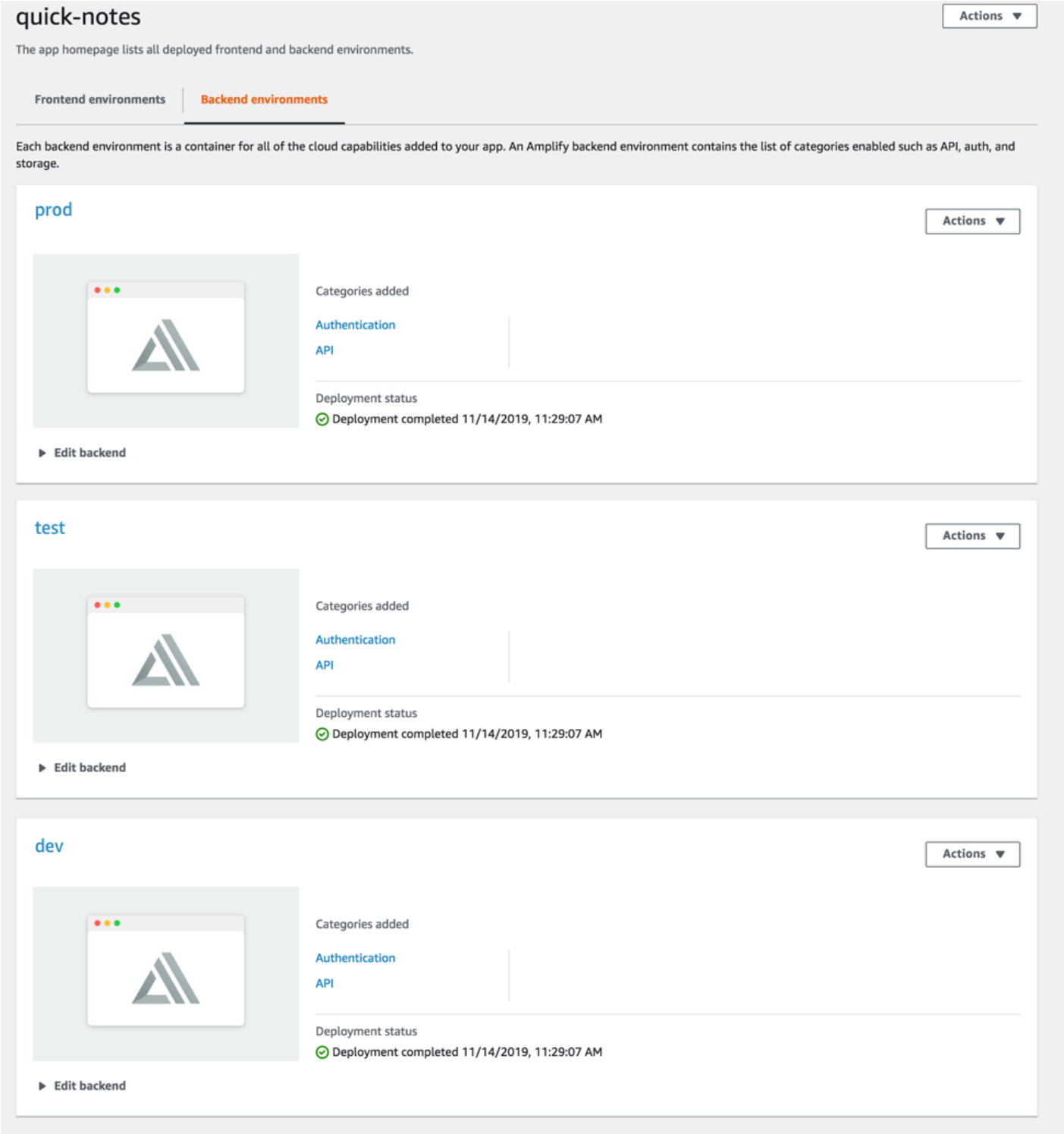
```
amplify env add
 ? Do you want to use an existing environment? (Y/n): n
 ? Enter a name for the environment: test
...
amplify push
```

```
amplify env add
 ? Do you want to use an existing environment? (Y/n): n
 ? Enter a name for the environment: dev
...
amplify push
```

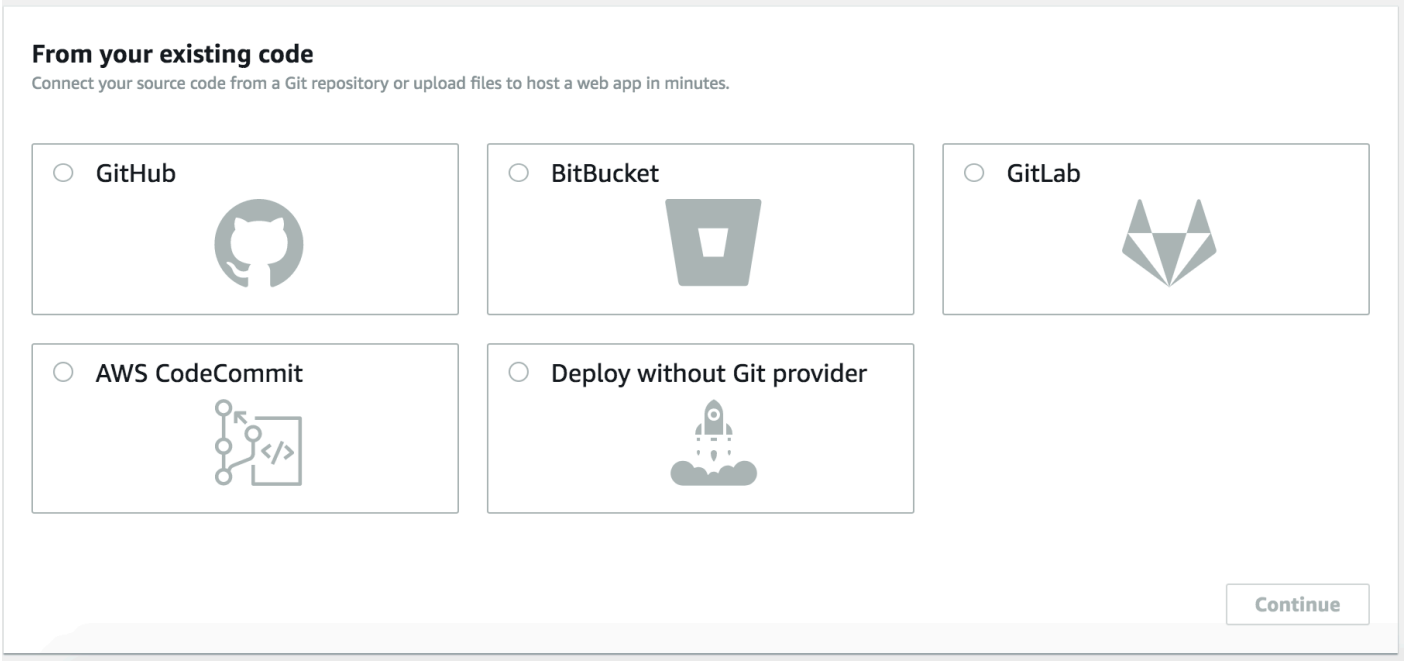
4. 선택한 Git 리포지토리로 코드를 푸시합니다(이 예에서는 사용자가 기본에 푸시한 것으로 가정함).

```
git commit -am 'Added dev, test, and prod environments'
git push origin main
```

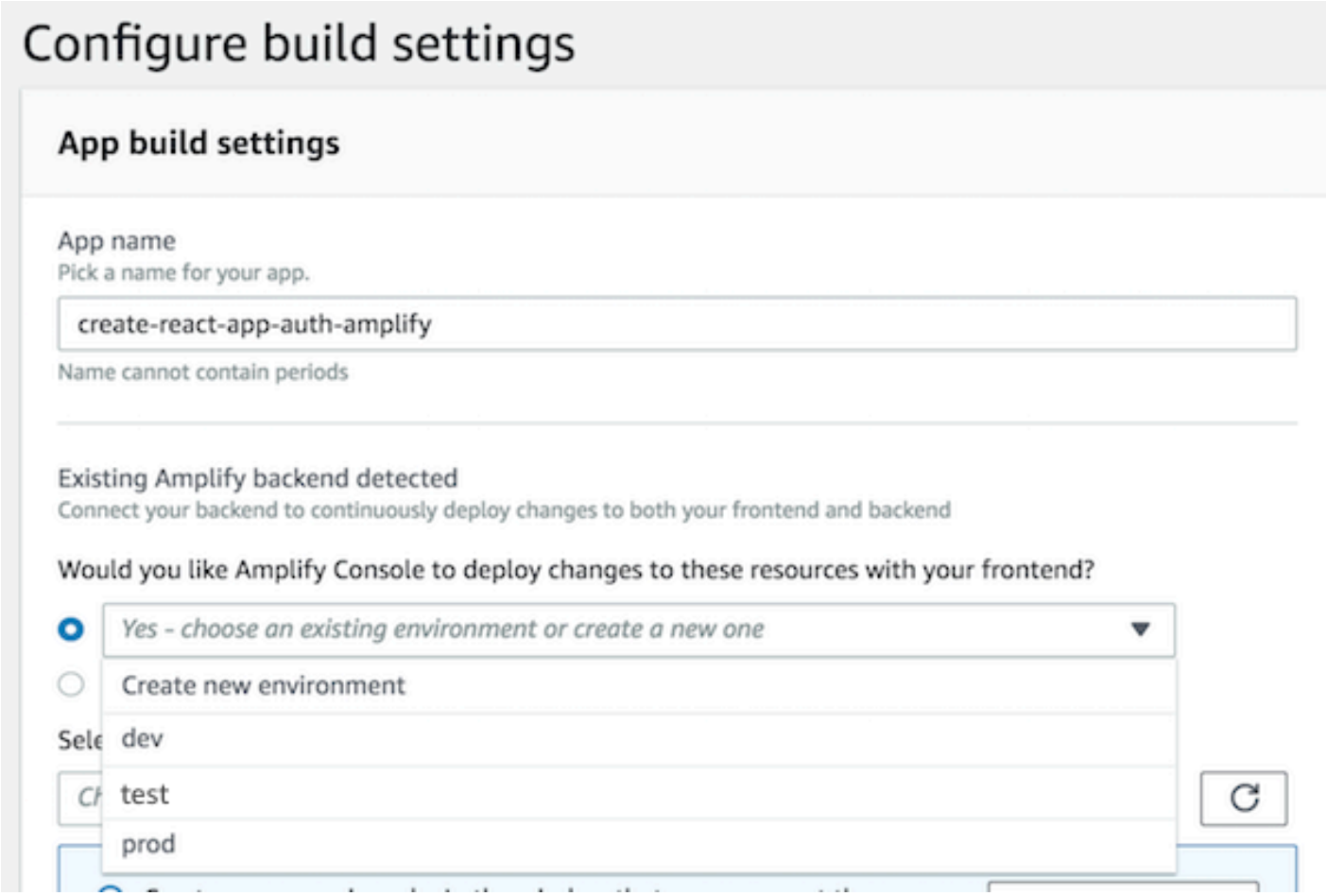
5. 현재 백엔드 환경을 AWS Management Console 보려면 Amplify를 방문하십시오. 탐색 경로에서 한 단계 위로 이동하면 백엔드 환경 탭에서 생성된 모든 백엔드 환경 목록을 볼 수 있습니다.



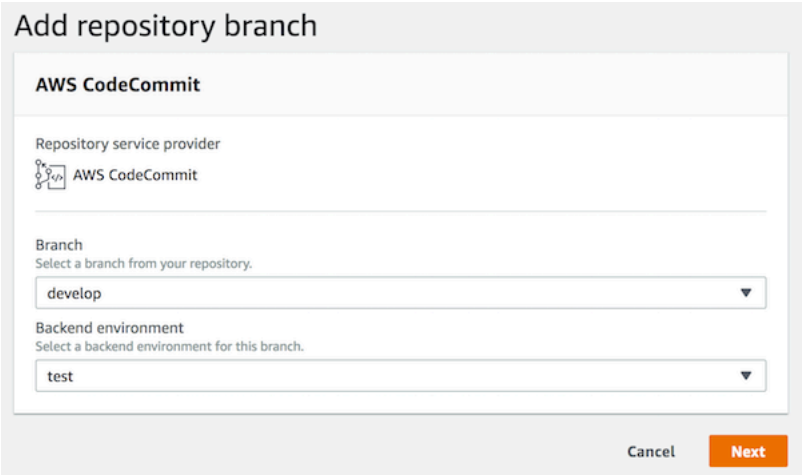
6. 프런트엔드 환경 탭으로 전환하여 리포지토리 제공자와 기본 브랜치를 연결하십시오.



7. 빌드 설정 화면에서 기존 백엔드 환경을 선택하여 메인 브랜치를 통한 지속적 배포를 설정합니다. 드롭다운에서 prod를 선택하고 Amplify에 서비스 역할을 부여합니다. 저장 및 배포를 선택합니다. 빌드가 완료된 후 https://main.appid.amplifyapp.com에서 사용 가능한 기본 브랜치 배포를 받게 됩니다.



8. Amplify에서 개발 브랜치를 연결합니다(이 시점에 개발 및 기본 브랜치가 동일한 것으로 가정함). test 백엔드 환경을 선택합니다.



9. 이제 Amplify가 설정되었습니다. 기능 브랜치에서 새 기능에 대한 작업을 시작할 수 있습니다. 로컬 워크스테이션에서 dev 백엔드 환경을 사용하여 백엔드 기능을 추가합니다.

```
git checkout -b newinternet
```

```
amplify env checkout dev
amplify add api
...
amplify push
```

10. 기능에 대한 작업을 종료한 후 코드를 커밋하고 풀 요청을 생성하여 내부적으로 검토합니다.

```
git commit -am 'Decentralized internet v0.1'
git push origin newinternet
```

11. 표시될 변경 사항을 미리 보려면 Amplify 콘솔로 이동하여 기능 브랜치를 연결합니다. 참고: Amplify CLI가 아닌 시스템에 AWS CLI 설치되어 있는 경우 터미널에서 직접 브랜치를 연결할 수 있습니다. 애플리케이션 설정 > 일반 > AppARN: arn:aws:amplify:<region>:<region>:apps/<appid>으로 이동하여 appid를 찾아볼 수 있습니다.

```
aws amplify create-branch --app-id <appid> --branch-name <branchname>
aws amplify start-job --app-id <appid> --branch-name <branchname> --job-type RELEASE
```

12. https://newinternet.appid.amplifyapp.com에 액세스하여 기능을 팀 메이트와 공유할 수 있습니다. 모든 것이 순조로워 보이면 PR을 개발 브랜치에 병합합니다.

```
git checkout develop
git merge newinternet
git push
```

13. 이렇게 하면 https://dev.appid.amplifyapp.com에서 브랜치 배포와 함께 Amplify에서 프런트엔드와 백엔드를 업데이트할 빌드가 시작됩니다. 내부 이해관계자가 새 기능을 검토할 수 있도록 이 링크를 내부 이해관계자와 공유할 수 있습니다.

14. Git, Amplify에서 기능 브랜치를 삭제하고, 클라우드에서 백엔드 환경을 제거합니다(언제든지 'amplify env checkout prod' 및 'amplify env add'를 실행하여 새 백엔드 환경을 생성할 수 있음).

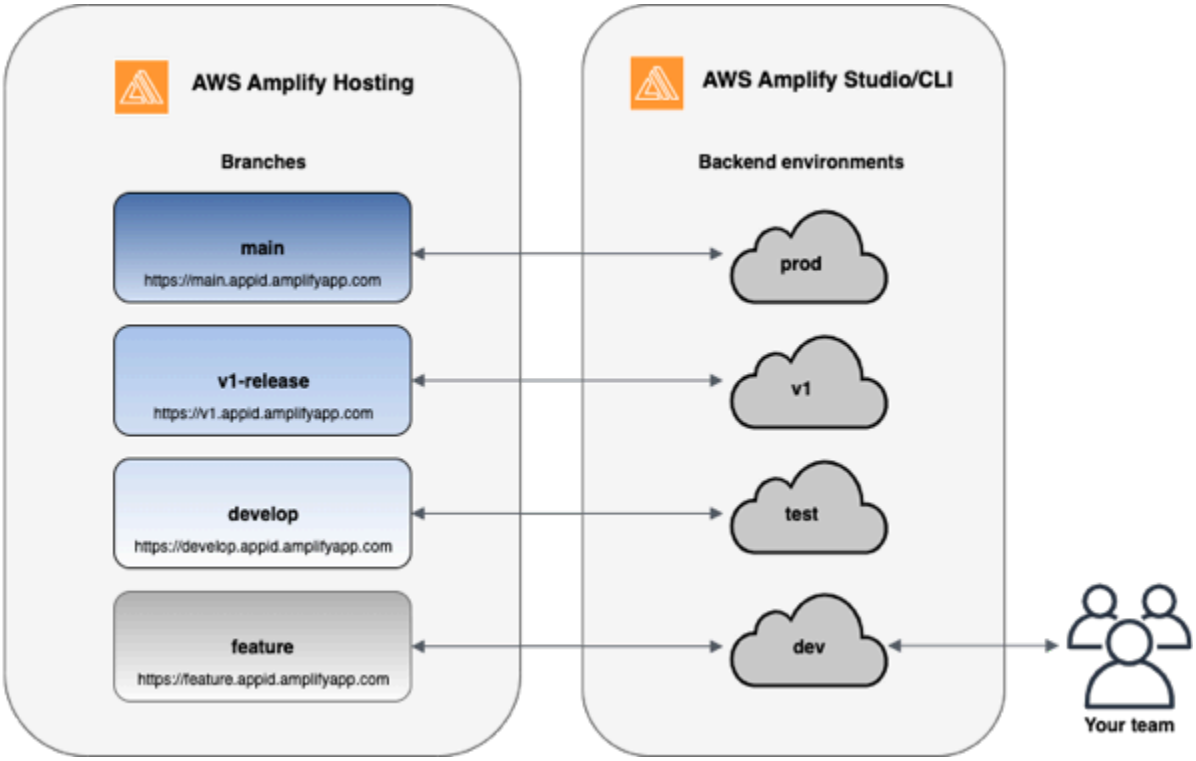
```
git push origin --delete newinternet
aws amplify delete-branch --app-id <appid> --branch-name <branchname>
amplify env remove dev
```

GitFlow 워크플로우

GitFlow 두 개의 브랜치를 사용하여 프로젝트 기록을 기록합니다. 기본 브랜치는 릴리스 코드만 추적하고 개발 브랜치는 새 기능의 통합 브랜치로 사용됩니다. GitFlow 완료된 작업에서 새 개발을 분리하여

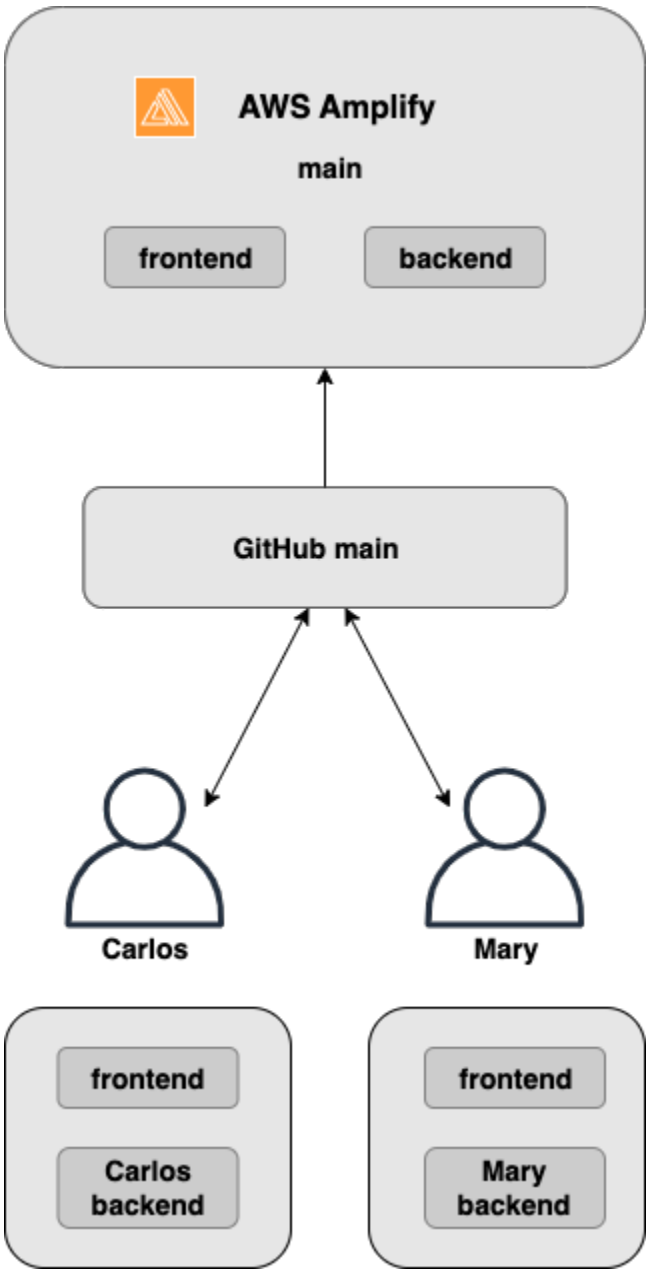
병렬 개발을 간소화합니다. 새로운 개발(예: 기능 및 비정기적인 버그 수정)은 기능 브랜치에서 수행됩니다. 개발자가 코드를 릴리스할 준비가 완료되면 기능 브랜치는 통합 개발 브랜치로 병합됩니다. 기본 브랜치에 대한 커밋만 릴리스 브랜치와 핫픽스 브랜치를 병합합니다(긴급 버그 수정).

아래 다이어그램은 권장 설정을 보여줍니다. GitFlow 위의 기능 브랜치 워크플로우 섹션에서 설명된 것과 동일한 절차를 따를 수 있습니다.



각 개발자의 샌드박스

- 팀의 각 개발자는 자신의 로컬 컴퓨터와 별도로 클라우드에 샌드박스 환경을 만듭니다 이를 통해 개발자는 다른 팀원의 변경 사항을 덮어쓰지 않고도 서로 격리되어 작업할 수 있습니다.
- Amplify 의 각 브랜치에는 자체 백엔드가 있습니다. 이렇게 하면 팀의 개발자가 직접 로컬 컴퓨터에서 프로덕션 환경으로 백엔드 또는 프런트엔드를 수동으로 푸시하지 않고 Amplify가 Git 리포지토리를 변경 사항 배포를 위한 단일 소스로 사용할 수 있습니다.



1. Amplify CLI를 설치하여 새 Amplify 프로젝트를 초기화합니다.

```
npm install -g @aws-amplify/cli
```

2. 프로젝트에 대해 mary 백엔드 환경을 초기화합니다. 프로젝트가 없다면, Gatsby와 같은 create-react-app 부트스트랩 도구를 사용하여 프로젝트를 만드세요.

```
cd next-unicorn
amplify init
 ? Do you want to use an existing environment? (Y/n): n
```

```
 ? Enter a name for the environment: mary
...
amplify push
```

3. 선택한 Git 리포지토리로 코드를 푸시합니다(이 예에서는 사용자가 기본에 푸시한 것으로 가정함).

```
git commit -am 'Added mary sandbox'
git push origin main
```

4. 리포지토리 > 기본을 Amplify에 연결합니다.
5. Amplify 콘솔은 Amplify CLI에 의해 형성된 백엔드 환경을 감지합니다. 드롭다운에서 새 환경 생성을 선택하고 Amplify에 서비스 역할을 부여합니다. 저장 및 배포를 선택합니다. 빌드가 완료된 후 https://main.appid.amplifyapp.com에서 사용 가능한 마스터 브랜치 배포를 받게 되고 새 백엔드 환경은 브랜치에 연결됩니다.
6. Amplify에서 개발 브랜치를 연결하고 (이 시점에서 개발 브랜치와 기본 브랜치가 동일하다고 가정) Create를 선택합니다.

패턴 기반 기능 브랜치 배포

배턴 기반 브랜치 배포를 사용하면 특정 패턴을 Amplify에 일치시키는 브랜치를 자동으로 배포할 수 있습니다. 릴리스에 기능 브랜치 또는 GitFlow 워크플로를 사용하는 제품 팀은 이제 'release**'와 같은 패턴을 정의하여 'release'로 시작하는 Git 브랜치를 공유 가능한 URL에 자동으로 배포할 수 있습니다. 이 블로그 게시물에서는 팀 워크플로우가 다른 이러한 기능의 사용을 설명합니다.

1. 앱 설정 > 브랜치 설정 > 편집을 선택합니다.
2. 분기 자동 감지를 선택하여 패턴 세트와 일치하는 분기를 Amplify에 자동으로 연결합니다.
3. 브랜치 자동 감지 - 패턴 상자에 브랜치를 자동으로 배포하기 위한 패턴을 입력합니다.
   - ***** – 리포지토리의 모든 브랜치를 배포합니다.
   - **`release*`**— '릴리스'라는 단어로 시작하는 모든 브랜치를 배포합니다.
   - **`release*/`** – ‘release /’ 패턴과 일치하는 모든 브랜치를 배포합니다.
   - 여러 패턴을 쉼표로 구분된 목록으로 지정합니다. 예를 들어 `release*, feature*`입니다.
4. Branch 자동 감지 액세스 제어를 선택하여 자동으로 생성되는 모든 브랜치에 대해 자동 비밀번호 보호를 설정합니다.
5. Amplify 백엔드로 구축된 1세대 애플리케이션의 경우 연결된 모든 브랜치에 대해 새 환경을 생성하거나 모든 브랜치가 기존 백엔드를 가리키도록 선택할 수 있습니다.
6. 저장을 선택합니다.

사용자 지정 도메인에 연결된 앱을 위한 패턴 기반 기능 분기 배포

Amazon Route 53 사용자 지정 도메인에 연결된 앱에 대해 패턴 기반 기능 분기 배포를 사용할 수 있습니다.

- 패턴 기반 기능 분기 배포 지침은 Amazon Route 53 사용자 지정 도메인을 위한 자동 하위 도메인을 설정합니다. 단원을 참조하십시오.
- Route 53에서 관리되는 사용자 지정 도메인에 Amplify 앱을 연결하는 방법에 대한 지침은 Amazon Route 53에서 관리되는 사용자 지정 도메인 추가 단원을 참조하십시오.
- Route 53 사용에 대한 자세한 내용은 Amazon Route 53이란을 참조하십시오.

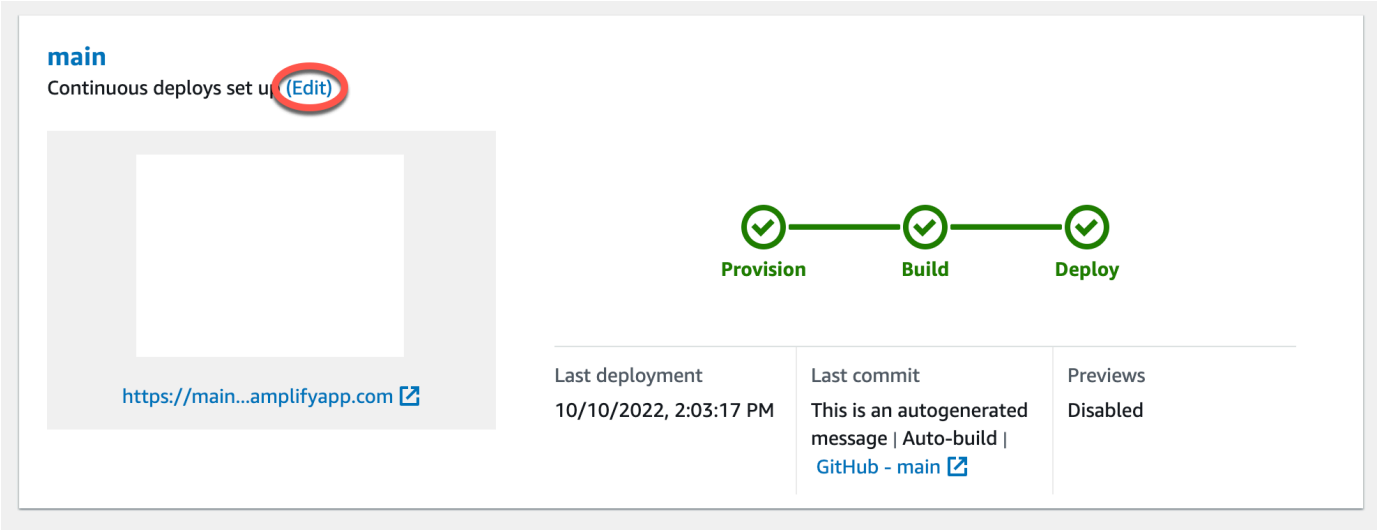
Amplify 구성의 자동 빌드 타임 생성 (1세대 앱만 해당)

> **Note**
>
> 이 섹션의 정보는 1세대 앱에만 해당됩니다. 2세대 앱의 기능 브랜치에서 변경된 인프라 및 애플리케이션 코드를 자동으로 배포하려면 Amplify 문서의 Fullstack 브랜치 배포를 참조하십시오.

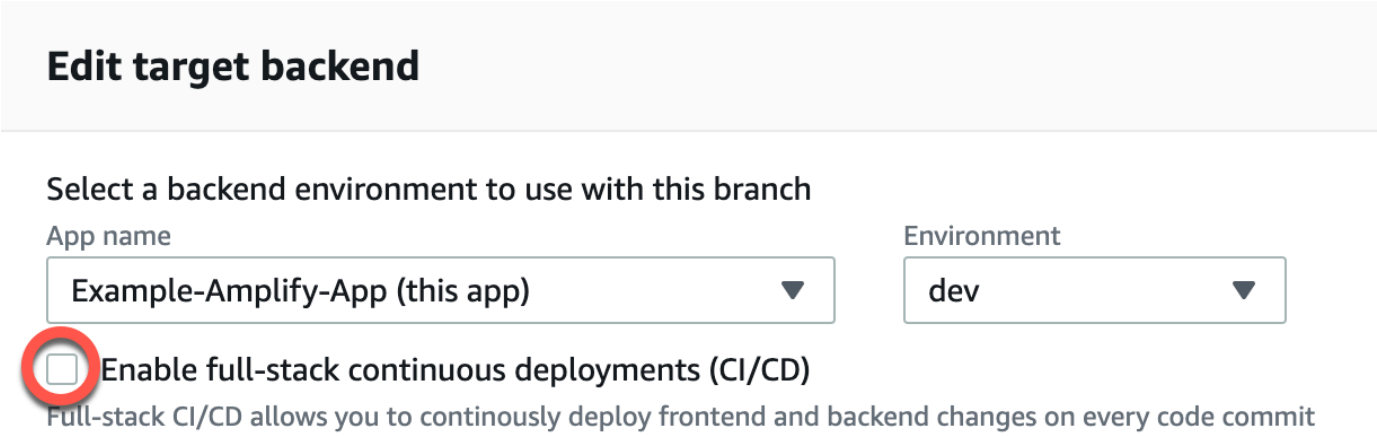
Amplify는 1세대 앱을 위한 Amplify 구성 `aws-exports.js` 파일의 자동 빌드 타임 생성을 지원합니다. 풀 스택 CI/CD 배포를 끄면 앱이 `aws-exports.js` 파일을 자동 생성하고 빌드 시 백엔드가 업데이트되지 않도록 할 수 있습니다.

빌드 시 **`aws-exports.js`**를 자동 생성하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 편집할 앱을 선택합니다.
3. 호스팅 환경 탭을 선택합니다.
4. 편집할 브랜치를 찾아 편집을 선택합니다.



5. 대상 백엔드 편집 페이지에서 풀 스택 연속 배포(CI/CD)활성화를 선택 취소하여 이 백엔드의 풀 스택 CI/CD를 끕니다.



6. 기존 서비스 역할을 선택하여 Amplify에 앱 백엔드를 변경하는 데 필요한 권한을 부여합니다. 서비스 역할을 생성해야 하는 경우, 새 역할 생성을 선택합니다. 서비스 역할 생성에 대한 자세한 내용은 서비스 역할 추가을 참조하십시오.
7. 저장을 선택합니다. Amplify는 다음에 앱을 구축할 때 이러한 변경 사항을 적용합니다.

조건부 백엔드 빌드 (1세대 앱만 해당)

> **Note**
>
> 이 섹션의 정보는 1세대 앱에만 해당됩니다. Amplify Gen 2는 코드 우선 TypeScript 기반의 개발자 경험을 제공합니다. 따라서 2세대 백엔드에는 이 기능이 필요하지 않습니다.

Amplify는 1세대 앱의 모든 브랜치에서 조건부 백엔드 빌드를 지원합니다. 조건부 백엔드 빌드를 구성하려면 `AMPLIFY_DIFF_BACKEND` 환경 변수를 `true`으로 설정합니다. 조건부 백엔드 빌드를 활성화하면 프런트엔드만 변경하는 빌드의 속도를 높이는 데 도움이 됩니다.

diff 기반 백엔드 빌드를 활성화하면 Amplify는 각 빌드를 시작할 때 리포지토리의 `amplify` 폴더에서 diff 실행을 시도합니다. Amplify에서 차이점을 발견하지 못하면 백엔드 빌드 단계를 건너뛰고 백엔드 리소스를 업데이트하지 않습니다. 프로젝트의 리포지토리에 `amplify` 폴더가 없는 경우, Amplify는 `AMPLIFY_DIFF_BACKEND` 환경 변수 값을 무시합니다. `AMPLIFY_DIFF_BACKEND`환경 변수 설정에 대한 지침은 을 참조하십시오. 1세대 앱의 diff 기반 백엔드 빌드를 활성화 또는 비활성화합니다.

현재 백엔드 단계의 빌드 설정에 사용자 지정 명령이 지정되어 있는 경우, 조건부 백엔드 빌드는 작동하지 않습니다. 이러한 사용자 지정 명령을 실행하려면 앱의 `amplify.yml` 파일에 있는 빌드 설정의 프런트엔드 단계로 해당 명령을 이동해야 합니다. `amplify.yml` 파일을 업데이트하는 방법에 대한 자세한 내용은 빌드 사양 명령 및 설정을 참조하십시오.

여러 앱에서 Amplify 백엔드 사용 (1세대 앱만 해당)

> **Note**
>
> 이 섹션의 정보는 1세대 앱에만 해당됩니다. 2세대 앱의 백엔드 리소스를 공유하려면 Amplify 문서에서 브랜치 간 리소스 공유를 참조하십시오.

Amplify를 사용하면 특정 지역의 모든 1세대 앱에서 기존 백엔드 환경을 재사용할 수 있습니다. 새 앱을 만들거나, 새 브랜치를 기존 앱에 연결하거나, 다른 백엔드 환경을 가리키도록 기존 프런트엔드를 업데이트할 때 이 작업을 수행할 수 있습니다.

새 앱 생성 시 백엔드 재사용

새 Amplify 앱을 만들 때 백엔드를 재사용하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 이 예를 활용하려면 다음과 같이 하십시오.

   a. 서비스 탐색 창에서 모든 앱을 선택합니다.

   b. 새 앱, 앱 빌드를 선택합니다.

   c. 앱의 이름(예: **`Example-Amplify-App`**)을 입력합니다.

   d. 배포 확인을 선택합니다.
3. 프런트엔드를 새 백엔드에 연결하려면 호스팅 환경 탭을 선택합니다.
4. Git 공급자를 선택하고 브랜치 연결을 선택합니다.
5. 리포지토리 브랜치 추가 페이지에서 최근 업데이트된 리포지토리의 경우, 리포지토리 이름을 선택합니다. 브랜치의 경우, 리포지토리에서 연결할 브랜치를 선택합니다.
6. 빌드 설정 페이지에서 다음 작업을 수행하십시오.

   a. 앱 이름에서 백엔드 환경을 추가하는 데 사용할 앱을 선택합니다. 현재 앱 또는 현재 지역의 다른 앱을 선택할 수 있습니다.

   b. 환경에서 추가할 백엔드 환경의 이름을 선택합니다. 기존의 환경을 사용하거나 새 환경을 생성할 수 있습니다.

   c. 기본적으로 풀스택 CI/CD는 꺼져 있습니다. 풀스택 CI/CD를 끄면 앱이 풀 전용 모드로 실행됩니다. 빌드 시 Amplify는 백엔드 환경을 수정하지 않고 `aws-exports.js` 파일만 자동으로 생성합니다.

   d. 기존 서비스 역할을 선택하여 Amplify에 앱 백엔드를 변경하는 데 필요한 권한을 부여합니다. 서비스 역할을 생성해야 하는 경우, 새 역할 생성을 선택합니다. 서비스 역할 생성에 대한 자세한 내용은 서비스 역할 추가을 참조하십시오.

   e. 다음을 선택합니다.
7. 저장 및 배포를 선택합니다.

브랜치를 기존 앱에 연결할 때 백엔드를 재사용하십시오.

브랜치를 기존 Amplify 앱에 연결할 때 백엔드를 재사용하려면

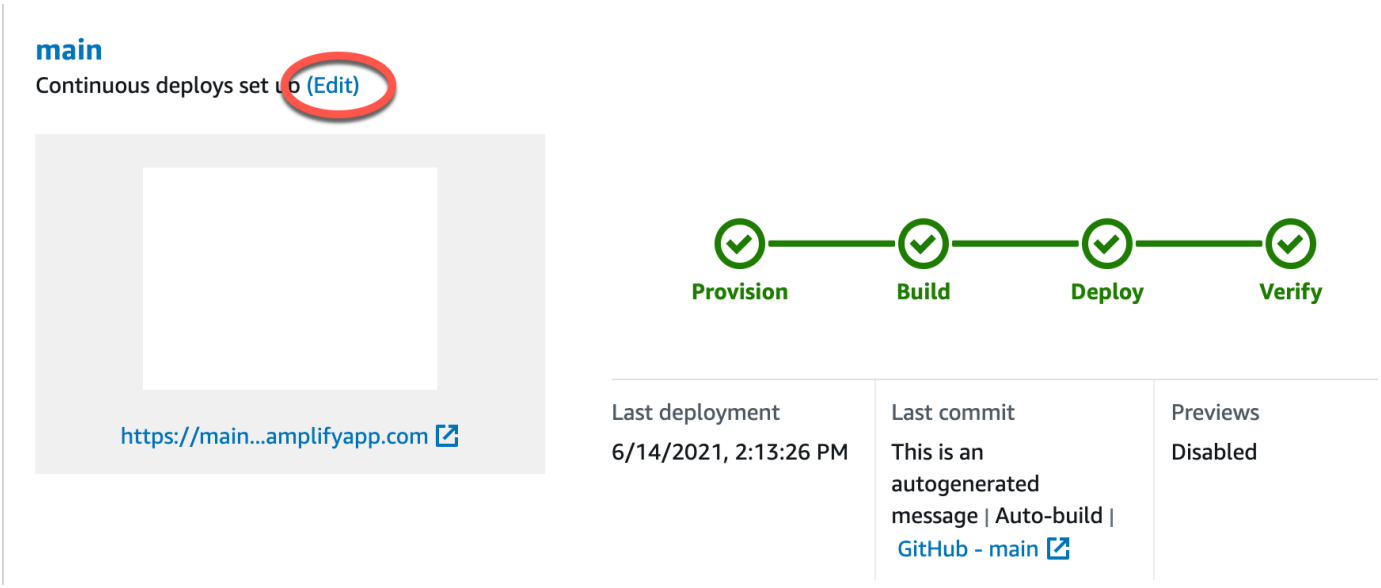
1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.

2. 새 브랜치를 연결할 앱을 선택합니다.
3. 탐색 창에서 앱 설정, 일반을 선택합니다.
4. 브랜치 섹션에서 브랜치 연결을 선택합니다.
5. 리포지토리 브랜치 추가 페이지에서 브랜치의 경우, 리포지토리에서 연결할 브랜치를 선택합니다.
6. 앱 이름에서 백엔드 환경을 추가하는 데 사용할 앱을 선택합니다. 현재 앱 또는 현재 지역의 다른 앱을 선택할 수 있습니다.
7. 환경에서 추가할 백엔드 환경의 이름을 선택합니다. 기존의 환경을 사용하거나 새 환경을 생성할 수 있습니다.
8. Amplify에 앱 백엔드를 변경하는 데 필요한 권한을 부여하기 위해 서비스 역할을 설정해야 하는 경우, 콘솔에 이 작업을 수행하라는 메시지가 표시됩니다. 서비스 역할 생성에 대한 자세한 내용은 서비스 역할 추가을 참조하십시오.
9. 기본적으로 풀스택 CI/CD는 꺼져 있습니다. 풀스택 CI/CD를 끄면 앱이 풀 전용 모드로 실행됩니다. 빌드 시 Amplify는 백엔드 환경을 수정하지 않고 `aws-exports.js` 파일만 자동으로 생성합니다.
10. 다음을 선택합니다.
11. 저장 및 배포를 선택합니다.

다른 백엔드를 가리키도록 기존 프론트엔드를 편집합니다.

다른 백엔드를 가리키도록 프런트엔드 Amplify 앱을 편집하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 백엔드를 편집할 앱을 선택합니다.
3. 호스팅 환경 탭을 선택합니다.
4. 편집할 브랜치를 찾아 편집을 선택합니다.



5. 이 브랜치와 함께 사용할 백엔드 환경 선택 페이지에서 앱 이름으로 백엔드 환경을 편집하려는 프런트엔드 앱을 선택합니다. 현재 앱 또는 현재 지역의 다른 앱을 선택할 수 있습니다.
6. 백엔드 환경의 경우, 추가할 백엔드 환경의 이름을 선택합니다.
7. 기본적으로 풀스택 CI/CD가 활성화됩니다. 이 백엔드의 풀 스택 CI/CD를 끄려면 이 옵션을 선택 취소하십시오. 풀스택 CI/CD를 끄면 앱이 풀 전용 모드로 실행됩니다. 빌드 시 Amplify는 백엔드 환경을 수정하지 않고 `aws-exports.js` 파일만 자동으로 생성합니다.
8. 저장을 선택합니다. Amplify는 다음에 앱을 구축할 때 이러한 변경 사항을 적용합니다.

애플리케이션을 위한 백엔드 구축

AWS Amplify 를 사용하여 배포되는 데이터, 인증, 스토리지 및 프런트엔드 호스팅을 포함하는 풀스택 애플리케이션을 구축할 수 있습니다. AWS

AWS Amplify Gen 2는 백엔드를 정의하기 TypeScript 위한 코드 우선 기반의 개발자 환경을 도입합니다. Amplify Gen 2를 사용하여 백엔드를 빌드하고 앱에 연결하는 방법을 알아보려면 Amplify 문서에서 백엔드 구축 및 연결을 참조하십시오.

CLI와 Amplify Studio를 사용하여 1세대 앱용 백엔드를 구축하는 방법에 대한 설명서를 찾으려면 1세대 Amplify 문서에서 백엔드 구축 및 연결을 참조하십시오.

주제

- 2세대 앱을 위한 백엔드 만들기
- 1세대 앱을 위한 백엔드 만들기

2세대 앱을 위한 백엔드 만들기

TypeScript기반 백엔드를 사용하여 Amplify Gen 2 풀스택 애플리케이션을 만드는 단계를 안내하는 자습서는 Amplify 문서에서 시작하기를 참조하십시오.

1세대 앱을 위한 백엔드 만들기

이 자습서에서는 Amplify를 사용하여 풀스택 CI/CD 워크플로를 설정합니다. Amplify 호스팅에 프런트엔드 앱을 배포합니다. 그런 다음 Amplify Studio를 사용하여 백엔드를 생성합니다. 마지막으로 클라우드 백엔드를 프런트엔드 앱에 연결합니다.

필수 조건

이 자습서를 시작하기 전에 다음 사전 요구 사항을 완료하세요.

등록하여 AWS 계정

> 아직 AWS 고객이 아닌 경우 온라인 지침에 따라 AWS 계정가입해야 합니다. 가입하면 Amplify 및 애플리케이션과 함께 사용할 수 있는 기타 AWS 서비스에 액세스할 수 있습니다.

Git 리포지토리 만들기

Amplify는 비트버킷 GitHub, GitLab 및 을 지원합니다. AWS CodeCommit애플리케이션을 Git 리포지토리로 푸시합니다.

Amplify 명령줄 인터페이스 (CLI) 설치

자세한 지침은 Amplify 프레임워크 설명서의 Amplify CLI 설치를 참조하십시오.

1단계: 프론트엔드 배포

이 예제에 사용하려는 기존 프런트엔드 앱이 git 저장소에 있는 경우, 프런트엔드 앱 배포 안내를 진행하면 됩니다.

이 예제에 사용할 새 프론트엔드 앱을 만들어야 하는 경우 React 앱 만들기 설명서의 React 앱 만들기 지침을 따르세요.

프론트엔드 앱을 배포하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 모든 앱 페이지에서 새 앱을 선택한 다음 오른쪽 상단에서 웹 앱 호스팅을 선택합니다.
3. 사용자 GitHub, Bitbucket 또는 AWS CodeCommit 리포지토리 공급자를 선택한 다음 계속을 선택합니다. GitLab
4. Amplify는 git 리포지토리에 대한 액세스를 승인합니다. GitHub 리포지토리의 경우 Amplify는 이제 GitHub 앱 기능을 사용하여 Amplify 액세스를 승인합니다.

   앱 설치 및 인증에 대한 자세한 내용은 을 참조하십시오. GitHub GitHub 리포지토리에 대한 Amplify 액세스 설정
5. 리포지토리 브랜치 추가 페이지에서 다음을 수행하십시오.

   a. 최근 업데이트된 리포지토리 목록에서 연결할 리포지토리 이름을 선택합니다.

   b. 브랜치 목록에서 연결할 리포지토리 브랜치의 이름을 선택합니다.

   c. 다음을 선택합니다.
6. 보안 설정 구성 페이지에서 다음을 선택합니다.
7. 검토 페이지에서 저장 및 배포를 선택합니다. 배포가 완료되면 `amplifyapp.com` 기본 도메인에서 앱을 볼 수 있습니다.

> **Note**
>
> Amplify 애플리케이션의 보안을 강화하기 위해 amplifyapp.com 도메인은 공개 서픽스 목록(PSL)에 등록되어 있습니다. 보안 강화를 위해 Amplify 애플리케이션의 기본 도메인 이름에 민감한 쿠키를 설정해야 하는 경우, `__Host-` 접두사가 있는 쿠키를 사용하는 것이 좋습니다. 이렇게 쿠키를 설정하면 교차 사이트 요청 위조 시도(CSRF)로부터 도메인을 보호하는 데 도움이 됩니다. 자세한 내용은 Mozilla 개발자 네트워크의 Set-Cookie 페이지를 참조하십시오.

2단계: 백엔드 생성

이제 Amplify 호스팅에 프런트엔드 앱을 배포했으므로 백엔드를 만들 수 있습니다. 다음 지침에 따라 간단한 데이터베이스 및 GraphQL API 엔드포인트가 있는 백엔드를 생성하십시오.

백엔드를 생성하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 모든 앱 페이지에서 1단계에서 만든 앱을 선택합니다.
3. 앱 홈페이지에서 백엔드 환경 탭을 선택한 다음 시작하기을 선택합니다. 그러면 기본 스테이징 환경을 위한 설정 프로세스가 시작됩니다.
4. 설정이 완료되면 스튜디오 실행을 선택하여 Amplify Studio의 스테이징 백엔드 환경에 액세스합니다.

Amplify Studio는 백엔드를 생성 및 관리하고 프론트엔드 UI 개발을 가속화하는 시각적 인터페이스입니다. Amplify Studio에 대한 자세한 내용은 Amplify Studio 설명서를 참조하십시오.

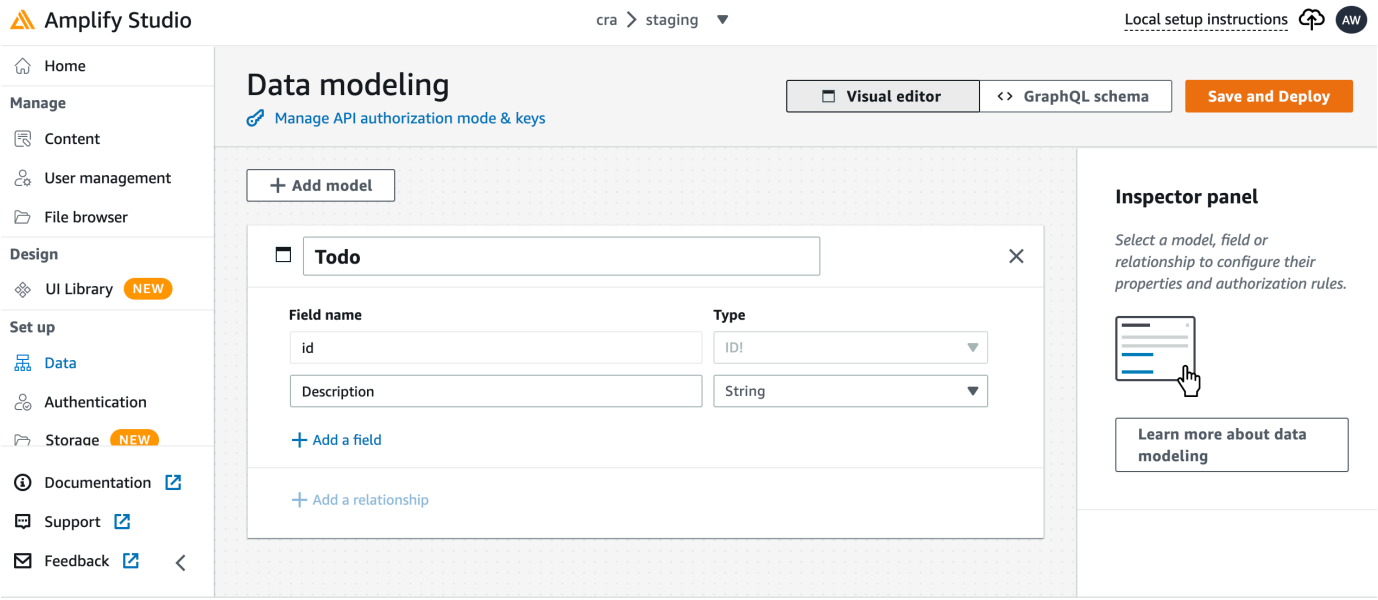
다음 지침에 따라 Amplify Studio 비주얼 백엔드 빌더 인터페이스를 사용하여 간단한 데이터베이스를 생성하십시오.

데이터 모델 생성

1. 앱의 스테이징 환경 홈 페이지에서 데이터 모델 생성을 선택합니다. 그러면 데이터 모델 디자이너가 열립니다.
2. 데이터 모델링 페이지에서 모델 추가를 선택합니다.
3. 제목으로 **Todo**을(를) 입력합니다.
4. 필드 추가를 선택합니다.

5. 모델 이름에 **Description**을(를) 입력합니다.

   다음 스크린샷은 디자이너에서 데이터 모델이 어떻게 보일지 보여주는 예입니다.



6. 저장 및 배포를 선택합니다.
7. Amplify Hosting 콘솔로 돌아가면 스테이징 환경 배포가 진행됩니다.

배포 중에 Amplify Studio는 데이터에 액세스하기 위한 AWS AppSync GraphQL API와 Todo 항목을 호스팅하기 위한 Amazon DynamoDB 테이블을 포함하여 필요한 모든 AWS 리소스를 백엔드에 생성합니다. Amplify는 백엔드를 AWS CloudFormation 배포하는 데 사용하며, 이를 통해 백엔드 정의를 다음과 같이 저장할 수 있습니다. infrastructure-as-code

3단계: 백엔드를 프런트엔드에 연결

이제 프런트엔드를 배포하고 데이터 모델을 포함하는 클라우드 백엔드를 만들었으므로 프런트엔드를 연결해야 합니다. Amplify CLI를 사용하여 백엔드 정의를 로컬 앱 프로젝트로 가져오려면 다음 지침을 따르십시오.

클라우드 백엔드를 로컬 프런트엔드에 연결하려면

1. 터미널 창을 열고 로컬 프로젝트의 루트 디렉터리로 이동합니다.
2. 터미널 창에서 다음 명령을 실행하여 빨간색 텍스트를 프로젝트의 고유한 앱 ID 및 백엔드 환경 이름으로 대체합니다.

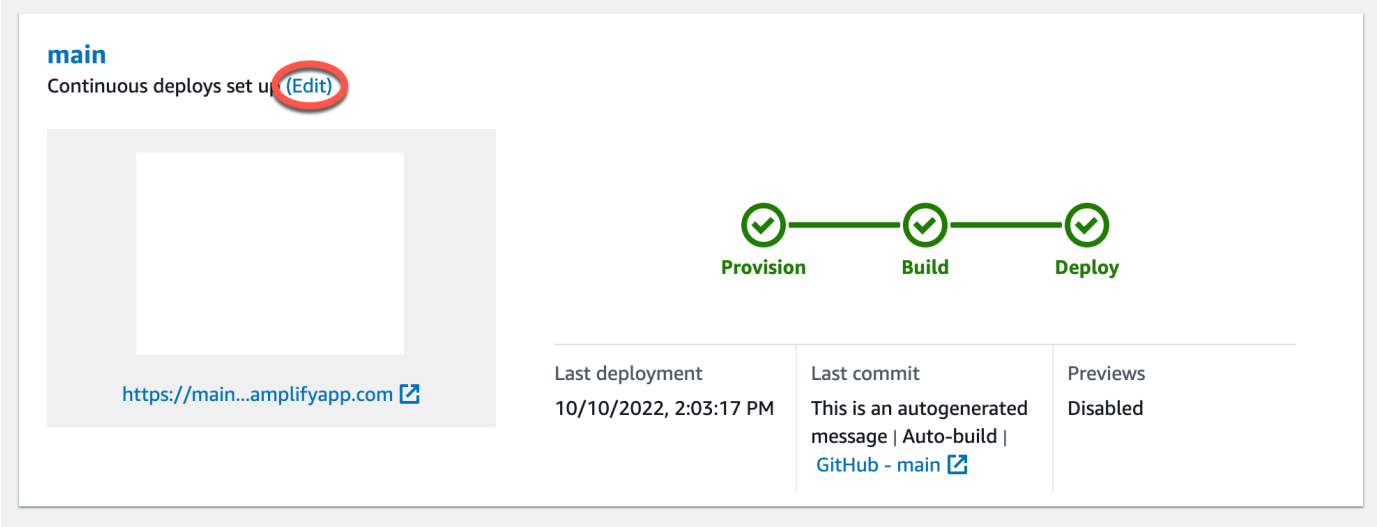
```
amplify pull --appId abcd1234 --envName staging
```

3. 터미널 창의 지침에 따라 프로젝트 설정을 완료하십시오.

이제 지속적 배포 워크플로에 백엔드를 추가하도록 빌드 프로세스를 구성할 수 있습니다. Amplify 호스팅 콘솔에서 프런트엔드 브랜치를 백엔드에 연결하려면 다음 지침을 따르십시오.

프런트엔드 앱 브랜치와 클라우드 백엔드를 연결하려면

1. 앱 홈페이지에서 호스팅 환경 탭을 선택합니다.
2. 기본 브랜치를 찾아 편집을 선택합니다.



3. 대상 백엔드 편집 창의 환경에서 연결할 백엔드의 이름을 선택합니다. 이 예시에서는 2단계에서 만든 스테이징 백엔드를 선택합니다.

   기본적으로 풀스택 CI/CD가 활성화됩니다. 이 백엔드의 풀 스택 CI/CD를 끄려면 이 옵션을 선택 취소하십시오. 풀스택 CI/CD를 끄면 앱이 풀 전용 모드로 실행됩니다. 빌드 시 Amplify는 백엔드 환경을 수정하지 않고 `aws-exports.js` 파일만 자동으로 생성합니다.
4. 다음으로 앱 백엔드를 변경하는 데 필요한 권한을 Amplify에 제공하도록 서비스 역할을 설정해야 합니다. 새로운 서비스 역할을 만들거나 기존 역할을 사용할 수 있습니다. 지침은 서비스 역할 추가을 참조하세요.
5. 서비스 역할을 추가한 후 대상 백엔드 편집 창으로 돌아가서 저장을 선택합니다.
6. 스테이징 백엔드를 프론트엔드 앱의 기본 브랜치에 연결하는 작업을 마치려면 프로젝트의 새 빌드를 수행하십시오.

   다음 중 하나를 수행하십시오.
   - git 리포지토리에서 일부 코드를 푸시하여 Amplify 콘솔에서 빌드를 시작합니다.
   - Amplify 콘솔에서 앱의 빌드 세부 정보 페이지로 이동한 다음 이 버전 재배포를 선택합니다.

다음 단계

기능 브랜치 배포 설정

권장 워크플로에 따라 여러 백엔드 환경에서 기능 브랜치 배포를 설정하십시오.

Amplify Studio에서 프론트엔드 UI 만들기

Studio를 사용하여 ready-to-use UI 구성 요소 집합으로 프런트엔드 UI를 빌드한 다음 이를 앱 백엔드에 연결합니다. 자세한 내용 및 자습서는 Amplify 프레임워크 설명서에서 Amplify Studio 사용 설명서를 참조하십시오.

수동 배포

수동 배포를 사용하면 Git 공급자에게 연결하지 않고 웹 앱을 Amplify Hosting에 게시할 수 있습니다. 데스크톱에서 폴더를 끌어서 놓으면 몇 초 안에 사이트를 호스팅할 수 있습니다. 또는 Amazon S3 버킷의 자산을 참조하거나 파일이 저장된 위치의 퍼블릭 URL을 지정할 수 있습니다.

Amazon S3의 경우 새 자산이 업로드될 때마다 사이트를 업데이트하도록 AWS Lambda 트리거를 설정할 수도 있습니다. 이 시나리오 설정에 대한 자세한 내용은 Amazon S3, Dropbox 또는 데스크톱에 저장된 파일을 AWS Amplify 콘솔에 배포하기 블로그 게시물을 참조하십시오.

Amplify Hosting은 서버 측 렌더링(SSR) 앱의 수동 배포를 지원하지 않습니다. 자세한 정보는 Amplify Hosting을 통해 서버 측 렌더링 앱 배포을 참조하세요.

드래그 앤 드롭 방식의 수동 배포

드래그 앤 드롭을 사용하여 앱을 수동으로 배포하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 오른쪽 상단에서 새 앱 만들기를 선택합니다.
3. Amplify로 빌드 시작 페이지에서 Git을 사용하지 않고 배포를 선택합니다. 그리고 다음을 선택합니다.
4. 수동 배포 시작 섹션의 앱 이름에 앱 이름을 입력합니다.
5. 브랜치 이름에는 또는 와 같은 **`development`** 의미 있는 이름을 입력합니다. **`production`**
6. 방법에서 드래그 앤 드롭을 선택합니다.
7. 데스크탑에서 드롭 존으로 폴더를 드래그 앤 드롭하거나.zip 폴더 선택을 사용하여 컴퓨터에서 파일을 선택합니다. 끌어서 놓거나 선택하는 파일은 빌드 출력의 콘텐츠가 포함된 zip 폴더여야 합니다.
8. 저장 및 배포를 선택합니다.

Amazon S3 또는 URL 수동 배포

Amazon S3 또는 퍼블릭 URL에서 앱을 수동으로 배포하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 오른쪽 상단에서 새 앱 만들기를 선택합니다.

3. Amplify로 빌드 시작 페이지에서 Git을 사용하지 않고 배포를 선택합니다. 그리고 다음을 선택합니다.
4. 수동 배포 시작 섹션의 앱 이름에 앱 이름을 입력합니다.
5. 브랜치 이름에는 또는 와 같은 **development** 의미 있는 이름을 입력합니다. **production**
6. 방법에서 Amazon S3 또는 모든 URL을 선택합니다.
7. 파일 업로드 절차는 업로드 방법에 따라 다릅니다.
   - Amazon S3
     a. Amazon S3 버킷의 경우 목록에서 Amazon S3 버킷의 이름을 선택합니다. 선택한 버킷에 액세스 제어 목록(ACL)을 활성화해야 합니다. 자세한 정보는 Amazon S3 버킷 액세스 문제 해결을 참조하세요.
     b. zip 파일에는 배포할 zip 파일의 이름을 선택합니다.
   - 모든 URL
     - 리소스 URL에는 배포할 압축 파일의 URL을 입력합니다.
8. 저장 및 배포를 선택합니다.

> **Note**
>
> zip 폴더를 만들 때는 최상위 폴더가 아닌 빌드 출력의 콘텐츠를 압축해야 합니다. 예를 들어 빌드 출력에서 이름이 “build” 또는 “public”인 폴더가 생성되면 먼저 해당 폴더로 이동하여 모든 콘텐츠를 선택한 다음 압축합니다. 이렇게 하지 않으면 사이트의 루트 디렉터리가 제대로 초기화되지 않기 때문에 “액세스 거부됨” 오류가 표시됩니다.

Amazon S3 버킷 액세스 문제 해결

Amazon S3 버킷 생성 시 Amazon S3 객체 소유권 설정을 사용하여 버킷에 대한 액세스 제어 목록(ACL) 활성화 여부를 제어합니다. Amazon S3 버킷에서 Amplify에 앱을 수동으로 배포하려면 버킷에 ACL을 활성화해야 합니다.

Amazon S3 버킷에서 배포 시 `AccessControlList` 오류가 발생하는 경우, ACL이 비활성화된 상태로 버킷이 생성되었으므로 Amazon S3 콘솔에서 ACL을 활성화해야 합니다. 지침을 보려면 Amazon Simple Storage Service 사용 설명서에서 기존 버킷에 객체 소유권 설정을 참조하십시오.

Amplify에 배포 버튼

Amplify Hosting에 배포 버튼을 사용하면 GitHub 프로젝트를 공개적으로 또는 팀 내에서 공유할 수 있습니다. 다음은 버튼 이미지입니다.

Amplify Hosting에 배포 버튼을 리포지토리 또는 블로그에 추가

버튼을 GitHub README.md 파일, 블로그 게시물, 또는 HTML을 렌더링하는 기타 마크업 페이지에 추가합니다. 버튼은 두 가지 구성 요소를 갖습니다.

1. URL `https://oneclick.amplifyapp.com/button.svg`에 있는 SVG 이미지
2. GitHub 리포지토리 링크가 포함된 Amplify 콘솔 URL. 리포지토리의 URL(예: `https://github.com/username/repository`)을 복사하거나 특정 폴더(예: `https://github.com/username/repository/tree/branchname/folder`)에 딥 링크를 제공할 수 있습니다. Amplify Hosting은 리포지토리의 기본 브랜치를 배포합니다. 앱을 연결한 후에 추가 브랜치를 연결할 수 있습니다.

다음 예제를 사용하여 GitHub Readme.md와 같은 마크다운 파일에 버튼을 추가합니다. `https://github.com/username/repository`을(를) 리포지토리의 URL로 바꿉니다.

```
[![amplifybutton](https://oneclick.amplifyapp.com/button.svg)](https://
console.aws.amazon.com/amplify/home#/deploy?repo=https://github.com/username/
repository)
```

다음 예제를 사용하여 HTML 문서에 버튼을 추가할 수 있습니다. `https://github.com/username/repository`을 리포지토리의 URL로 바꿉니다.

```
<a href="https://console.aws.amazon.com/amplify/home#/deploy?repo=https://github.com/
username/repository">
    <img src="https://oneclick.amplifyapp.com/button.svg" alt="Deploy to Amplify
 Hosting">
</a>
```

GitHub 리포지토리에 대한 Amplify 액세스 설정

Amplify는 이제 GitHub 앱 기능을 사용하여 GitHub 리포지토리에 대한 Amplify의 읽기 전용 액세스를 승인합니다. Amplify GitHub 앱을 사용하면 권한이 더욱 세밀하게 조정되므로 지정한 리포지토리에만 Amplify에 액세스 권한을 부여할 수 있습니다. GitHub 앱에 대해 자세히 알아보려면 GitHub 웹 사이트의 GitHub 앱 정보를 참조하세요.

GitHub 리포지토리에 저장된 새 앱을 연결하면 Amplify는 기본적으로 GitHub 앱을 사용하여 리포지토리에 액세스합니다. 하지만 이전에 GitHub 리포지토리에서 연결한 기존 Amplify 앱은 액세스에 OAuth를 사용합니다. CI/CD는 이러한 앱에서 계속 작동하지만 새로운 Amplify GitHub 앱을 사용하도록 마이그레이션하는 것이 좋습니다.

Amplify 콘솔을 사용하여 새 앱을 배포하거나 기존 앱을 마이그레이션하면 Amplify GitHub 앱의 설치 위치로 자동 안내됩니다. 앱의 설치 랜딩 페이지에 수동으로 액세스하려면 웹 브라우저를 열고 리전별로 앱을 탐색하세요. 형식 `https://github.com/apps/aws-amplify-`*`REGION`*을(를) 사용하여 *#*#을 Amplify 앱을 배포할 리전으로 대체하세요. 예를 들어, 미국 서부(오레곤)리전에 Amplify GitHub 앱을 설치하려면 https://github.com/apps/aws-amplify-us-west-2으로 이동하세요.

주제

- 새 배포를 위한 Amplify GitHub 앱 설치 및 권한 부여
- 기존 OAuth 앱을 Amplify GitHub 앱으로 마이그레이션하기
- AWS CloudFormation, CLI 및 SDK 배포를 위한 Amplify GitHub 앱 설정
- Amplify GitHub 앱을 사용하여 웹 미리 보기 설정하기

새 배포를 위한 Amplify GitHub 앱 설치 및 권한 부여

GitHub 리포지토리의 기존 코드를 사용하여 Amplify에 새 앱을 배포하는 경우, 다음 지침에 따라 GitHub 앱을 설치하고 승인하세요.

Amplify GitHub 앱을 설치하고 승인하려면

1. AWS Management Console에 로그인하고 Amplify 콘솔을 엽니다.
2. 모든 앱 페이지에서 새 앱을 선택한 다음 웹 앱 호스팅을 선택합니다.
3. Amplify Hosting 시작하기 페이지에서 GitHub를 선택한 다음 계속을 선택합니다.
4. GitHub 리포지토리를 처음 연결하는 경우, GitHub.com의 브라우저에 GitHub 계정에서 AWS Amplify을(를) 승인할 수 있는 권한을 요청하는 새 페이지가 열립니다. 승인을 선택합니다.

5. 다음으로 GitHub 계정에 Amplify GitHub 앱을 설치해야 합니다. GitHub 계정에 AWS Amplify의 설치 및 승인을 요청하는 페이지가 GitHub.com에서 열립니다.
6. Amplify GitHub 앱을 설치할 GitHub 계정을 선택합니다.
7. 다음 중 하나를 수행하세요.
   - 모든 리포지토리에 설치를 적용하려면 모든 리포지토리를 선택합니다.
   - 선택한 특정 리포지토리로 설치를 제한하려면 리포지토리만 선택을 선택합니다. 선택한 리포지토리에 마이그레이션하려는 앱의 리포지토리를 포함해야 합니다.
8. 설치 및 승인을 선택합니다.
9. Amplify 콘솔에서 앱의 리포지토리 분기 추가 페이지로 리디렉션됩니다.
10. 최근 업데이트된 리포지토리 목록에서 연결할 리포지토리 이름을 선택합니다.
11. 브랜치 목록에서 연결할 리포지토리 브랜치의 이름을 선택합니다.
12. 다음을 선택합니다.
13. 보안 설정 구성 페이지에서 다음을 선택합니다.
14. 검토 페이지에서 저장 및 배포를 선택합니다.

기존 OAuth 앱을 Amplify GitHub 앱으로 마이그레이션하기

이전에 GitHub 리포지토리에서 연결한 기존 Amplify 앱은 리포지토리 액세스에 OAuth를 사용합니다. Amplify GitHub 앱을 사용하려면 이러한 앱을 마이그레이션하는 것이 좋습니다.

다음 지침에 따라 앱을 마이그레이션하고 GitHub 계정에서 해당 OAuth 웹후크를 삭제하세요. 참고로 마이그레이션 절차는 Amplify GitHub 앱이 이미 설치되어 있는지 여부에 따라 달라집니다. 첫 번째 앱을 마이그레이션하고 GitHub 앱을 설치 및 승인한 후에는 후속 앱 마이그레이션을 위해 리포지토리 권한만 업데이트하면 됩니다.

앱을 OAuth에서 GitHub 앱으로 마이그레이션하려면

1. AWS Management Console에 로그인하고 Amplify 콘솔을 엽니다.
2. 마이그레이션할 앱을 선택합니다.
3. 앱의 정보 페이지에서 파란색 GitHub 앱으로 마이그레이션 메시지를 찾아 마이그레이션 시작을 선택합니다.
4. GitHub 앱 설치 및 승인 페이지에서 GitHub 앱 구성을 선택합니다.
5. GitHub.com의 브라우저에 GitHub 계정에서 AWS Amplify를 승인할 수 있는 권한을 요청하는 새 페이지가 열립니다. Authorize를 선택합니다.

6. Amplify GitHub 앱을 설치할 GitHub 계정을 선택합니다.
7. 다음 중 하나를 수행하세요.
   - 모든 리포지토리에 설치를 적용하려면 모든 리포지토리를 선택합니다.
   - 선택한 특정 리포지토리로 설치를 제한하려면 리포지토리만 선택을 선택합니다. 선택한 리포지토리에 마이그레이션하려는 앱의 리포지토리를 포함해야 합니다.
8. 설치 및 승인을 선택합니다.
9. Amplify 콘솔의 앱에 대한 GitHub 앱 설치 및 승인 페이지로 리디렉션됩니다. GitHub 인증에 성공하면 성공 메시지가 표시됩니다. 다음을 선택합니다.
10. 설치 완료 페이지에서 설치 완료를 선택합니다. 이 단계는 기존 웹후크를 삭제하고, 새 웹후크를 만들고, 마이그레이션을 완료합니다.

AWS CloudFormation, CLI 및 SDK 배포를 위한 Amplify GitHub 앱 설정

이전에 GitHub 리포지토리에서 연결한 기존 Amplify 앱은 리포지토리 액세스에 OAuth를 사용합니다. 여기에는 Amplify 명령줄 인터페이스(CLI), AWS CloudFormation, 또는 SDK를 사용하여 배포한 앱이 포함될 수 있습니다. 새 Amplify GitHub 앱을 사용하려면 이러한 앱을 마이그레이션하는 것이 좋습니다. 마이그레이션은 Amplify 콘솔의 AWS Management Console에서 수행해야 합니다. 지침은 기존 OAuth 앱을 Amplify GitHub 앱으로 마이그레이션하기 단원을 참조하세요.

AWS CloudFormation, Amplify CLI, SDK를 사용하여 리포지토리 액세스를 위해 GitHub 앱을 사용하는 새로운 Amplify 앱을 배포할 수 있습니다. 이 프로세스를 진행하려면 먼저 GitHub 계정에 Amplify GitHub 앱을 설치해야 합니다. 다음으로 GitHub 계정에서 개인용 액세스 토큰을 생성해야 합니다. 마지막으로 앱을 배포하고 개인용 액세스 토큰을 지정합니다.

계정에 Amplify GitHub 앱을 설치하세요.

1. 웹 브라우저를 열고 앱을 배포할 AWS 리전의 Amplify GitHub 앱 설치 위치로 이동합니다.

   *##*을 사용자가 직접 입력한 것으로 대체하는 형식 `https://github.com/apps/aws-amplify-`*`REGION`*`/installations/new`을(를) 사용하세요. 예를 들어 미국 서부(오레곤) 리전에 앱을 설치하는 경우, `https://github.com/apps/aws-amplify-us-west-2/installations/new`을(를) 지정합니다.
2. Amplify GitHub 앱을 설치할 GitHub 계정을 선택합니다.
3. 다음 중 하나를 수행하세요.

- 모든 리포지토리에 설치를 적용하려면 모든 리포지토리를 선택합니다.
- 선택한 특정 리포지토리로 설치를 제한하려면 리포지토리만 선택을 선택합니다. 선택한 리포지토리에 마이그레이션하려는 앱의 리포지토리를 포함해야 합니다.

4. 설치를 선택합니다.

GitHub 계정에서 개인용 액세스 토큰 생성

1. GitHub 계정에 가입합니다.
2. 오른쪽 상단에서 프로필 사진을 찾아 메뉴에서 설정을 선택합니다.
3. 왼쪽 탐색 메뉴에서 개발자 설정을 선택합니다.
4. GitHub 앱 페이지의 왼쪽 탐색 메뉴에서 개인용 액세스 토큰을 선택합니다.
5. 개인용 액세스 토큰 페이지에서 새 토큰 생성을 선택합니다.
6. 새 개인용 액세스 토큰 페이지에서 노트에 토큰을 설명하는 이름을 입력합니다.
7. 범위 선택 섹션에서 admin:repo_hook을 선택합니다.
8. 토큰 생성을 선택합니다.
9. 개인용 액세스 토큰을 복사하고 저장합니다. CLI, AWS CloudFormation 또는 SDK를 사용하여 Amplify 앱을 배포할 때 이를 제공해야 합니다.

Amplify GitHub 앱을 GitHub 계정에 설치하고 개인용 액세스 토큰을 생성한 후에는 Amplify CLI, AWS CloudFormation 또는 SDK를 사용하여 새 앱을 배포할 수 있습니다. `accessToken` 필드를 사용하여 이전 절차에서 생성한 개인용 액세스 토큰을 지정합니다. 자세한 내용은 Amplify API 참조의 CreateApp 및 AWS CloudFormation 사용 설명서의 AWS::Amplify::앱을 참조하세요.

다음 CLI 명령은 리포지토리 액세스를 위해 GitHub 앱을 사용하는 새로운 Amplify 앱을 배포합니다. *myapp-using-Githubapp*, *https://Github.com/Myaccount/react-app*, *MY_TOKEN*을 사용자 고유의 정보로 바꾸세요.

```
aws amplify create-app --name myapp-using-githubapp --repository https://github.com/
Myaccount/react-app --access-token MY_TOKEN
```

Amplify GitHub 앱을 사용하여 웹 미리 보기 설정하기

웹 미리보기는 GitHub 리포지토리에 대한 모든 풀 요청(PR)을 고유한 미리 보기 URL에 배포합니다. 프리뷰는 이제 Amplify GitHub 앱을 사용하여 GitHub 리포지토리에 액세스할 수 있습니다. 웹 미리 보기용 GitHub 앱 설치 및 권한 부여에 대한 지침은 웹 미리 보기를 활성화합니다. 단원을 참조하세요.

pull 요청를 위한 웹 미리 보기

웹 미리 보기는 개발 및 품질 보증(QA) 팀이 코드를 프로덕션 또는 통합 브랜치에 병합하기 전에 pull 요청(PR) 의 변경 사항을 미리 볼 수 있는 방법을 제공합니다. pull 요청를 사용하면 리포지토리의 브랜치에 푸시한 변경 내용을 다른 사람에게 알릴 수 있습니다. pull 요청가 열리면 공동 작업자와 잠재적 변경 사항을 논의 및 검토하고 변경 사항을 기본 브랜치에 병합하기 전에 후속 커밋을 추가할 수 있습니다.

웹 미리 보기는 리포지토리에 대한 모든 pull 요청을 기본 사이트에서 사용하는 URL과 완전히 다른 고유한 미리 보기 URL에 배포합니다. Amplify CLI 또는 Amplify Studio를 사용하여 백엔드 환경을 프로비저닝하는 앱의 경우 모든 pull 요청 (프라이빗 Git 리포지토리만 해당) 은 PR이 종료될 때 삭제되는 임시 백엔드를 생성합니다.

앱에 웹 미리보기를 켜면 각 PR은 앱당 50개 브랜치인 Amplify 할당량에 포함됩니다. 이 할당량을 초과하지 않도록 하려면 PR을 닫아야 합니다. 할당량에 대한 자세한 내용은 Amplify Hosting 서비스 할당량 섹션을 참조하세요.

> **Note**
>
> 현재 `AWS_PULL_REQUEST_ID` 환경 변수를 리포지토리 AWS CodeCommit 공급자로 사용할 때는 사용할 수 없습니다.

웹 미리 보기를 활성화합니다.

GitHub 리포지토리에 저장된 앱의 경우 미리보기는 Amplify GitHub 앱을 사용하여 리포지토리에 액세스할 수 있습니다. 액세스용 OAuth를 사용하여 이전에 리포지토리에서 GitHub 배포한 기존 Amplify 앱에서 웹 미리 보기를 활성화하려면 먼저 Amplify 앱을 사용하도록 앱을 마이그레이션해야 합니다. GitHub 마이그레이션 지침은 기존 OAuth 앱을 Amplify GitHub 앱으로 마이그레이션하기 단원을 참조하십시오.

> **Important**
>
> 보안을 위해 개인 리포지토리가 있는 모든 앱에서 웹 미리 보기를 활성화할 수 있지만 공개 리포지토리가 있는 모든 앱에서는 활성화할 수 없습니다. Git 저장소가 공용인 경우 IAM 서비스 역할이 필요하지 않은 앱에 대해서만 미리 보기를 설정할 수 있습니다.

예를 들어 백엔드가 있는 앱과 WEB_COMPUTE 호스팅 플랫폼에 배포된 앱에는 IAM 서비스 역할이 필요합니다. 따라서 리포지토리가 퍼블릭인 경우 이러한 유형의 앱에 대해 웹 미리 보기를 활성화할 수 없습니다.
Amplify는 제3자가 앱의 IAM 역할 권한을 사용하여 실행되는 임의 코드를 제출하지 못하도록 이러한 제한을 적용합니다.

pull 요청의 웹 미리 보기를 활성화하려면

1. 호스팅을 선택한 다음 미리보기를 선택합니다.

   > **Note**
   >
   > 앱이 지속적 배포를 위해 설정되고 Git 리포지토리에 연결된 경우에만 앱 설정 메뉴에 미리 보기가 표시됩니다. 이러한 유형의 배포에 대한 지침은 기존 코드로 시작하기를 참조하십시오.

2. GitHub 리포지토리의 경우에만 다음을 수행하여 계정에 Amplify GitHub 앱을 설치하고 승인하십시오.

   a. 미리 보기를 활성화하려면 GitHub 앱 설치 창에서 앱 설치를 선택합니다. GitHub

   b. Amplify GitHub 앱을 구성하려는 GitHub 계정을 선택합니다.

   c. 계정에 대한 리포지토리 권한을 구성할 수 있는 페이지가 GitHub.com에서 열립니다.

   d. 다음 중 하나를 수행하십시오.

      - 모든 리포지토리에 설치를 적용하려면 모든 리포지토리를 선택합니다.
      - 선택한 특정 리포지토리로 설치를 제한하려면 리포지토리만 선택을 선택합니다. 선택한 리포지토리에 웹 미리 보기를 활성화하려는 앱의 리포지토리를 포함해야 합니다.

   e. 저장을 선택합니다.

3. 리포지토리의 미리 보기를 활성화한 후 Amplify 콘솔로 돌아가서 특정 분기에 대한 미리 보기를 활성화하십시오. 미리 보기 페이지의 목록에서 브랜치를 선택하고 설정 편집을 선택합니다.

4. 미리 보기 설정 관리 페이지에서 풀 요청 미리 보기를 켜십시오. 그 다음 확인을 선택합니다.

5. 풀스택 애플리케이션의 경우 다음 중 하나를 수행하십시오.

   - 모든 pull 요청에 대해 새 백엔드 환경을 생성을 선택하십시오. 이 옵션을 사용하면 프로덕션에 영향을 주지 않고 변경 사항을 테스트할 수 있습니다.
   - 이 브랜치에 대한 모든 pull 요청이 기존 환경을 가리키도록 설정을 선택합니다.

6. 확인을 선택합니다.

다음에 브랜치에 대한 pull 요청를 제출하면 Amplify는 PR을 빌드하여 미리 보기 URL에 배포합니다. pull 요청가 종료되면 미리 보기 URL이 삭제되고 pull 요청에 연결된 임시 백엔드 환경도 삭제됩니다. GitHub 리포지토리의 경우에만 계정의 풀 리퀘스트에서 직접 URL 미리보기에 액세스할 수 있습니다. GitHub

하위 도메인을 통한 웹 미리 보기 액세스

Amazon Route 53에서 관리하는 사용자 지정 도메인에 연결된 Amplify 앱의 하위 도메인을 통해 풀 요청에 대한 웹 미리 보기에 액세스할 수 있습니다. pull 요청가 종료되면 풀 요청과 관련된 브랜치와 하위 도메인이 자동으로 삭제됩니다. 이는 앱의 패턴 기반 기능 분기 배포를 설정한 후 웹 미리 보기의 기본 동작입니다. 자동 하위 도메인을 설정하는 지침은 Amazon Route 53 사용자 지정 도메인을 위한 자동 하위 도메인을 설정합니다. 단원을 참조하십시오.

Amplify 앱에 end-to-end 사이프러스 테스트 추가

Amplify 앱의 테스트 단계에서 end-to-end (E2E) 테스트를 실행하여 코드를 프로덕션으로 푸시하기 전에 회귀를 잡을 수 있습니다. 테스트 단계는 빌드 사양 YAML에서 구성할 수 있습니다. 현재는 빌드 중에 Cypress 테스트 프레임워크만 실행할 수 있습니다.

튜토리얼: Cypress로 테스트 설정 end-to-end

Cypress는 브라우저에서 E2E 테스트를 실행할 수 있는 JavaScript 기반 테스트 프레임워크입니다. E2E 테스트 설정 방법을 보여주는 자습서는 Amplify를 사용한 풀스택 CI/CD 배포를 위한 end-to-end Cypress 테스트 실행 블로그 게시물을 참조하십시오.

기존 Amplify 앱에 테스트 추가

Amplify 콘솔에서 앱의 빌드 설정을 업데이트하여 기존 앱에 Cypress 테스트를 추가할 수 있습니다. 빌드 사양 YAML에는 Amplify에서 빌드를 실행하는 데 사용할 빌드 명령 및 관련 설정 모음이 포함되어 있습니다. 이 `test` 단계를 사용하여 빌드 시 모든 테스트 명령을 실행할 수 있습니다. E2E 테스트의 경우 Amplify Hosting은 테스트용 UI 보고서를 생성할 수 있는 Cypress와의 긴밀한 통합을 제공합니다.

다음 목록에서는 테스트 설정 및 사용 방법에 대해 설명합니다.

테스트 전

Cypress 테스트를 실행하는 데 필요한 종속성을 설치합니다. Amplify Hosting은 mochawesome을 사용하여 보고서를 생성하고 테스트 결과를 확인하며 빌드 중에 로컬 호스트 서버를 설정하기 위해 대기합니다.

테스트

cypress 명령을 실행하여 mochawesome을 사용하는 테스트를 수행합니다.

테스트 후

출력 JSON에서 mochawesome 보고서가 생성됩니다. Yarn을 사용하는 경우 이 명령을 자동 모드에서 실행하여 mochawesome 보고서를 생성해야 한다는 점에 유의합니다. Yarn에는 다음 명령을 사용할 수 있습니다.

```
yarn run --silent mochawesome-merge cypress/report/mochawesome-report/
mochawesome*.json > cypress/report/mochawesome.json
```

artifacts>baseDirectory

테스트가 실행되는 디렉터리입니다.

아티팩트> configFilePath

생성된 테스트 보고서 데이터입니다.

artifacts>files

생성된 아티팩트(스크린샷 및 동영상)를 다운로드할 수 있습니다.

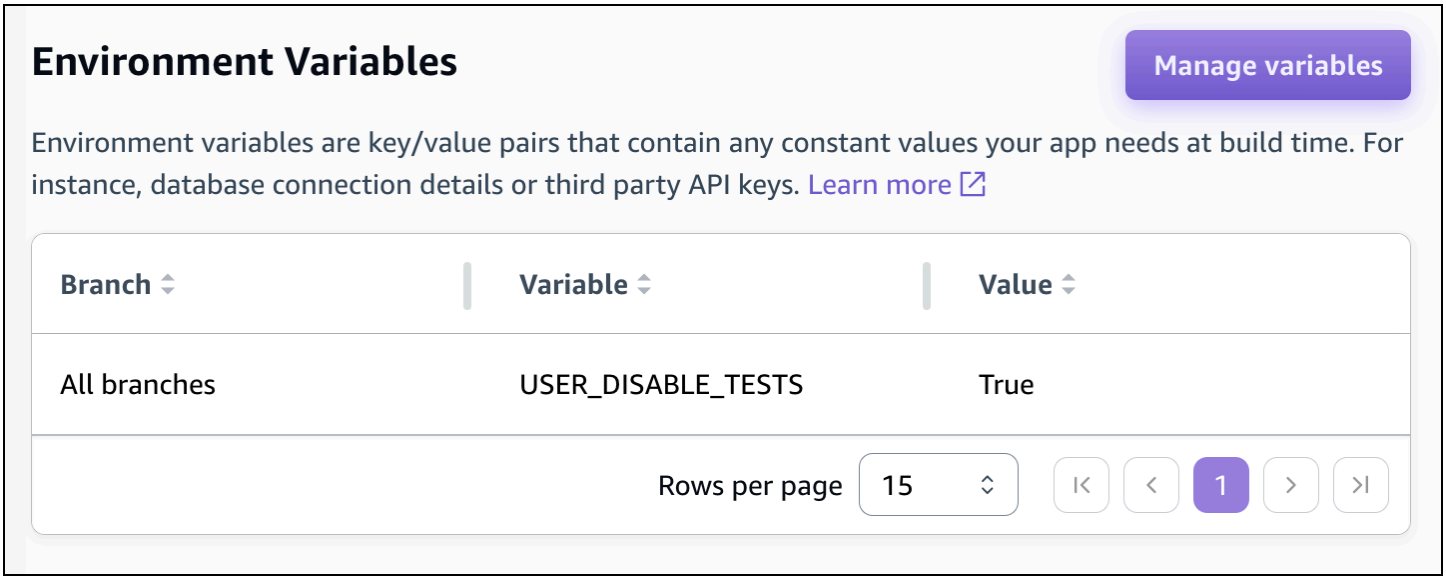
빌드 사양 `amplify.yml` 파일에서 발췌한 다음 예시는 앱에 Cypress 테스트를 추가하는 방법을 설명합니다.

```
test:
  phases:
    preTest:
      commands:
        - npm ci
        - npm install -g pm2
        - npm install -g wait-on
        - npm install mocha mochawesome mochawesome-merge mochawesome-report-generator
        - pm2 start npm -- start
        - wait-on http://localhost:3000
    test:
      commands:
        - 'npx cypress run --reporter mochawesome --reporter-options
 "reportDir=cypress/report/mochawesome-
report,overwrite=false,html=false,json=true,timestamp=mmddyyyy_HHMMss"'
    postTest:
      commands:
        - npx mochawesome-merge cypress/report/mochawesome-report/mochawesome*.json >
 cypress/report/mochawesome.json
        - pm2 kill
  artifacts:
    baseDirectory: cypress
    configFilePath: '**/mochawesome.json'
    files:
      - '**/*.png'
      - '**/*.mp4'
```

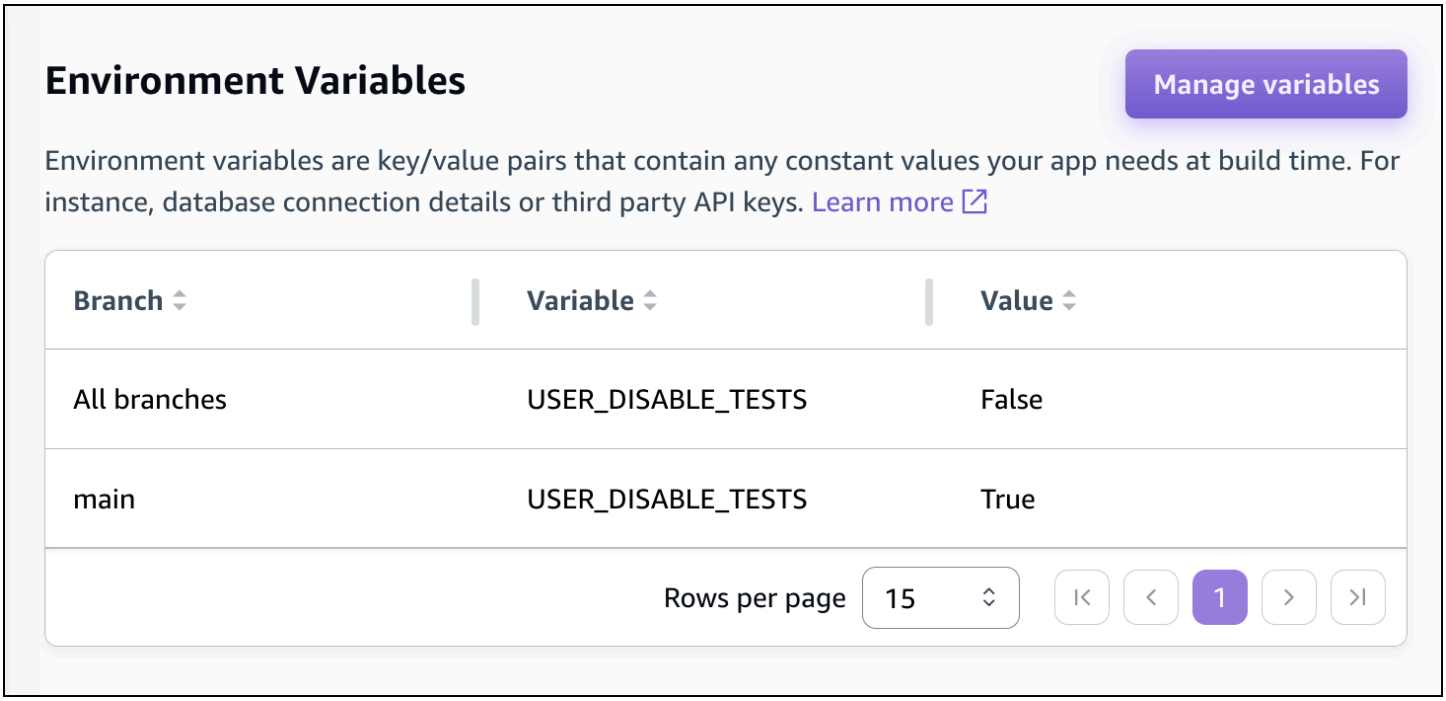
테스트 비활성화

테스트 구성을 `amplify.yml` 빌드 설정에 추가한 후에는 모든 브랜치의 모든 빌드에 대해 `test` 단계가 실행됩니다. 테스트 실행을 전역적으로 비활성화하거나 특정 브랜치에 대한 테스트만 실행하려는 경우, 빌드 설정을 수정하는 대신 USER_DISABLE_TESTS 환경 변수를 사용할 수 있습니다.

모든 브랜치에 대한 테스트를 전역적으로 비활성화하려면 모든 브랜치에 대해 값이 `true`인 USER_DISABLE_TESTS 환경 변수를 추가합니다. 다음 스크린샷은 모든 브랜치에 대해 테스트가 비활성화된 Amplify 콘솔의 환경 변수 섹션을 나타냅니다.



특정 브랜치에 대한 테스트를 비활성화하려면 모든 브랜치에 대해 값이 `false`인 USER_DISABLE_TESTS 환경 변수를 추가한 다음, 비활성화하려는 각 브랜치에 대해 값이 `true`인 재정의를 추가합니다. 다음 스크린샷에서는 기본 브랜치에 테스트가 비활성화되고 다른 모든 브랜치에서는 활성화되어 있습니다.



이 변수를 사용하여 테스트를 비활성화하면 빌드 중에 테스트 단계를 완전히 건너뜁니다. 테스트를 다시 활성화하려면 이 값을 `false`로 설정하거나 환경 변수를 삭제합니다.

리디렉션 사용

리디렉션을 사용하면 웹 서버가 하나의 URL에서 다른 URL로 경로를 다시 라우팅할 수 있습니다. 리디렉션을 사용하는 일반적인 이유는 다음과 같습니다. URL의 모양을 사용자 지정하고 링크가 끊어지지 않도록 하며 주소를 변경하지 않고 앱이나 사이트의 호스팅 위치를 이동하고 요청된 URL을 웹 앱에 필요한 형식으로 변경합니다.

리디렉션 유형

Amplify는 콘솔에서 다음과 같은 리디렉션 유형을 지원합니다.

영구적 리디렉션(301)

301 리디렉션은 웹 주소의 대상 주소를 지속적으로 변경하려는 것입니다. 원본 주소의 검색 엔진 순위 기록이 새 대상 주소에 적용됩니다. 리디렉션은 클라이언트 측에서 발생하므로 리디렉션 후에 브라우저 탐색 모음에 대상 주소가 표시됩니다.

301 리디렉션을 사용하는 일반적인 이유는 다음과 같습니다.

- 페이지 주소가 바뀔 때 링크가 끊어지지 않도록 합니다.
- 사용자가 주소에 흔히 하는 오타를 낼 때 링크가 끊어지지 않도록 합니다.

임시 리디렉션(302)

302 리디렉션은 웹 주소의 대상 주소를 임시로 변경하려는 것입니다. 원본 주소의 검색 엔진 순위 기록이 새 대상 주소에 적용되지 않습니다. 리디렉션은 클라이언트 측에서 발생하므로 리디렉션 후에 브라우저 탐색 모음에 대상 주소가 표시됩니다.

302 리디렉션을 사용하는 일반적인 이유는 다음과 같습니다.

- 원본 주소로 복구하는 동안 우회합니다.
- 사용자 인터페이스의 A/B 비교를 위한 테스트 페이지를 제공합니다.

> **Note**
>
> 앱이 예상치 못한 302 응답을 반환하는 경우, 해당 오류가 발생하는 이유는 앱의 리디렉션 및 사용자 지정 헤더 구성을 변경했기 때문일 수 있습니다. 이 문제를 해결하려면 사용자 지정 헤더가 유효한지 확인한 다음, 앱의 기본 404 다시 쓰기 규칙을 다시 활성화합니다.

다시 쓰기(200)

200 리디렉션(다시 쓰기)은 원본 주소에서 제공된 것처럼 대상 주소의 콘텐츠를 표시하기 위한 것입니다. 검색 엔진 순위 기록이 원본 주소에 계속 적용됩니다. 리디렉션은 서버 측에서 발생하므로 리디렉션 후에 브라우저 탐색 모음에 원래 주소가 표시됩니다. 200 리디렉션을 사용하는 일반적인 이유는 다음과 같습니다.

- 사이트의 주소를 변경하지 않고 전체 사이트를 새 호스팅 위치로 리디렉션합니다.
- 모든 트래픽을 단일 페이지 웹 앱(SPA)의 index.html 페이지로 리디렉션하여 클라이언트 측 라우터 기능으로 처리합니다.

찾을 수 없음(404)

404 리디렉션은 요청이 존재하지 않는 주소를 가리킬 때 발생합니다. 요청된 페이지 대신 404의 대상 주소 페이지가 표시됩니다. 404 리디렉션이 발생하는 일반적인 이유는 다음과 같습니다.

- 사용자가 잘못된 URL을 입력할 때 메시지 링크가 끊어지지 않도록 방지합니다.
- 웹 앱의 존재하지 않는 페이지에 대한 요청이 index.html 페이지를 향하도록 하여 클라이언트 측 라우터 기능으로 처리합니다.

리디렉션 생성 및 편집

Amplify 콘솔에서 앱에 대한 리디렉션을 생성하고 편집할 수 있습니다. 시작하기 전에 리디렉션의 각 부분에 대한 다음 정보가 필요합니다.

원본 주소

사용자가 요청한 주소입니다.

대상 주소

사용자가 보는 콘텐츠를 실제로 제공하는 주소입니다.

리디렉션 유형

유형에는 영구 리디렉션(301), 임시 리디렉션(302), 다시 쓰기(200) 또는 찾을 수 없음(404)이 포함됩니다.

두 글자로 된 국가 코드(선택 사항)

앱의 사용자 경험을 리전별로 분류하기 위해 포함할 수 있는 값입니다.

Amplify 콘솔에서 리디렉션을 생성하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 리디렉션을 생성하려는 앱을 선택합니다.
3. 탐색 창에서 호스팅을 선택한 다음 재작성 및 리디렉션을 선택합니다.
4. 재작성 및 리디렉션 페이지에서 리디렉션 관리를 선택합니다.
5. 리디렉션을 추가하는 절차는 규칙을 개별적으로 추가할지 아니면 일괄 편집을 수행할지에 따라 달라집니다.
   - 개별 리디렉션을 만들려면 재작성 추가를 선택합니다.
     a. 원본 주소에는 사용자가 요청한 원본 주소를 입력합니다.
     b. 대상 주소에는 사용자에게 콘텐츠를 렌더링할 대상 주소를 입력합니다.
     c. 유형에는 목록에서 리디렉션 유형을 선택합니다.
     d. (선택 사항) 국가 코드에는 두 글자로 된 국가 코드 조건을 입력합니다.
   - 리디렉션을 일괄 수정하려면 텍스트 편집기 열기를 선택합니다.
     - 재작성 및 리디렉션 JSON 편집기에서 리디렉션을 수동으로 추가 또는 업데이트합니다.
6. 저장을 선택합니다.

리디렉션 순서

리디렉션은 목록의 맨 위에서 아래로 실행됩니다. 이러한 순서가 의도한 효과를 발휘하는지 확인합니다. 예를 들어 다음과 같은 리디렉션 순서를 통해 /docs/ 아래의 특정 경로에 대한 모든 요청이 /documents/ 아래의 동일한 경로로 리디렉션합니다(단, /docs/specific-filename.html은 /documents/different-filename.html로 리디렉션합니다.

```
/docs/specific-filename.html /documents/different-filename.html 301
/docs/<*> /documents/<*>
```

다음 순서로 리디렉션하면 specific-filename.html의 different-filename.html로 리디렉션이 무시됩니다.

```
/docs/<*> /documents/<*>
/docs/specific-filename.html /documents/different-filename.html 301
```

쿼리 파라미터

쿼리 파라미터를 사용하여 URL 일치에 대한 제어를 강화할 수 있습니다. Amplify는 다음 예외의 경우를 제외하고 모든 쿼리 파라미터를 301 및 302 리디렉션을 위한 대상 경로로 전달합니다.

- 원본 주소에 특정 값으로 설정된 쿼리 문자열이 포함된 경우, Amplify는 쿼리 파라미터를 전달하지 않습니다. 이 경우, 리디렉션은 지정된 쿼리 값을 가진 대상 URL에 대한 요청에만 적용됩니다.
- 일치 규칙의 대상 주소에 쿼리 파라미터가 있는 경우, 쿼리 파라미터는 전달되지 않습니다. 예를 들어 리디렉션의 대상 주소가 `https://example-target.com?q=someParam`인 경우, 쿼리 파라미터는 전달되지 않습니다.

심플 리디렉션 및 다시 쓰기

이 섹션에는 일반적인 리디렉션 시나리오에 대한 예제 코드가 포함되어 있습니다.

> **Note**
>
> 일치하는 원래 주소 도메인에서는 대소문자를 구분하지 않습니다.

다음 예제 코드를 사용하여 특정 페이지를 새 주소로 영구적으로 리디렉션할 수 있습니다.

원본 주소	대상 주소	리디렉션 유형	국가 코드
`/original.html`	`/destination.html`	`permanent redirect (301)`	

JSON [{"source": "/original.html", "status": "301", "target": "/destination.html", "condition": null}]

다음 예제 코드를 사용하여 폴더 아래의 경로를 다른 폴더 아래의 동일한 경로로 리디렉션할 수 있습니다.

원본 주소	대상 주소	리디렉션 유형	국가 코드
`/docs/<*>`	`/documents/<*>`	`permanent redirect (301)`	

JSON [{"source": "/docs/<*>", "status": "301", "target": "/documents/<*>", "condition": null}]

다음 예제 코드를 사용하여 다시 쓰기로 모든 트래픽을 index.html로 리디렉션할 수 있습니다. 이 시나리오에서는 다시 쓰기를 통해 원본 주소에 도착했음을 사용자에게 알립니다.

원본 주소	대상 주소	리디렉션 유형	국가 코드
/<*>	/index.html	rewrite (200)	

JSON [{"source": "/<*>", "status": "200", "target": "/index.html", "condition": null}]

다음 예제 코드를 사용하여 사용자에게 표시되는 하위 도메인을 변경하는 데 다시 쓰기를 사용할 수 있습니다.

원본 주소	대상 주소	리디렉션 유형	국가 코드
https://mydomain.com	https://www.mydomain.com	rewrite (200)	

JSON [{"source": "https://mydomain.com", "status": "200", "target": "https://www.mydomain.com", "condition": null}]

다음 예제 코드를 사용하여 경로 접두사가 있는 다른 도메인으로 리디렉션할 수 있습니다.

원본 주소	대상 주소	리디렉션 유형	국가 코드
https://mydomain.com	https://www.mydomain.com/documents	temporary redirect (302)	

JSON [{"source": "https://mydomain.com", "status": "302", "target": "https://www.mydomain.com/documents/", "condition": null}]

다음 예제 코드를 사용하여 찾을 수 없는 폴더 아래의 경로를 사용자 지정 404 페이지로 리디렉션할 수 있습니다.

원본 주소	대상 주소	리디렉션 유형	국가 코드
/<*>	/404.html	not found (404)	

JSON [{"source": "/<*>", "status": "404", "target": "/404.html", "condition": null}]

단일 페이지 웹 앱(SPA)에 대한 리디렉션

대부분의 SPA 프레임워크는 HTML5 history.pushState()를 지원하여 서버 요청을 트리거하지 않고 브라우저 위치를 변경합니다. 이는 루트(또는 /index.html)에서 여정을 시작하지만 다른 페이지로 직접 이동하는 사용자에게는 적합하지 않습니다.

다음 예제에서는 정규식을 사용하여 정규식에 지정된 특정 파일 확장명을 제외한 모든 파일에 대해 index.html에 대한 200 다시 쓰기를 설정합니다.

원본 주소	대상 주소	리디렉션 유형	국가 코드
</^[^.]+$\|\.(?!(css\|gif\|ico\|jpg\|js\|png\|txt\|svg\|woff\|woff2\|ttf\|map\|json\|webp)$)([^.]+$)/>	/index.html	200	

JSON [{"source": "</^[^.]+$|\.(?!(css|gif|ico|jpg|js|png|txt|svg|woff|woff2|ttf|map|json|webp)$)([^.]+$)/>", "status": "200", "target": "/index.html", "condition": null}]

역방향 프록시 다시 쓰기

다음 예제에서는 다른 위치의 프록시 콘텐츠에 대해 다시 쓰기를 사용하여 사용자에게 도메인이 변경되지 않은 것처럼 표시합니다.

원본 주소	대상 주소	리디렉션 유형	국가 코드
/images/<*>	https://images.otherdomain.com/<*>	rewrite (200)	

JSON [{"source": "/images/<*>", "status": "200", "target": "https://images.otherdomain.com/<*>", "condition": null}]

후행 슬래시 및 클린 URL

Hugo와 같은 정적 사이트 생성기는 about.html 대신 about과 같은 깔끔한 URL 구조를 만들기 위해 index.html(/about/index.html)이 있는 페이지 디렉터리를 생성합니다. Amplify는 필요한 경우, 후행 슬래시를 추가하여 자동으로 클린 URL을 생성합니다. 아래 표는 다양한 시나리오를 하이라이트합니다.

브라우저의 사용자 입력	검색 주소창의 URL	제공된 문서
/about	/about	/about.html
/about (when about.html returns 404)	/about/	/about/index.html
/about/	/about/	/about/index.html

자리 표시자

다음 예제 코드를 사용하여 폴더 구조의 경로를 다른 폴더의 일치하는 구조로 리디렉션할 수 있습니다.

원본 주소	대상 주소	리디렉션 유형	국가 코드
/docs/<year>/<month>/<date>/<itemid>	/documents/<year>/<month>/<date>/<itemid>	permanent redirect (301)	

JSON [{"source": "/docs/<year>/<month>/<date>/<itemid>", "status": "301", "target": "/documents/<year>/<month>/<date>/<itemid>", "condition": null}]

쿼리 문자열 및 경로 파라미터

다음 예제 코드를 사용하여 원본 주소의 쿼리 문자열 요소 값과 이름이 일치하는 폴더로 경로를 리디렉션할 수 있습니다.

원본 주소	대상 주소	리디렉션 유형	국가 코드
`/docs?id=<my-blog-id-value`	`/documents/<my-blog-post-id-value>`	`permanent redirect (301)`	

JSON [{"source": "/docs?id=<my-blog-id-value>", "status": "301", "target": "/documents/<my-blog-id-value>", "condition": null}]

> **Note**
>
> Amplify는 301 및 302 리디렉션에 대한 대상 경로로 모든 쿼리 문자열 파라미터를 전달합니다. 그러나 이 예제에서 볼 수 있듯이 특정 값으로 설정된 쿼리 문자열이 원본 주소에 포함된 경우, Amplify는 쿼리 파라미터를 전달하지 않습니다. 이 경우, 리디렉션은 지정된 쿼리 값 `id`을(를) 가진 대상 주소로 보내는 요청에만 적용됩니다.

다음 예제 코드를 사용하여 폴더 구조의 특정 수준에서 찾을 수 없는 모든 경로를 지정된 폴더의 index.html로 리디렉션할 수 있습니다.

원본 주소	대상 주소	리디렉션 유형	국가 코드
`/documents/<folder>/<child-folder>/<grand-child-folder>`	`/documents/index.html`	`not found (404)`	

JSON [{"source": "/documents/<x>/<y>/<z>", "status": "404", "target": "/documents/index.html", "condition": null}]

리전 기반 리디렉션

다음 예제 코드를 사용하여 리전을 기반으로 요청을 리디렉션할 수 있습니다.

원본 주소	대상 주소	리디렉션 유형	국가 코드
/documents	/documents/us/	temporary redirect (302)	<US>

JSON [{"source": "/documents", "status": "302", "target": "/documents/us/", "condition": "<US>"}]

리디렉션 및 재작성의 와일드카드 표현식

리디렉션 또는 재작성에 대해 원래 주소의 와일드카드 표현식<*>, 를 사용할 수 있습니다. 표현식은 원래 주소 끝에 배치해야 하며 고유해야 합니다. Amplify는 와일드카드 표현식이 두 개 이상 포함된 원래 주소를 무시하거나 다른 위치에 사용합니다.

다음은 와일드카드 표현식을 사용한 유효한 리디렉션의 예입니다.

원본 주소	대상 주소	리디렉션 유형	국가 코드
/docs/<*>	/documents/<*>	permanent redirect (301)	

다음 두 예제는 와일드카드 표현식을 사용한 잘못된 리디렉션을 보여줍니다.

원본 주소	대상 주소	리디렉션 유형	국가 코드
/docs/<*>/content	/documents/<*>/content	permanent redirect (301)	
/docs/<*>/content/<*>	/documents/<*>/content/<*>	permanent redirect (301)	

브랜치 액세스 제한

출시되지 않은 기능을 사용하는 경우 기능 분기를 암호로 보호하여 특정 사용자에 대한 액세스를 제한할 수 있습니다. 브랜치에 액세스 제어가 설정된 경우, 브랜치 URL에 액세스하려고 하면 사용자에게 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다.

개별 지점 또는 전 세계 모든 연결 지점에 적용되는 비밀번호를 설정할 수 있습니다. 지사 및 글로벌 수준에서 액세스 제어를 활성화한 경우 지사 수준 암호가 글로벌 (응용 프로그램) 수준 암호보다 우선합니다.

기능 브랜치에 암호를 설정하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 기능 브랜치 암호를 설정하려는 앱을 선택하십시오.
3. 탐색 창에서 호스팅을 선택한 다음 액세스 제어를 선택합니다.
4. 액세스 제어 설정 섹션에서 액세스 관리를 선택합니다.
5. 액세스 제어 관리 페이지에서 다음 중 하나를 수행하십시오.
   - 연결된 모든 지점에 적용되는 사용자 이름과 비밀번호를 설정하려면
     - 모든 지점의 액세스 관리를 켜십시오. 예를 들어, 메인 브랜치, 개발 브랜치, 피처 브랜치가 연결되어 있는 경우 모든 브랜치에 동일한 사용자 이름과 비밀번호를 적용할 수 있습니다.
   - 개별 브랜치에 사용자 이름과 비밀번호를 적용하려면
     a. 모든 브랜치에 대한 액세스 관리를 끕니다.
     b. 관리하려는 지점을 찾으세요. 액세스 설정에서 제한적-비밀번호 필요를 선택합니다.
     c. 사용자 이름에 사용자 이름을 입력합니다.
     d. 암호에는 암호를 입력합니다.
   - 저장을 선택합니다.
6. 서버 측 렌더링(SSR)앱의 액세스 제어를 관리하는 경우, Git 리포지토리에서 새 빌드를 수행하여 앱을 재배포하십시오. 이 단계는 Amplify를 활성화하여 액세스 제어 설정을 적용하는 데 필요합니다.

환경 변수

환경 변수란 Amplify Hosting에서 사용할 수 있도록 애플리케이션 설정에 추가할 수 있는 키-값 페어입니다. 모범 사례로 환경 변수를 사용하여 이러한 애플리케이션 구성 데이터를 노출할 수 있습니다. 추가하는 모든 환경 변수는 불법 액세스를 방지하기 위해 암호화됩니다.

Amplify에서는 접두사가 `AWS` 있는 환경 변수를 만들 수 없습니다. 이 접두사는 Amplify 내부용으로만 사용됩니다.

> **Important**
>
> 환경 변수를 사용하여 암호를 저장하지 않도록 합니다. AWS Systems Manager 파라미터 저장소를 사용하여 만든 환경 시크릿에 시크릿을 저장합니다. 자세한 정보는 환경 암호을 참조하세요.

Amplify 환경 변수

다음 환경 변수는 Amplify 콘솔 내에서 기본적으로 액세스할 수 있습니다.

변수 이름	설명	예시 값
_BUILD_TIMEOUT	빌드 타임아웃 기간(분)	`30`
_LIVE_UPDATES	도구가 최신 버전으로 업그레이드됩니다.	`[{"name":"Amplify CLI","pkg":"@aws-amplify/cli","type":"npm","version":"latest"}]`
USER_DISABLE_TESTS	빌드 중에 테스트 단계를 생략합니다. 앱의 모든 브랜치 또는 특정 브랜치에 대한 테스트를 비활성화할 수 있습니다. 이 환경 변수는 빌드 단계에서 테스트를 수행하는 앱에 사용됩니다. 이 변수 설정에 대한 자	`true`

변수 이름	설명	예시 값
	세한 내용을 알아보려면 테스트 비활성화을 참조하십시오.	
AWS_APP_ID	현재 빌드의 앱 ID	`abcd1234`
AWS_BRANCH	현재 빌드의 브랜치 이름	`main`, `develop`, `beta`, `v2.0`
AWS_BRANCH_ARN	현재 빌드의 브랜치 Amazon 리소스 이름(ARN)	`aws:arn:amplify:us-west-2:123456789012:appname/branch/...`
AWS_CLONE_URL	git 리포지토리 콘텐츠를 가져오기 위해 사용된 복제 URL	`git@github.com:<user-name>/<repo-name>.git`
AWS_COMMIT_ID	현재 빌드의 커밋 ID 다시 빌드하기 위한 "HEAD"	`abcd1234`
AWS_JOB_ID	현재 빌드의 작업 ID입니다. 여기에는 제로 패딩('0')이 포함되므로 길이가 항상 동일합니다.	`0000000001`
AWS_PULL_REQUEST_ID	풀 리퀘스트 웹 프리뷰 빌드의 풀 리퀘스트 ID입니다. 리포지토리 AWS CodeCommit 공급자로 사용할 때는 이 환경 변수를 사용할 수 없습니다.	1
AWS_PULL_REQUEST_SOURCE_BRANCH	Amplify 콘솔에서 애플리케이션 브랜치에 제출되는 풀 리퀘스트 미리보기의 기능 브랜치 이름입니다.	`featureA`

변수 이름	설명	예시 값
AWS_PULL_REQUEST_DESTINATION_BRANCH	기능 브랜치 풀 요청이 제출되는 Amplify 콘솔의 애플리케이션 브랜치 이름입니다.	`main`
AMPLIFY_AMAZON_CLIENT_ID	Amazon 클라이언트 ID	`123456`
AMPLIFY_AMAZON_CLIENT_SECRET	Amazon 클라이언트 암호	`example123456`
AMPLIFY_FACEBOOK_CLIENT_ID	Facebook 클라이언트 ID	`123456`
AMPLIFY_FACEBOOK_CLIENT_SECRET	Facebook 클라이언트 암호	`example123456`
AMPLIFY_GOOGLE_CLIENT_ID	Google 클라이언트 ID	`123456`
AMPLIFY_GOOGLE_CLIENT_SECRET	Google 클라이언트 암호	`example123456`
AMPLIFY_DIFF_DEPLOY	diff 기반 프런트엔드 배포를 활성화 또는 비활성화합니다. 자세한 정보는 diff 기반 프런트엔드 빌드 및 배포 활성화 또는 비활성화을 참조하세요.	`true`
AMPLIFY_DIFF_DEPLOY_ROOT	리포지토리의 루트를 기준으로 diff 기반 프런트엔드 배포를 비교하는 데 사용할 경로입니다.	`dist`

변수 이름	설명	예시 값
AMPLIFY_DIFF_BACKEND	diff 기반 백엔드 빌드를 활성화 또는 비활성화합니다. 이는 1세대 앱에만 적용됩니다. 자세한 정보는 1세대 앱의 diff 기반 백엔드 빌드를 활성화 또는 비활성화합니다. 섹션을 참조하십시오.	`true`
AMPLIFY_BACKEND_PULL_ONLY	Amplify는 이 환경 변수를 관리합니다. 이는 1세대 앱에만 적용됩니다. 자세한 정보는 다른 백엔드를 가리키도록 기존 프론트엔드를 편집합니다. 섹션을 참조하십시오.	`true`
AMPLIFY_BACKEND_APP_ID	Amplify는 이 환경 변수를 관리합니다. 이는 1세대 앱에만 적용됩니다. 자세한 정보는 다른 백엔드를 가리키도록 기존 프론트엔드를 편집합니다. 섹션을 참조하십시오.	`abcd1234`
AMPLIFY_SKIP_BACKEND_BUILD	빌드 사양에 백엔드 섹션이 없고 백엔드 빌드를 비활성화하려면 이 환경 변수를 `true`으(로) 설정합니다. 이는 1세대 앱에만 적용됩니다.	`true`
AMPLIFY_ENABLE_DEBUG_OUTPUT	로그에 스택 `true` 트레이스를 인쇄하려면 이 변수를 로 설정합니다. 이는 백엔드 빌드 오류를 디버깅하는 데 유용합니다.	`true`
AMPLIFY_MONOREPO_APP_ROOT	리포지토리의 루트를 기준으로 모노레포 앱의 앱 루트를 지정하는 데 사용할 경로입니다.	`apps/react-app`

변수 이름	설명	예시 값
AMPLIFY_USERPOOL_ID	인증을 위해 가져온 Amazon Cognito 사용자 풀의 ID	`us-west-2_example`
AMPLIFY_WEBCLIENT_ID	웹 애플리케이션에서 사용할 앱 클라이언트의 ID AMPLIFY_USERPOOL_ID 환경 변수로 지정된 Amazon Cognito 사용자 풀에 액세스할 수 있도록 앱 클라이언트를 구성해야 합니다.	`123456`
AMPLIFY_NATIVECLIENT_ID	네이티브 애플리케이션에서 사용할 앱 클라이언트의 ID AMPLIFY_USERPOOL_ID 환경 변수로 지정된 Amazon Cognito 사용자 풀에 액세스할 수 있도록 앱 클라이언트를 구성해야 합니다.	`123456`
AMPLIFY_IDENTITYPOOL_ID	Amazon Cognito 자격 증명 풀의 ID	`example-identitypool-id`
AMPLIFY_PERMISSIONS_BOUNDARY_ARN	Amplify에서 생성한 모든 IAM 역할에 적용되는 권한 경계로 사용할 IAM 정책의 ARN입니다. 자세한 내용은 Amplify 생성 역할의 IAM 권한 경계를 참조하십시오.	`arn:aws:iam::123456789012:policy/example-policy`
AMPLIFY_DESTRUCTIVE_UPDATES	잠재적으로 데이터 손실을 일으킬 수 있는 스키마 작업으로 GraphQL API를 업데이트할 수 있도록 하려면 이 환경 변수를 true로 설정합니다.	`true`

> **Note**
>
> `AMPLIFY_AMAZON_CLIENT_ID`및 `AMPLIFY_AMAZON_CLIENT_SECRET` 환경 변수는 OAuth 토큰이지 AWS 액세스 키와 비밀 키가 아닙니다.

환경 변수 설정

Amplify 콘솔에서 애플리케이션의 환경 변수를 설정하려면 다음 지침을 따르십시오.

> **Note**
>
> 앱이 연속 배포되도록 설정하고 git 리포지토리에 연결된 경우에만 Amplify 콘솔의 앱 설정 메뉴에 환경 변수가 표시됩니다. 이러한 유형의 배포에 대한 지침은 기존 코드로 시작하기를 참조하십시오.

환경 변수를 설정하는 방법

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. Amplify 콘솔에서 호스팅을 선택한 다음 환경 변수를 선택합니다.
3. 환경 변수 페이지에서 변수 관리를 선택합니다.
4. 변수에 키를 입력합니다. 값에 값을 입력합니다. 기본적으로 Amplify는 환경 변수를 모든 브랜치에 적용하므로 새로운 브랜치에 연결할 때 변수를 다시 입력할 필요가 없습니다.
5. (선택 사항) 브랜치에 맞게 환경 변수를 사용자 지정하려면 다음과 같이 브랜치 재정의를 추가합니다.
   a. 작업을 선택한 다음, 변수 재정의 추가를 선택합니다.
   b. 이제 브랜치별 환경 변수 집합을 갖게 되었습니다.
6. 저장을 선택합니다.

빌드 시 환경 변수에 액세스

빌드 중 환경 변수에 액세스하려면 빌드 명령에 환경 변수를 포함하도록 빌드 설정을 편집하십시오.

빌드 구성의 각 명령은 Bash 쉘 내에서 실행됩니다. Bash에서 환경 변수를 사용하는 방법에 대한 자세한 내용은 GNU Bash 매뉴얼의 쉘 확장을 참조하십시오.

환경 변수를 포함하도록 빌드 설정을 편집하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. Amplify 콘솔에서 호스팅을 선택한 다음 빌드 설정을 선택합니다.
3. 앱 빌드 사양 섹션에서 편집을 선택합니다.
4. 환경 변수를 빌드 명령에 추가합니다. 이제 다음 빌드 동안 환경 변수에 액세스할 수 있어야 합니다. 이 예제는 npm의 동작(BUILD_ENV)을 변경하고 나중에 사용할 수 있도록 외부 서비스용 API 토큰(TWITCH_CLIENT_ID)을 환경 파일에 추가합니다.

```
build:
  commands:
    - npm run build:$BUILD_ENV
    - echo "TWITCH_CLIENT_ID=$TWITCH_CLIENT_ID" >> backend/.env
```

5. 저장을 선택합니다.

환경 변수가 서버 측 런타임에 액세스할 수 있도록 만들기

Next.js 서버 구성 요소는 기본적으로 앱의 환경 변수에 액세스할 수 없습니다. 이는 애플리케이션이 빌드 단계에서 사용하는 환경 변수에 저장된 모든 암호를 보호하기 위한 것입니다.

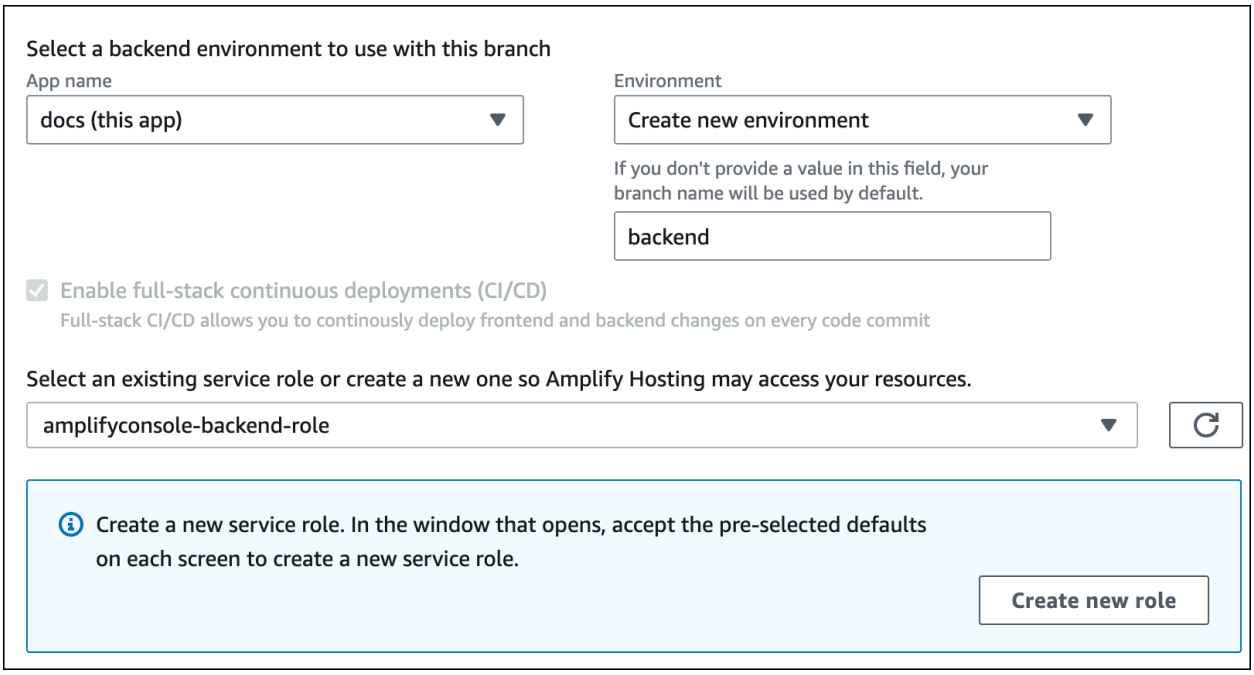
특정 환경 변수를 Next.js에 액세스할 수 있게 하려면 Next.js가 인식하는 환경 파일에 환경 변수를 설정하도록 Amplify 빌드 사양 파일을 수정해야 합니다. 이를 통해 Amplify는 애플리케이션을 빌드하기 전에 환경 변수를 로드할 수 있습니다. 빌드 사양 수정에 대한 자세한 내용은 빌드 명령 섹션에서 환경 변수를 추가하는 방법의 예를 참조하십시오.

소셜 로그인을 위한 인증 파라미터를 사용하여 새 백엔드 환경 생성

브랜치를 앱에 연결하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 브랜치를 앱에 연결하는 절차는 브랜치를 새 앱과 기존 앱 중 어디에 연결하는지에 따라 달라집니다.
   - 브랜치를 새 앱에 연결
     a. 빌드 설정 페이지에서 이 브랜치에 사용할 백엔드 환경 선택 섹션을 찾습니다. 환경에서 새 환경 생성을 선택하고 백엔드 환경의 이름을 입력합니다. 다음 스크린샷은 빌드 설정

페이지의 이 브랜치에 사용할 백엔드 환경 선택 섹션에 백엔드 환경 이름을 **backend**로 입력한 모습입니다.



b. 빌드 설정 페이지에서 고급 설정 섹션을 확장하고 소셜 로그인 키에 대한 환경 변수를 추가합니다. 예를 들어 **AMPLIFY_FACEBOOK_CLIENT_SECRET**은(는) 유효한 환경 변수입니다. 기본적으로 사용할 수 있는 Amplify 시스템 환경 변수 목록은 Amplify 환경 변수의 표를 참조하십시오.

- 브랜치를 기존 앱에 연결

a. 새 브랜치를 기존 앱에 연결하는 경우 브랜치를 연결하기 전에 소셜 로그인 환경 변수를 설정합니다. 탐색 창에서 앱 설정, 환경 변수를 선택합니다.

b. 환경 변수 섹션에서 변수 관리를 선택합니다.

c. 변수 관리 섹션에서 변수 추가를 선택합니다.

d. 변수(키) 에 클라이언트 ID를 입력합니다. 값에 클라이언트 암호를 입력합니다.

e. 저장을 선택합니다.

프런트엔드 프레임워크 환경 변수

자체 환경 변수를 지원하는 프런트엔드 프레임워크로 앱을 개발하는 경우 이러한 변수는 Amplify 콘솔에 구성하는 환경 변수와 동일하지 않다는 점을 이해하는 것이 중요합니다. 예를 들어 React(접두사: REACT_APP)와 Gatsby(접두사: GATSBY)는 해당 프레임워크가 프런트엔드 프로덕션 빌드에 자동으

로 번들링하는 런타임 환경 변수를 만들 수 있습니다. 이러한 환경 변수를 사용하여 값을 저장하는 데 따르는 영향을 이해하려면 사용 중인 프런트엔드 프레임워크 설명서를 참조하십시오.

API 키와 같이 중요한 값을 이러한 프런트엔드 프레임워크 접두사가 붙은 환경 변수 내에 저장하는 것은 모범 사례가 아니므로 권장하지 않습니다. 이러한 목적으로 Amplify의 빌드 시간 환경 변수를 사용하는 예는 빌드 시 환경 변수에 액세스 섹션을 참조하십시오.

환경 암호

환경 암호는 환경 변수와 비슷하지만 암호화할 수 있는 AWS Systems Manager (SSM) 파라미터 저장소 키 값 쌍입니다. Amplify에 대한 'Apple 프라이빗 키로 로그인'과 같은 일부 값은 암호화되어야 합니다.

환경 암호 설정

콘솔을 사용하여 Amplify 앱의 환경 암호를 설정하려면 다음 지침을 따르십시오. AWS Systems Manager

환경 암호를 설정하려면

1. 에 AWS Management Console 로그인하고 AWS Systems Manager 콘솔을 엽니다.
2. 탐색 창에서 애플리케이션 관리를 선택한 다음, Parameter Store를 선택합니다.
3. AWS Systems Manager Parameter Store 페이지에서 파라미터 생성을 선택합니다.
4. 파라미터 생성 페이지의 파라미터 세부 정보 섹션에서 다음을 수행합니다.
   a. 이름에 파라미터를 **/amplify/{your_app_id}/{your_backend_environment_name}/{your_parameter_name}** 형식으로 입력합니다.
   b. 유형(Type)에서 SecureString를 선택합니다.
   c. KMS 키 소스의 경우 내 현재 계정을 선택하여 계정의 기본 키를 사용합니다.
   d. 값 에는 암호화할 암호 값을 입력합니다.
5. 파라미터 생성을 선택합니다.

> **Note**
>
> Amplify는 특정 환경 빌드용 `/amplify/{your_app_id}/{your_backend_environment_name}` 키에만 액세스할 수 있습니다. Amplify가 값을 AWS KMS key 해독할 수 있도록 하려면 기본값을 지정해야 합니다.

환경 암호에 액세스

빌드 중에 환경 암호에 액세스하는 것은 환경 암호가 JSON 문자열로 `process.env.secrets`에 저장된다는 점을 제외하면 환경 변수에 액세스하는 것과 비슷합니다.

Amplify 환경 암호

Systems Manager 파라미터를 `/amplify/{your_app_id}/{your_backend_environment_name}/AMPLIFY_SIWA_CLIENT_ID` 형식으로 지정합니다.

Amplify 콘솔 내에서 기본적으로 액세스할 수 있는 다음 환경 암호를 사용할 수 있습니다.

변수 이름	설명	예시 값
AMPLIFY_SIWA_CLIENT_ID	Apple 클라이언트 ID로 로그인	`com.yourapp.auth`
AMPLIFY_SIWA_TEAM_ID	Apple 팀 ID로 로그인	`ABCD123`
AMPLIFY_SIWA_KEY_ID	Apple 키 ID로 로그인	`ABCD123`
AMPLIFY_SIWA_PRIVATE_KEY	Apple 프라이빗 키로 로그인	-----프라이빗 키 시작----- ****..... -----프라이빗 키 종료-----

사용자 지정 헤더

사용자 지정 HTTP 헤더를 사용하면 모든 HTTP 응답에 대해 헤더를 지정할 수 있습니다. 응답 헤더는 디버깅, 보안 및 정보 제공을 목적으로 사용할 수 있습니다. Amplify 콘솔에서 헤더를 지정하거나 앱 `customHttp.yml` 파일을 다운로드 및 편집한 후 프로젝트의 루트 디렉터리에 저장하여 헤더를 지정할 수 있습니다. 자세한 절차는 사용자 지정 헤더 설정 섹션을 참조하십시오.

이전에는 에서 빌드 사양 (buildspec) 을 편집하거나 `amplify.yml` 파일을 다운로드 및 업데이트한 다음 프로젝트의 루트 디렉터리에 저장하는 방식으로 앱에 대한 사용자 지정 HTTP 헤더를 지정했습니다. AWS Management Console 이러한 방식으로 지정된 사용자 지정 헤더는 buildspec 및 `amplify.yml` 파일 외부로 마이그레이션해야 합니다. 지침은 사용자 지정 헤더 마이그레이션 섹션을 참조하십시오.

사용자 지정 헤더 YAML 형식

다음 YAML 형식을 사용하여 사용자 지정 헤더를 지정합니다.

```
customHeaders:
  - pattern: '*.json'
    headers:
    - key: 'custom-header-name-1'
      value: 'custom-header-value-1'
    - key: 'custom-header-name-2'
      value: 'custom-header-value-2'
  - pattern: '/path/*'
    headers:
    - key: 'custom-header-name-1'
      value: 'custom-header-value-2'
```

모노레포의 경우, 다음 YAML 형식을 사용합니다.

```
applications:
  - appRoot: app1
    customHeaders:
    - pattern: '**/*'
      headers:
      - key: 'custom-header-name-1'
        value: 'custom-header-value-1'
  - appRoot: app2
    customHeaders:
```

```
    - pattern: '/path/*.json'
      headers:
      - key: 'custom-header-name-2'
        value: 'custom-header-value-2'
```

앱에 사용자 지정 헤더를 추가할 때 다음에 대해 고유한 값을 지정해야 합니다.

패턴

사용자 지정 헤더는 패턴과 일치하는 모든 URL 파일 경로에 적용됩니다.

헤더

파일 패턴과 일치하는 헤더를 정의합니다.

키

사용자 지정 헤더의 이름입니다.

값

사용자 지정 헤더의 값입니다.

HTTP 헤더에 대한 자세한 내용은 Mozilla의 HTTP 헤더 목록을 참조하십시오.

사용자 지정 헤더 설정

Amplify 앱의 사용자 지정 HTTP 헤더를 지정하는 방법에는 두 가지가 있습니다. Amplify 콘솔에서 헤더를 지정하거나 앱 `customHttp.yml` 파일을 다운로드 및 편집한 후 프로젝트의 루트 디렉터리에 저장하여 헤더를 지정할 수 있습니다.

앱의 사용자 지정 헤더를 설정하고 콘솔에 저장하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 사용자 지정 헤더를 설정할 앱을 선택합니다.
3. 탐색 창에서 호스팅을 선택한 다음 사용자 지정 헤더를 선택합니다.
4. 사용자 지정 헤더 페이지에서 편집을 선택합니다.
5. 사용자 지정 헤더 편집 창에서 사용자 지정 헤더 YAML 형식을 사용하여 사용자 지정 헤더 정보를 입력합니다.

   a. `pattern`에 일치시킬 패턴을 입력합니다.

b. `key`에 사용자 지정 헤더의 이름을 입력합니다.

c. `value`에 사용자 지정 헤더의 값을 입력합니다.

6. 저장을 선택합니다.
7. 앱을 재배포하여 새 사용자 지정 헤더를 적용합니다.
   - CI/CD 앱의 경우, 배포할 브랜치로 이동한 다음 이 버전 재배포를 선택합니다. Git 리포지토리에서 새 빌드를 수행할 수도 있습니다.
   - 수동 배포 앱의 경우, Amplify 콘솔에서 앱을 다시 배포합니다.

앱의 사용자 지정 헤더를 설정하고 리포지토리의 루트에 저장하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 사용자 지정 헤더를 설정할 앱을 선택합니다.
3. 탐색 창에서 호스팅을 선택한 다음 사용자 지정 헤더를 선택합니다.
4. 사용자 지정 헤더 페이지에서 YML 다운로드를 선택합니다.
5. 다운로드한 `customHttp.yml` 파일을 선택한 코드 편집기에서 열고 사용자 지정 헤더 YAML 형식을 사용하여 사용자 지정 헤더에 대한 정보를 입력합니다.

   a. `pattern`에 일치시킬 패턴을 입력합니다.

   b. `key`에 사용자 지정 헤더의 이름을 입력합니다.

   c. `value`에 사용자 지정 헤더의 값을 입력합니다.

6. 편집된 `customHttp.yml` 파일을 프로젝트의 루트 디렉터리에 저장합니다. 모노레포로 작업하는 경우, 리포지토리의 루트에 `customHttp.yml` 파일을 저장합니다.
7. 앱을 재배포하여 새 사용자 지정 헤더를 적용합니다.
   - CI/CD 앱의 경우, 새 `customHttp.yml` 파일이 포함된 Git 리포지토리에서 새 빌드를 수행합니다.
   - 수동 배포 앱의 경우, Amplify 콘솔에서 앱을 다시 배포하고 업로드하는 아티팩트와 함께 새 `customHttp.yml` 파일을 포함합니다.

> **Note**
>
> `customHttp.yml`파일에 설정되고 앱의 루트 디렉터리에 배포된 사용자 지정 헤더는 Amplify 콘솔의 사용자 지정 헤더 섹션에 정의된 사용자 지정 헤더보다 우선합니다.

사용자 지정 헤더 마이그레이션

이전에는 Amplify 콘솔에서 buildspec을 편집하거나 `amplify.yml` 파일을 다운로드 및 업데이트하고 프로젝트의 루트 디렉터리에 저장하여 앱에 대한 사용자 지정 HTTP 헤더를 지정했습니다. 사용자 지정 헤더를 buildspec 및 `amplify.yml` 파일 외부로 마이그레이션하는 것이 좋습니다.

Amplify 콘솔의 사용자 지정 헤더 섹션에서 또는 파일을 다운로드하고 편집하여 사용자 지정 헤더를 지정합니다. `customHttp.yml`

Amplify 콘솔에 저장된 사용자 지정 헤더를 마이그레이션하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 사용자 지정 헤더 마이그레이션을 수행할 앱을 선택합니다.
3. 탐색 창에서 호스팅, 빌드 설정을 선택합니다. 앱 빌드 사양 섹션에서 앱의 buildspec을 검토할 수 있습니다.
4. 다운로드를 선택하여 현재 buildspec의 사본을 저장합니다. 설정을 복구해야 하는 경우, 나중에 이 사본을 참조할 수 있습니다.
5. 다운로드가 완료되면 편집을 선택합니다.
6. 나중에 9단계에서 사용하게 되므로 파일의 사용자 지정 헤더 정보를 기록해 둡니다. 편집 창에서 파일의 사용자 지정 헤더를 삭제하고 저장을 선택합니다.
7. 탐색 창에서 호스팅, 사용자 지정 헤더를 선택합니다.
8. 사용자 지정 헤더 페이지에서 편집을 선택합니다.
9. 사용자 지정 헤더 편집 창에서 6단계에서 삭제한 사용자 지정 헤더의 정보를 입력합니다.
10. 저장을 선택합니다.
11. 새 사용자 지정 헤더를 적용할 브랜치를 재배포합니다.

사용자 지정 헤더를 amplify.yml에서 customHttp.yml로 마이그레이션하려면

1. 앱의 루트 디렉터리에 현재 배포된 `amplify.yml` 파일로 이동합니다.
2. 원하는 코드 편집기에서 `amplify.yml` 파일을 엽니다.
3. 나중에 8단계에서 사용하게 되므로 파일의 사용자 지정 헤더 정보를 기록해 둡니다. 파일의 사용자 지정 헤더를 삭제합니다. 파일을 저장하고 닫습니다.
4. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
5. 사용자 지정 헤더를 설정할 앱을 선택합니다.

6. 탐색 창에서 호스팅, 사용자 지정 헤더를 선택합니다.
7. 사용자 지정 헤더 페이지에서 다운로드를 선택합니다.
8. 다운로드한 `customHttp.yml` 파일을 원하는 코드 편집기에서 열고 3단계의 `amplify.yml`에서 삭제한 사용자 지정 헤더의 정보를 입력합니다.
9. 편집된 `customHttp.yml` 파일을 프로젝트의 루트 디렉터리에 저장합니다. 모노레포로 작업하는 경우, 리포지토리의 루트에 파일을 저장합니다.
10. 앱을 재배포하여 새 사용자 지정 헤더를 적용합니다.
    - CI/CD 앱의 경우, 새 `customHttp.yml` 파일이 포함된 Git 리포지토리에서 새 빌드를 수행합니다.
    - 수동 배포 앱의 경우, Amplify 콘솔에서 앱을 다시 배포하고 업로드하는 아티팩트와 함께 새 `customHttp.yml` 파일을 포함합니다.

> **Note**
>
> `customHttp.yml`파일에 설정되고 앱의 루트 디렉터리에 배포된 사용자 지정 헤더는 Amplify 콘솔의 사용자 지정 헤더 섹션에 정의된 사용자 지정 헤더보다 우선합니다.

모노레포 사용자 지정 헤더

모노레포 앱에 대한 사용자 지정 헤더를 지정할 때는 다음 설정 요구 사항에 유의합니다.

- 모노레포에는 특정 YAML 형식이 있습니다. 사용자 지정 헤더 YAML 형식 섹션에서 올바른 구문을 참조하십시오.
- Amplify 콘솔의 사용자 지정 헤더 섹션을 사용하여 단일 저장소의 애플리케이션에 대한 사용자 지정 헤더를 지정할 수 있습니다. 새 사용자 지정 헤더를 적용하려면 애플리케이션을 재배포해야 합니다.
- 콘솔을 사용하는 대신 모노레포 앱에 대한 사용자 지정 헤더를 `customHttp.yml` 파일에 지정할 수 있습니다. `customHttp.yml` 파일을 리포지토리의 루트에 저장한 다음, 애플리케이션을 재배포하여 새 사용자 지정 헤더를 적용해야 합니다. `customHttp.yml`파일에 지정된 사용자 지정 헤더는 Amplify 콘솔의 사용자 지정 헤더 섹션을 사용하여 지정된 모든 사용자 지정 헤더보다 우선합니다.

보안 헤더 예제

사용자 지정 보안 헤더는 HTTPS 실행, XSS 공격 예방 및 클릭재킹으로부터 브라우저 보호를 활성화합니다. 다음 YAML 구문을 사용하여 앱에 사용자 지정 보안 헤더를 적용할 수 있습니다.

```
customHeaders:
  - pattern: '**'
    headers:
      - key: 'Strict-Transport-Security'
        value: 'max-age=31536000; includeSubDomains'
      - key: 'X-Frame-Options'
        value: 'SAMEORIGIN'
      - key: 'X-XSS-Protection'
        value: '1; mode=block'
      - key: 'X-Content-Type-Options'
        value: 'nosniff'
      - key: 'Content-Security-Policy'
        value: "default-src 'self'"
```

사용자 지정 캐시 제어 헤더

Amplify로 호스팅되는 앱은 사용자가 정의한 사용자 지정 `Cache-Control` 헤더로 재정의하지 않는 한 오리진에서 전송한 헤더를 준수합니다. Amplify는 상태 코드가 포함된 성공적인 응답에 대해 Cache-Control 사용자 지정 헤더만 적용합니다. `200 OK` 이렇게 하면 오류 응답이 캐시되어 동일한 요청을 하는 다른 사용자에게 제공되는 것을 방지할 수 있습니다.

앱의 성능 및 배포 가용성을 더 잘 제어하도록 `s-maxage` 디렉티브를 수동으로 조정할 수 있습니다. 예를 들어 콘텐츠가 엣지에 캐시되는 시간을 늘리려면 `s-maxage`을(를) 기본값인 600초(10분)보다 긴 값으로 업데이트하여 TTL(Time to Live)을 수동으로 늘릴 수 있습니다.

`s-maxage`에 사용자 지정 값을 지정하려면 다음 YAML 형식을 사용합니다. 이 예제에서는 관련 콘텐츠를 3,600초(1시간) 동안 엣지에 캐시된 상태로 유지합니다.

```
customHeaders:
  - pattern: '/img/*'
    headers:
      - key: 'Cache-Control'
        value: 's-maxage=3600'
```

헤더로 애플리케이션 성능을 제어하는 방법에 대한 자세한 내용은 헤더를 사용하여 캐시 기간 제어을 참조하십시오.

수신 웹후크

Amplify 콘솔에서 수신 웹후크를 설정하여 Git 리포지토리에 코드를 커밋하지 않고 빌드를 시작할 수 있습니다. 웹후크 트리거는 콘텐츠 변경에 관한 빌드를 트리거하거나 Zapier와 같은 서비스를 사용하여 일상적인 빌드를 트리거하기 위해 헤드리스 CMS 도구(예: Contentful 또는 GraphCMS)와 함께 사용될 수 있습니다.

수신 웹후크를 만들려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 웹후크를 생성할 앱을 선택합니다.
3. 탐색 창에서 호스팅을 선택한 다음 빌드 설정을 선택합니다.
4. 빌드 설정 페이지에서 수신 웹후크 섹션으로 스크롤하여 웹후크 생성을 선택합니다.
5. 웹후크 생성 대화 상자에서 다음 작업을 수행하십시오.
   a. 웹후크 이름에는 웹후크 이름을 입력합니다.
   b. 브랜치를 빌드하려면 들어오는 웹후크 요청에 빌드할 브랜치를 선택합니다.
   c. 웹후크 생성을 선택합니다.
6. 수신 웹후크 섹션에서 다음 중 하나를 수행하십시오.
   - 웹후크 URL을 복사하여 헤드리스 CMS 도구 또는 기타 서비스에 제공하여 빌드를 트리거합니다.
   - 터미널 창에서 curl 명령을 실행하여 새 빌드를 트리거합니다.

모니터링

AWS Amplify Amazon을 통해 지표를 CloudWatch 내보내고 앱에 대한 요청에 대한 세부 정보가 포함된 액세스 로그를 제공합니다. 이 섹션의 항목를 통해 이러한 지표와 로그를 사용하여 앱을 모니터링하는 방법을 알아보세요.

주제

를 통한 모니터링 CloudWatch

AWS Amplify CloudWatchAmazon과 통합되어 Amplify 애플리케이션의 메트릭을 거의 실시간으로 모니터링할 수 있습니다. 지표가 설정한 임계값을 초과할 경우, 알림을 보내는 경보를 생성할 수 있습니다. CloudWatch 서비스 작동 방식에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

지표

Amplify는 `AWS/AmplifyHosting` 네임스페이스에서 6가지 CloudWatch 메트릭을 지원하여 앱의 트래픽, 오류, 데이터 전송 및 지연 시간을 모니터링합니다. 이러한 지표는 1분 간격으로 집계됩니다. CloudWatch 모니터링 지표는 무료이며 CloudWatch 서비스 할당량에 포함되지 않습니다.

사용 가능한 모든 통계가 모든 지표에 적용되는 것은 아닙니다. 다음 표에는 각 지표에 대한 설명에 가장 관련성이 높은 통계가 나열되어 있습니다.

지표	설명
요청	앱에서 수신한 최종 사용자 요청의 총 수. 가장 관련성이 높은 통계는 `Sum`입니다. `Sum` 통계를 사용하여 총 요청 수를 확인할 수 있습니다.
BytesDownloaded	`GET`,`HEAD`, 요청에 대해 시청자가 앱을 통해 전송(다운로드)한 총 데이터 양(바이트)입니다. `OPTIONS`

지표	설명
	가장 관련성이 높은 통계는 Sum입니다.
BytesUploaded	POST및 PUT 요청을 사용하여 앱으로 전송(업로드)된 총 데이터 양(바이트) 가장 관련성이 높은 통계는 Sum입니다.
4XXErrors	HTTP 상태 코드 400-499 범위에서 오류를 반환한 요청 수. 가장 관련성이 높은 통계는 Sum입니다. Sum 통계를 사용하여 오류의 총 발생 횟수를 가져옵니다.
5XXErrors	HTTP 상태 코드 500-599 범위에서 오류를 반환한 요청 수. 가장 관련성이 높은 통계는 Sum입니다. Sum 통계를 사용하여 오류의 총 발생 횟수를 가져옵니다.
지연 시간	첫 바이트까지의 시간(초). Amplify Hosting에서 요청을 수신할 때부터 네트워크에 응답을 반환할 때까지의 총 시간입니다. 여기에는 응답이 뷰어 장치에 도달하는 데 발생한 네트워크 지연 시간은 포함되지 않습니다. 가장 관련성이 높은 통계는Average, Maximum, Minimum, p10, p50, p90, p95, p100.입니다. Average 통계를 사용하여 예상 지연 시간을 평가합니다.

Amplify는 다음과 같은 CloudWatch 미터 치수를 제공합니다.

측정기준	설명
앱	지표 데이터는 앱에서 제공합니다.
AWS 계정	지표 데이터는 의 모든 앱에서 제공됩니다. AWS 계정

https://console.aws.amazon.com/cloudwatch/ AWS Management Console 에서 CloudWatch 메트릭에 액세스할 수 있습니다. 또는 다음 절차를 따라 Amplify 콘솔에서 지표에 액세스할 수 있습니다.

Amplify 콘솔에서 지표에 액세스하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 앱 지표를 확인할 서비스를 선택합니다.
3. 탐색 창에서 앱 설정, 모니터링을 선택합니다.
4. 모니터링 페이지에서 지표를 선택합니다.

경보

Amplify 콘솔에서 특정 기준이 충족될 때 알림을 보내는 CloudWatch 경보를 생성할 수 있습니다. 경보는 단일 CloudWatch 지표를 감시하고 지표가 지정된 평가 기간 수의 임계값을 위반할 경우 Amazon Simple Notification Service 알림을 보냅니다.

CloudWatch콘솔에서 또는 API를 사용하여 지표 수학 식을 사용하는 고급 경보를 생성할 수 있습니다. CloudWatch 예를 들어, 4XXErrors의 비율이 세 기간 동안 연속으로 15%를 초과한 경우, 알림을 보내는 경보를 생성할 수 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 지표 수학 식을 기반으로 CloudWatch 경보 생성을 참조하십시오.

경보에는 표준 CloudWatch 요금이 적용됩니다. 자세한 내용은 Amazon CloudWatch 요금을 참조하십시오.

Amplify 콘솔에서 다음 절차에 따라 경고를 만듭니다.

Amplify 지표에 대한 CloudWatch 경보를 만들려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 경보를 설정할 앱을 선택합니다.

3. 탐색 창에서 앱 설정, 모니터링을 선택합니다.
4. 모니터링 페이지에서 경보를 선택합니다.
5. 경보 생성을 선택하세요.
6. 경보 생성 창에서 다음과 같이 경보를 구성합니다.

   a. 지표의 경우, 목록에서 모니터링할 지표의 이름을 선택합니다.

   b. 경보 이름에 경보 이름을 입력합니다. 예를 들어 요청을 모니터링하는 경우, 경보 이름을 지정할 수 **`HighTraffic`** 있습니다. 이름은 ASCII 문자만 포함해야 합니다.

   c. 알림 설정에 다음 중 하나를 실시합니다.

      - i. 새 Amazon SNS 주제를 설정하려면 새로 만들기 를 선택합니다.
        ii. 이메일 주소에는 알림 수신자의 이메일 주소를 입력합니다.
        iii. 새 이메일 주소 추가를 선택하여 수신자를 더 추가합니다.
      - i. Amazon SNS 주제를 재사용하려면 기존 항목 을 선택합니다.
        ii. SNS 항목에 대해서는 목록에서 기존 Amazon SNS 항목의 이름을 선택합니다.

   d. 메트릭의 통계 예시에서 알람 조건을 다음과 같이 설정하세요.

      i. 지표가 임계값보다 크거나, 작거나, 같아야 하는지 여부를 지정합니다.
      ii. 임곗값을 지정합니다.
      iii. 경보가 트리거되려면 경보 상태에 있어야 하는 연속 평가 기간 수를 지정합니다.
      iv. 평가 간격 시간의 길이를 지정합니다.

   e. 경보 생성을 선택하세요.

> **Note**
>
> 지정한 각 Amazon SNS 수신자는 AWS 알림으로부터 확인 이메일을 수신합니다. 이메일에는 수신자가 구독을 확인하고 알림을 받기 위해 따라야 하는 링크가 포함되어 있습니다.

SSR CloudWatch 앱용 아마존 로그

Amplify는 Next.js 런타임에 대한 정보를 사용자의 아마존 CloudWatch 로그에 전송합니다. AWS 계정 SSR 앱 배포 시 앱은 Amplify가 사용자를 대신하여 다른 서비스를 호출할 때 맡는 IAM 서비스 역할을 필요로 합니다. Amplify Hosting 컴퓨팅이 자동으로 서비스 역할을 생성하도록 허용하거나 사용자가 생성한 역할을 지정할 수 있습니다.

Amplify에서 IAM 역할을 생성하도록 허용하면 해당 역할에는 이미 로그를 생성할 권한이 있습니다. CloudWatch IAM 역할을 직접 생성하는 경우 Amplify가 Amazon CloudWatch Logs에 액세스할 수 있도록 하려면 정책에 다음 권한을 추가해야 합니다.

```
logs:CreateLogStream
logs:CreateLogGroup
logs:DescribeLogGroups
logs:PutLogEvents
```

서비스 역할에 대한 자세한 내용은 서비스 역할 추가 섹션을 참조하세요. 서버측 렌더링된 앱 배포에 대한 자세한 내용은 Amplify Hosting을 통해 서버 측 렌더링 앱 배포 단원을 참조하세요.

액세스 로그

Amplify는 Amplify에서 호스팅하는 모든 앱에 대한 액세스 로그를 저장합니다. 액세스 로그는 호스팅된 앱에 대해 이루어진 요청에 대한 정보를 포함합니다. Amplify는 앱을 삭제할 때까지 앱에 대한 모든 액세스 로그를 보관합니다. 앱에 대한 모든 액세스 로그는 Amplify 콘솔에서 사용할 수 있습니다. 하지만 액세스 로그에 대한 각 개별 요청은 지정한 2주 기간으로 제한됩니다.

Amplify는 고객 간 CloudFront 배포를 재사용하지 않습니다. Amplify는 CloudFront 배포를 미리 생성하므로 새 앱을 배포할 때 배포가 CloudFront 생성될 때까지 기다릴 필요가 없습니다. 이러한 배포는 Amplify 앱에 할당되기 전에 봇으로부터 트래픽을 수신할 수 있습니다. 하지만 할당되기 전에는 항상 찾을 수 없음으로 응답하도록 구성되어 있습니다. 앱 액세스 로그에 앱을 만들기 전 일정 기간의 항목이 포함되어 있는 경우, 이러한 항목은 이 활동과 관련이 있습니다.

> **Important**
>
> 모든 요청을 완전히 살펴보기 보다는 콘텐츠에 대한 요청 특성을 이해하는 데 로그를 사용하는 것이 좋습니다. Amplify는 최대 효과에 기초하여 액세스 로그를 전송합니다. 요청에 따라서는 실제로 요청이 처리된 지 한참 후에 로그 레코드가 전송되거나 아예 전송되지 않을 수도 있습니다. 액세스 로그에서 로그 항목을 생략하면 액세스 로그의 항목 수가 AWS 청구 및 사용 보고서에 나타나는 사용량과 일치하지 않습니다.

다음 절차를 사용하여 앱의 액세스 로그를 검색하십시오.

액세스 로그를 보기

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.

2. 액세스 로그를 보려는 앱을 선택합니다.
3. 탐색 창에서 앱 설정, 모니터링을 선택합니다.
4. 모니터링 페이지에서 액세스 로그를 선택합니다.
5. 시간 범위 편집을 선택합니다.
6. 시간 범위 편집 창에서 시작 날짜로 로그를 검색할 2주 간격 중 첫 번째 요일을 지정합니다. 시작 시간에서 로그 검색을 시작할 첫날의 시간을 선택합니다.
7. Amplify 콘솔은 액세스 로그 섹션에 지정된 시간 범위의 로그를 표시합니다. 다운로드를 선택하여 로그를 CSV 형식으로 저장합니다.

액세스 로그 분석

Amazon S3 버킷에 CSV 파일을 저장하여 액세스 로그를 분석할 수 있습니다. 액세스 로그를 분석하는 한 가지 방법은 Athena를 사용하는 것입니다. Athena는 서비스의 데이터를 분석하는 데 도움이 되는 대화형 쿼리 서비스입니다. AWS 여기의 step-by-step 지침에 따라 테이블을 생성할 수 있습니다. 테이블이 생성되면 다음과 같이 데이터를 쿼리할 수 있습니다.

```
SELECT SUM(bytes) AS total_bytes
FROM logs
WHERE "date" BETWEEN DATE '2018-06-09' AND DATE '2018-06-11'
LIMIT 100;
```

빌드에 대한 이메일 알림

빌드가 성공하거나 실패할 때 이해 관계자나 팀 구성원에게 알리도록 AWS Amplify 앱에 대한 이메일 알림을 설정할 수 있습니다. Amplify Hosting은 계정에서 Amazon Simple Notification Service(SNS)항목을 생성하고 이를 사용하여 이메일 알림을 구성합니다. Amplify 앱의 모든 분기 또는 특정 분기에 적용되도록 알림을 구성할 수 있습니다.

이메일 알림을 설정하세요.

다음 절차를 사용하여 Amplify 앱의 모든 분기 또는 특정 분기에 대해 이메일 알림을 설정합니다.

Amplify 앱의 이메일 알림을 설정하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 이메일 알림을 설정하려는 앱을 선택합니다.
3. 탐색 창에서 호스팅, 빌드 알림을 선택합니다. 빌드 알림 페이지에서 알림 관리를 선택합니다.
4. 알림 관리 페이지에서 새로 추가를 선택합니다.
5. 다음 중 하나를 수행하십시오.
   - 단일 브랜치에 알림을 보내려면 이메일에 알림을 보낼 이메일 주소를 입력합니다. 브랜치의 경우, 알림을 보낼 브랜치 이름을 선택합니다.
   - 연결된 모든 브랜치에 알림을 보내려면 이메일에 알림을 보낼 이메일 주소를 입력합니다. 브랜치의 경우, 모든 브랜치를 선택합니다.
6. 저장을 선택합니다.

사용자 지정 빌드 이미지 및 라이브 패키지 업데이트

주제

사용자 지정 빌드 이미지

사용자 지정 빌드 이미지를 사용하여 Amplify 앱에 사용자 지정된 빌드 환경을 제공할 수 있습니다. Amplify 컨테이너를 사용하여 빌드 중에 설치하는 데 오랜 시간이 걸리는 특정 종속성이 있는 경우, 자체 도커 이미지를 생성하여 빌드 중에 참조할 수 있습니다. 이미지는 Amazon Elastic Container Registry Public에 호스팅될 수 있습니다.

> **Note**
>
> 빌드 설정은 앱이 지속적 배포를 위해 설정되고 git 리포지토리에 연결된 경우에만 Amplify 콘솔의 호스팅 메뉴에 표시됩니다. 이러한 유형의 배포에 대한 지침은 기존 코드로 시작하기를 참조하십시오.

사용자 지정 빌드 이미지 요구 사항

사용자 지정 빌드 이미지가 Amplify 빌드 이미지로 작동하려면 다음 요구 사항을 충족해야 합니다.

1. GNU C Library(glibc)를 지원하는 Linux 배포판(예: Amazon Linux)을 지원하며 x86-64 아키텍처용으로 컴파일되었습니다.
2. cURL: 사용자 지정 이미지를 시작하는 경우 빌드 러너를 컨테이너로 다운로드하므로 cURL이 있어야 합니다. 이 종속성이 누락된 경우, 빌드 러너가 출력을 생성할 수 없으므로 빌드는 출력 없이 즉시 실패합니다.
3. Git: Git 리포지토리를 복제하려면 Git를 이미지에 설치해야 합니다. 이 종속성이 누락된 경우, 리포지토리 복제 단계는 실패합니다.
4. OpenSSH: 리포지토리를 안전하게 복제하려면 OpenSSH는 빌드 중에 일시적으로 SSH 키를 설정해야 합니다. OpenSSH 패키지는 빌드 러너가 이를 수행하는 데 필요한 명령을 제공합니다.
5. Bash 및 Bourne 쉘: 이 두 가지 유틸리티는 빌드할 때 명령을 실행하는 데 사용합니다. 설치하지 않으면 시작하기도 전에 빌드가 실패할 수 있습니다.

6. Node.JS+NPM: Amazon의 빌드 러너에서는 노드를 설치하지 않습니다. 대신 이미지에 설치된 노드와 NPM을 사용합니다. 이는 NPM 패키지 또는 노드 특정 명령을 요구하는 빌드에만 필수 항목입니다. 하지만 이미 보유하고 있는 경우 Amplify 빌드 러너에서 이러한 도구를 사용하여 빌드 실행을 개선할 수 있으니 설치하는 것이 좋습니다. Amplify의 패키지 재정의 기능에서는 Hugo에 재정의를 설정할 때 NPM을 사용하여 Hugo 확장 패키지를 설치합니다.

다음과 같은 패키지는 필수는 아니나 설치하는 것이 좋습니다.

1. NVM (Node Version Manager): Node의 다른 버전을 처리해야 한다면 이 버전 관리자를 설치하는 것이 좋습니다. 재정의를 설정하면 각 빌드 전에 Amplify의 패키지 재정의 기능에서 NVM을 사용하여 Node.js 버전을 변경합니다.
2. Wget: 빌드 프로세스 도중에 Amplify에서 Wget 유틸리티를 사용하여 파일을 다운로드할 수 있습니다. 사용자 지정 이미지에 설치하는 것이 좋습니다.
3. Tar: 빌드 프로세스 도중에 Amplify에서 Tar 유틸리티를 사용하여 다운로드된 파일의 압축을 해제할 수 있습니다. 사용자 지정 이미지에 설치하는 것이 좋습니다.

사용자 지정 빌드 이미지 구성

Amazon ECR에서 호스팅되는 사용자 지정 빌드 이미지 구성하기

1. 도커 이미지를 사용하여 Amazon ECR 퍼블릭 리포지토리를 설정하려면 Amazon ECR 퍼블릭 사용 설명서의 시작하기를 참조하십시오.
2. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
3. 사용자 지정 빌드 이미지를 구성하려는 앱을 선택합니다.
4. 탐색 창에서 호스팅, 빌드 설정을 선택합니다.
5. 빌드 설정 페이지의 빌드 이미지 설정 섹션에서 편집을 선택합니다.
6. 빌드 이미지 설정 편집 페이지에서 빌드 이미지 메뉴를 펼치고 사용자 지정 빌드 이미지를 선택합니다.
7. 1단계에서 만든 Amazon ECR 퍼블릭 리포지토리 이름을 입력합니다. 여기에서 빌드 이미지가 호스팅됩니다. 예를 들어 리포지토리 이름이 ecr-examplerepo인 경우, **`public.ecr.aws/xxxxxxxx/ecr-examplerepo`**를 입력합니다.
8. 저장을 선택합니다.

라이브 패키지 업데이트

라이브 패키지 업데이트를 사용하면 Amplify 기본 빌드 이미지에 사용할 패키지 및 종속성 버전을 지정할 수 있습니다. 기본 빌드 이미지에는 사전 설치된 여러 패키지 및 종속성이 부수됩니다(예: Hugo, Amplify CLI, Yarn 등). 라이브 패키지 업데이트를 사용하면 이러한 종속성을 재정의하고 특정 버전을 지정할 수 있으며, 또는 최신 버전이 설치되어 있는지 항상 확인할 수 있습니다.

라이브 패키지 업데이트가 활성화되어 있는 경우, 빌드가 실행되기 전에 먼저 빌드 러너가 특정 종속성을 업데이트(또는 다운그레이드)합니다. 이를 통해 빌드 시간은 종속성 업데이트에 소요되는 시간에 비례하여 증가하지만 애플리케이션 빌드에 동일한 종속성 버전이 사용되도록 확인할 수 있는 장점이 있습니다.

> **Warning**
>
> Node.js 버전을 최신으로 설정하면 빌드가 실패합니다. 대신에 `18`, `21.5` 또는 `v0.1.2`처럼 정확한 Node.js 버전을 지정해야 합니다.

라이브 패키지 업데이트 구성

라이브 패키지 업데이트를 구성하려면

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 라이브 패키지 업데이트를 구성할 앱을 선택합니다.
3. 탐색 창에서 호스팅, 빌드 설정을 선택합니다.
4. 빌드 설정 페이지의 빌드 이미지 설정 섹션에서 편집을 선택합니다.
5. 빌드 이미지 설정 편집 페이지의 라이브 패키지 업데이트 목록에서 새로 추가를 선택합니다.
6. Package의 경우 재정의할 종속성을 선택합니다.
7. 버전의 경우, 기본값을 최신으로 유지하거나 종속 항목의 특정 버전을 입력하십시오. 최신이 사용될 경우, 종속성은 사용 가능한 최신 버전으로 항상 업그레이드됩니다.
8. 저장을 선택합니다.

서비스 역할 추가

Amplify에는 프런트엔드와 함께 백엔드 리소스를 배포할 수 있는 권한이 필요합니다. 서비스 역할을 사용하여 이를 수행합니다. 서비스 역할은 사용자를 대신하여 다른 서비스를 호출할 때 Amplify가 맡는 AWS Identity and Access Management (IAM) 역할입니다. 이 가이드에서는 계정 관리 권한이 있고 Amplify 애플리케이션이 백엔드를 배포, 생성 및 관리하는 데 필요한 리소스에 대한 직접 액세스를 명시적으로 허용하는 Amplify 서비스 역할을 생성하는 방법을 알아봅니다.

서비스 역할 생성

서비스 역할을 생성하는 방법

1. IAM 콘솔을 열고 왼쪽 탐색 모음에서 역할을 선택한 다음, 역할 생성을 선택합니다.
2. 신뢰할 수 있는 엔터티 선택 페이지에서 AWS 서비스를 선택합니다. 사용 사례의 경우 Amplify를 선택하고 다음을 선택합니다.
3. 권한 추가 페이지에서 다음을 선택합니다.
4. 이름, 보기 및 만들기 페이지에서 역할 이름에 의미 있는 이름 (예**AmplifyConsoleServiceRole-AmplifyRole**:) 을 입력합니다.
5. 모든 기본값을 적용하고 역할 만들기를 선택합니다.
6. Amplify 콘솔로 돌아가서 앱에 역할을 연결합니다.
   - 새 앱을 배포하는 중인 경우
     a. 서비스 역할 목록을 새로 고칩니다.
     b. 방금 생성한 역할을 선택합니다. 이 예시에서는 다음과 AmplifyConsoleServiceRole 같아야 합니다. AmplifyRole
     c. 다음을 선택하고 단계에 따라 앱 배포를 완료합니다.
   - 기존 앱이 있는 경우
     a. 탐색 창에서 앱 설정을 선택한 다음 일반 설정을 선택합니다.
     b. 일반 설정 페이지에서 편집을 선택합니다.
     c. 일반 설정 편집 페이지의 서비스 역할 목록에서 방금 만든 역할을 선택합니다.
     d. 저장을 선택합니다.
7. 이제 Amplify 콘솔에 앱의 백엔드 리소스를 배포할 권한이 있습니다.

혼동된 대리자 방지

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. 자세한 정보는 교차 서비스 혼동된 대리인 방지을 참조하세요.

현재 `Amplify-Backend Deployment` 서비스 역할에 대한 기본 신뢰 정책은 `aws:SourceArn` 및 `aws:SourceAccount` 글로벌 조건 컨텍스트 키를 적용하여 혼동된 대리자를 방지합니다. 하지만 이전에 `Amplify-Backend Deployment` 역할을 계정에 생성한 경우에는 역할의 신뢰 정책을 업데이트하여 이러한 조건을 추가함으로써 혼동된 대리자를 방지할 수 있습니다.

다음 예제를 사용하여 계정의 앱에 대한 액세스를 제한할 수 있습니다. 예제의 지역 및 애플리케이션 ID를 자체 정보로 바꾸십시오.

```
"Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:amplify:us-east-1:123456789012:apps/*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
```

를 사용하여 역할의 신뢰 정책을 편집하는 방법에 대한 지침은 IAM 사용 설명서의 역할 (콘솔) 수정을 참조하십시오. AWS Management Console

앱 성능 관리

Amplify의 기본 호스팅 아키텍처는 호스팅 성능과 배포 가용성 간의 균형을 최적화합니다. 대부분의 고객에게는 기본 아키텍처를 사용하는 것이 좋습니다.

앱 성능을 더 세밀하게 제어해야 하는 경우 콘텐츠를 콘텐츠 전송 네트워크 (CDN) 에지에 더 긴 기간 동안 캐시된 상태로 유지함으로써 호스팅 성능을 최적화하도록 HTTP `Cache-Control` 헤더를 수동으로 설정할 수 있습니다.

헤더를 사용하여 캐시 기간 제어

HTTP `Cache-Control` `max-age` 헤더와 `s-maxage` 지시문은 앱의 콘텐츠 캐싱 기간에 영향을 줍니다. `max-age` 명령을 사용하면 오리진 서버에서 콘텐츠를 새로 고치기 전에 캐시에 유지하려는 시간(초)을 브라우저에 알려 줍니다. `s-maxage` 명령을 사용하면 `max-age`을(를) 재정의하고 오리진 서버에서 콘텐츠를 새로 고치기 전에 CDN 엣지에 보관하려는 시간(초)을 지정할 수 있습니다.

Amplify로 호스팅되는 앱은 사용자가 정의한 사용자 지정 `Cache-Control` 헤더로 재정의하지 않는 한 오리진에서 전송한 헤더를 준수합니다. Amplify는 상태 코드가 포함된 성공적인 응답에 대해 `Cache-Control` 사용자 지정 헤더만 적용합니다. `200 OK` 이렇게 하면 오류 응답이 캐시되어 동일한 요청을 하는 다른 사용자에게 제공되는 것을 방지할 수 있습니다.

앱의 성능 및 배포 가용성을 더 잘 제어하도록 `s-maxage` 디렉티브를 수동으로 조정할 수 있습니다. 예를 들어, 콘텐츠가 엣지에 캐시되는 시간을 늘리려면 `s-maxage`을(를) 기본값인 600초(10분)보다 긴 값으로 업데이트하여 TTL(Time to Live)을 수동으로 늘릴 수 있습니다.

Amplify 콘솔의 사용자 지정 헤더 섹션에서 앱의 사용자 지정 헤더를 정의할 수 있습니다. YAML 형식의 예는 사용자 지정 캐시 제어 헤더 단원을 참조하십시오.

앱 성능을 높이기 위한 cache-control 헤더 설정

다음 절차를 사용하여 콘텐츠를 CDN 엣지에 24시간 동안 캐시된 상태로 유지하도록 `s-maxage` 지침을 설정하십시오.

사용자 지정 헤더를 설정하려면 cache-control

1. 에 AWS Management Console 로그인하고 Amplify 콘솔을 엽니다.
2. 사용자 지정 헤더를 설정할 앱을 선택합니다.
3. 탐색 창에서 호스팅, 사용자 지정 헤더를 선택합니다.

4. 사용자 지정 헤더 페이지에서 편집을 선택합니다.
5. 사용자 지정 헤더 편집 창에서 다음과 같이 사용자 지정 헤더의 정보를 입력합니다.

   a. 의 `pattern` 경우 모든 경로에 **`**/*`** 를 입력합니다.
   b. `key`에 **`cache-control`**를 입력합니다.
   c. `value`에 **`s-maxage=86400`**를 입력합니다.
6. 저장을 선택합니다.
7. 앱을 재배포하여 새 사용자 지정 헤더를 적용합니다.

AWS CloudTrail를 사용하여 Amplify API 호출 로깅

AWS Amplify는 사용자, 역할, 또는 Amplify의 AWS 서비스가 수행한 작업에 대한 레코드를 제공하는 서비스인 AWS CloudTrail과 통합됩니다. CloudTrail은 Amplify에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 Amplify 콘솔로부터의 호출과 Amplify API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하면 Amplify 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail이 수집하는 정보를 사용하여 Amplify에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

CloudTrail의 Amplify 정보

CloudTrail은 AWS 계정에서 기본적으로 활성화되어 있습니다. Amplify에서 어떤 활동이 발생하는 경우 해당 활동이 이벤트 기록(Event history)의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서에서 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

Amplify에 대한 이벤트를 포함하여 AWS 계정의 이벤트의 지속적인 레코드의 경우, 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 또는 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 AWS CloudTrail User Guide의 다음 섹션을 참조하세요.

- AWS 계정에 대한 추적 생성
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 지역에서 CloudTrail 로그 파일 받기 및 여러 계정에서 CloudTrail 로그 파일 받기

모든 Amplify 작업은 CloudTrail에 기록되며 AWS Amplify Console API 참조, AWS Amplify Admin UI API 참조, 및 Amplify UI Builder API 참조에 문서화되어 있습니다. 예를 들어, `CreateApp`, `DeleteApp` 및 `DeleteBackendEnvironment` 작업에 대한 호출은 CloudTrail 로그 파일의 항목을 생성합니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 자격 증명 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management(IAM) 사용자 보안 인증을 통해 이루어졌습니다.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 인증을 사용하여 요청이 생성되었습니다.
- 요청이 다른 AWS 서비스를 통해 이루어졌습니다.

자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail userIdentity 요소를 참조하세요.

Athena 로그 파일 항목의 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 포함합니다. CloudTrail 로그 파일은 퍼블릭 API 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는AWS Amplify Console API Reference `ListApps` 작업을 보여주는 CloudTrail 로그 항목입니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Mary_Major",
        "accountId": "444455556666",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary_Major",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-01-12T05:48:10Z"
            }
        }
    },
    "eventTime": "2021-01-12T06:47:29Z",
    "eventSource": "amplify.amazonaws.com",
```

```
    "eventName": "ListApps",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.255",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.898
 Linux/4.9.230-0.1.ac.223.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.275-b01
 java/1.8.0_275 vendor/Oracle_Corporation",
    "requestParameters": {
        "maxResults": "100"
    },
    "responseElements": null,
    "requestID": "1c026d0b-3397-405a-95aa-aa43aexample",
    "eventID": "c5fca3fb-d148-4fa1-ba22-5fa63example",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "444455556666"
}
```

다음 예제는AWS Amplify Admin UI API Reference ListBackendJobs 작업을 보여주는 CloudTrail 로그 항목입니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Mary_Major",
        "accountId": "444455556666",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary_Major",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-01-13T00:47:25Z"
            }
        }
    },
    "eventTime": "2021-01-13T01:15:43Z",
    "eventSource": "amplifybackend.amazonaws.com",
    "eventName": "ListBackendJobs",
```

```
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.255",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.898
 Linux/4.9.230-0.1.ac.223.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.275-b01
 java/1.8.0_275 vendor/Oracle_Corporation",
    "requestParameters": {
        "appId": "d23mv2oexample",
        "backendEnvironmentName": "staging"
    },
    "responseElements": {
        "jobs": [
            {
                "appId": "d23mv2oexample",
                "backendEnvironmentName": "staging",
                "jobId": "ed63e9b2-dd1b-4bf2-895b-3d5dcexample",
                "operation": "CreateBackendAuth",
                "status": "COMPLETED",
                "createTime": "1610499932490",
                "updateTime": "1610500140053"
            },
            {
                "appId": "d23mv2oexample",
                "backendEnvironmentName": "staging",
                "jobId": "06904b10-a795-49c1-92b7-185dfexample",
                "operation": "CreateBackend",
                "status": "COMPLETED",
                "createTime": "1610499657938",
                "updateTime": "1610499704458"
            }
        ],
        "appId": "d23mv2oexample",
        "backendEnvironmentName": "staging"
    },
    "requestID": "7adfabd6-98d5-4b11-bd39-c7deaexample",
    "eventID": "68769310-c96c-4789-a6bb-68b52example",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "444455556666"
}
```

Amplify의 보안

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 기업과 기업 간의 공동 책임입니다. AWS 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다. AWS AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 적용되는 규정 준수 프로그램에 대해 자세히 알아보려면 규정 준수 프로그램별 범위 내AWS 서비스 규정 준수 참조하십시오. AWS Amplify
- 클라우드에서의 보안 - 귀하의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Amplify 사용 시 책임 분담 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 항목에서는 보안 및 규정 준수 목표를 충족하도록 Amplify를 구성하는 방법을 보여줍니다. 또한 Amplify 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

Amplify의 ID 및 액세스 관리

AWS Identity and Access Management (IAM) 은 관리자가 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 AWS 도와줍니다. IAM 관리자는 누가 Amplify 리소스를 사용하도록 인증되고

(로그인) 권한이 부여되는지(권한 보유)를 제어합니다. IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

주제

고객

사용 방법 AWS Identity and Access Management (IAM) 은 Amplify에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 – Amplify 서비스를 사용하여 작업을 수행하는 경우, 필요한 자격 증명과 권한을 관리자가 제공합니다. 다른 Amplify 기능을 사용하여 작업을 수행한다면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. Amplify의 기능에 액세스할 수 없다면 Amplify 자격 증명 및 액세스 문제 해결 부분을 참조하십시오.

서비스 관리자 – 회사에서 Amplify 리소스를 책임지고 있다면 Amplify에 대한 완전한 액세스 권한이 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Amplify 기능과 리소스를 결정합니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하십시오. 회사가 Amplify에서 IAM을 사용하는 방법에 대해 자세히 알아보려면 Amplify에서 IAM을 사용하는 방법 섹션을 참조하십시오.

IAM 관리자 - IAM 관리자라면 Amplify에 대한 액세스 권한을 관리하는 정책을 작성하는 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 Amplify 자격 증명 기반 정책 예제를 보려면 Amplify의 자격 증명 기반 정책 예 섹션을 참조하십시오.

자격 증명을 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 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 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용자 설명서의 AWS에서 다중 인증(MFA) 사용을 참조합니다.

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 태스크를 수행하는 데 사용하세요. 루트 사용자로 로그인해야 하는 태스크의 전체 목록은 IAM 사용자 안내서의 루트 사용자 보안 인증이 필요한 태스크를 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS Directory Service페더레이션 ID에 AWS 계정액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여

모든 사용자 및 애플리케이션에서 사용할 수 있습니다. AWS 계정 IAM Identity Center에 대한 자세한 내용은AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇입니까?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한을 AWS 계정 가진 사용자 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 정보는 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하세요.

IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM 역할 사용을 참조하세요.

임시 보안 인증 정보가 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 아이덴티티에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 연동 자격 증명이 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 타사 자격 증명 공급자의 역할 만들기를 참조하세요. IAM Identity Center를 사용하는 경우 권한 세트를 구성합니다. 인증 후 자격 증명이 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관짓습니다. 권한 세트에 대한 자세한 내용은AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 태스크에 대한 다양한 권한을 임시로 받을 수 있습니다.

- 크로스 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 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 크로스 계정 액세스를 위한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.
- 서비스 간 액세스 — 일부는 다른 AWS 서비스서비스의 기능을 AWS 서비스 사용합니다. 예컨대, 어떤 서비스에서 호출을 수행하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 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 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용자 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조합니다.
  - 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 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 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 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.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용자 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조합니다.

정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 JSON 정책 개요를 참조하세요.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole`태스크를 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

ID 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

자격 증명 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. IAM의 AWS 관리형 정책은 리소스 기반 정책에 사용할 수 없습니다.

액세스 제어 목록(ACLs)

액세스 제어 목록(ACLs)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는 지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAF ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 안내서의 액세스 제어 목록(ACL) 개요를 참조하세요.

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 보안 인증 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 엔터티의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 보안 주체로 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용자 설명서의 IAM 엔터티에 대한 권한 경계를 참조합니다.
- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 기능을 활성화할 경우 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 구성원 계정의 엔티티 (각 엔티티 포함) 에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 정보는AWS Organizations 사용 설명서의 SCP 작동 방식을 참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 연합된 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할 자격 증명 기반 정책의 교차 및 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용자 설명서의 세션 정책을 참조합니다.

여러 정책 타입

여러 정책 타입이 요청에 적용되는 경우 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련되어 있을 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하십시오.

Amplify에서 IAM을 사용하는 방법

IAM을 사용하여 Amplify에 대한 액세스를 관리하기 전에 Amplify와 함께 사용할 수 있는 IAM 기능을 알아보십시오.

Amplify를 통해 사용할 수 있는 IAM 기능

IAM 특성	Amplify 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예
ACLs	아니요
ABAC(정책 내 태그)	부분
임시 보안 인증	예
전달 액세스 세션(FAS)	예
서비스 역할	예
서비스 연결 역할	아니요

Amplify 및 AWS 기타 서비스가 대부분의 IAM 기능과 어떻게 작동하는지 자세히 알아보려면 IAM 사용 설명서에서 IAM과 함께 작동하는 서비스를AWS 참조하십시오.

Amplify의 자격 증명 기반 정책

ID 기반 정책 지원	예

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부되는 작업와 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 자격 증명 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하십시오.

Amplify의 자격 증명 기반 정책 예

Amplify 자격 증명 기반 정책 예제를 보려면 Amplify의 자격 증명 기반 정책 예 섹션을 참조하십시오.

Amplify 내 리소스 기반 정책

리소스 기반 정책 지원	아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

계정 간 액세스를 활성화하려는 경우 전체 계정이나 다른 계정의 IAM 엔터티를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 다른 AWS 계정경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 개체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 개체에 자격 증명 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하십시오.

Amplify에 대한 정책 작업

정책 작업 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

ACM 작업 목록을 보려면 서비스 권한 부여 참조의 AWS Amplify에서 정의한 작업을 참조하십시오.

Amplify의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
amplify
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "amplify:action1",
      "amplify:action2"
         ]
```

Amplify 자격 증명 기반 정책 예제를 보려면 Amplify의 자격 증명 기반 정책 예 섹션을 참조하십시오.

Amplify 정책 리소스

정책 리소스 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 개체를 지정합니다. 문장에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 타입을 지원하는 작업에 대해 이 작업을 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

Amplify 리소스 유형 및 해당 ARN의 목록을 보려면 서비스 권한 부여 참조의 AWS Amplify에서 정의한 리소스를 참조하십시오. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 AWS Amplify가 정의한 작업을 참조하십시오.

Amplify 자격 증명 기반 정책 예제를 보려면 Amplify의 자격 증명 기반 정책 예 섹션을 참조하십시오.

Amplify의 정책 조건 키

서비스별 정책 조건 키 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition`요소를 지정하거나 단일 `Condition`요소에서 여러 키를 지정하는 경우 AWS 는 논리적 `AND`태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 `OR` 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

Amplify 조건 키 목록을 보려면 서비스 권한 부여 참조의 AWS Amplify을(를) 위한 조건 키를 참조하십시오. 조건 키를 사용할 수 있는 작업 및 리소스에 대해 알아보려면 작업 정의 기준을 참조하십시오. AWS Amplify

Amplify 자격 증명 기반 정책 예제를 보려면 Amplify의 자격 증명 기반 정책 예 섹션을 참조하십시오.

Amplify의 액세스 제어 목록(ACL)

ACL 지원	아니요

액세스 제어 목록(ACLs)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는 지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Amplify의 ABAC(속성 기반 액세스 제어)

ABAC(정책 내 태그) 지원	부분

속성 기반 액세스 제어(ABAC)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 개체 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그를 기반으로 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 타입에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 타입에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 정보는 IAM 사용 설명서의 ABAC란 무엇인가요?를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하십시오.

Amplify에서 임시 자격 증명 사용

임시 보안 인증 지원	예

임시 자격 증명을 사용하여 로그인하면 작동하지 AWS 서비스 않는 것도 있습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 IAM 사용 설명서의 IAM과AWS 서비스 연동되는 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 정보는 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하세요.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 인증 섹션을 참조하세요.

Amplify의 전달 액세스 세션

전달 액세스 세션(FAS) 지원	예

IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하라는 요청과 결합하여 사용합니다. AWS 서비스 FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

Amplify의 서비스 역할

서비스 역할 지원	예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하십시오.

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 Amplify 기능이 중단될 수 있습니다. Amplify에서 관련 지침을 제공하는 경우에만 서비스 역할을 편집합니다.

Amplify에 대한 서비스 연결 역할

서비스 연결 역할 지원	아니요

서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 IAM 사용 설명서의 IAM으로 작업하는AWS 서비스 섹션을 참조하십시오. 서비스 연결 역할 열에서 Yes가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

Amplify의 자격 증명 기반 정책 예

기본적으로 사용자 및 역할은 Amplify 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

각 리소스 유형에 대한 ARN 형식을 포함하여 Amplify에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조에서 AWS Amplify에 대한 작업, 리소스 및 조건 키를 참조하십시오.

주제

- 정책 모범 사례
- Amplify 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용

정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Amplify 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책으로 시작하고 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 해당 내용은 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS managed policies(관리형 정책) 또는 AWS managed policies for job functions(직무에 대한 관리형 정책)를 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 태스크를 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 Policies and permissions in IAM(IAM의 정책 및 권한)을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하tpdy.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 Configuring MFA-protected API access(MFA 보호 API 액세스 구성)를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하십시오.

Amplify 콘솔 사용

AWS Amplify 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해 내 Amplify 리소스에 대한 세부 정보를 나열하고 볼 수 있어야 합니다. AWS 계정최소 필수 권한보다 더 제한적인 자격 증명 기반 정책을 만들면 콘솔이 해당 정책에 연결된 엔터티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

Amplify Studio가 릴리스됨에 따라 앱 또는 백엔드를 삭제하려면 `amplify` 및 `amplifybackend` 권한이 모두 필요합니다. IAM 정책이 `amplify` 권한만 제공하는 경우, 사용자가 앱을 삭제하려고 하면 권한 오류가 발생합니다. 정책을 작성하는 관리자인 경우 삭제 작업을 수행해야 하는 사용자에게 제공할 올바른 권한을 결정하십시오.

사용자와 역할이 Amplify 콘솔을 계속 사용할 수 있도록 하려면 Amplify `ConsoleAccess` 또는 `ReadOnly` AWS 관리형 정책도 엔티티에 연결하십시오. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하십시오.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예시는 IAM 사용자가 자신의 사용자 자격 증명에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 API를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 AWS CLI 권한이 포함됩니다. AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
```

```
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 관리형 정책은 다음과 같습니다. AWS Amplify

AWS 관리형 정책은 에서 생성하고 관리하는 독립 실행형 정책입니다. AWS AWS 관리형 정책은 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었으므로 사용자, 그룹 및 역할에 권한을 할당하기 시작할 수 있습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한 권한을 부여하지 않을 수도 있다는 점에 유의하세요. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

관리형 정책에 정의된 권한은 변경할 수 없습니다. AWS AWS 관리형 정책에 정의된 권한을 업데이트하는 경우 AWS 해당 업데이트는 정책이 연결된 모든 주체 ID (사용자, 그룹, 역할) 에 영향을 미칩니다. AWS 새 API 작업이 시작되거나 기존 서비스에 새 AWS 서비스 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 가장 높습니다.

자세한 내용은 IAM 사용자 설명서의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AdministratorAccess -증폭

`AdministratorAccess-Amplify` 정책을 IAM 보안 인증에 연결할 수 있습니다. Amplify는 또한 이 정책을 서비스 역할에 연결하여 Amplify가 사용자를 대신하여 작업을 수행할 수 있습니다.

Amplify 콘솔에 백엔드를 배포할 때는 Amplify에서 리소스를 생성하고 관리하는 데 사용하는 서비스 역할을 `Amplify-Backend Deployment` 생성해야 합니다. AWS IAM이 `AdministratorAccess-Amplify` 관리형 정책을 `Amplify-Backend Deployment` 서비스 역할에 연결합니다.

이 정책은 Amplify 애플리케이션이 백엔드를 생성하고 관리하는 데 필요한 리소스에 대한 직접 액세스를 명시적으로 허용하는 동시에 계정 관리 권한을 부여합니다.

권한 세부 정보

이 정책은 IAM 작업을 비롯한 여러 AWS 서비스에 대한 액세스를 제공합니다. 이러한 작업을 통해 이 정책의 ID를 AWS Identity and Access Management 사용하여 권한이 있는 다른 ID를 생성할 수 있습니다. 이렇게 하면 권한 에스컬레이션이 가능하므로 이 정책은 `AdministratorAccess` 정책만큼 강력한 것으로 간주해야 합니다.

이 정책은 모든 리소스에 대한 `iam:PassRole` 작업 권한을 부여합니다. 이는 Amazon Cognito 사용자 풀 구성을 지원하는 데 필요합니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조의 AdministratorAccess-Amplify를 참조하십시오.

AWS 관리형 정책: AmplifyBackendDeployFullAccess

`AmplifyBackendDeployFullAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 를 사용하여 Amplify 백엔드 리소스를 배포할 수 있는 전체 액세스 권한을 Amplify에 부여합니다. AWS Cloud Development Kit (AWS CDK)권한은 필요한 정책 권한이 있는 AWS CDK 역할로 이월됩니다. `AdministratorAccess`

권한 세부 정보

이 정책에는 다음 작업을 수행할 수 있는 권한이 포함됩니다.

- `Amplify`— 배포된 애플리케이션에 대한 메타데이터를 검색합니다.
- `AWS CloudFormation`— Amplify 관리 스택을 생성, 업데이트 및 삭제합니다.
- `SSM`— Amplify 관리형 SSM 파라미터 스토어 `String` 및 파라미터를 생성, 업데이트 및 삭제합니다. `SecureString`
- `AWS AppSync`— AWS AppSync 스키마, 리졸버 및 함수 리소스를 업데이트하고 검색합니다. 목적은 2세대 샌드박스 핫스왑 기능을 지원하는 것입니다.
- `Lambda`— Amplify 관리 기능의 구성을 업데이트하고 검색합니다. 목적은 2세대 샌드박스 핫스왑 기능을 지원하는 것입니다.

- `Amazon S3`— Amplify 배포 자산을 검색합니다.
- `AWS Security Token Service`— AWS Cloud Development Kit (AWS CDK) CLI가 배포 역할을 맡을 수 있도록 합니다.
- `Amazon RDS`— DB 인스턴스, 클러스터 및 프록시의 메타데이터를 읽습니다.
- `Amazon EC2`— 서브넷의 가용 영역 정보를 읽습니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조를 참조하십시오 AmplifyBackendDeployFullAccess.

관리형 정책에 대한 AWS 업데이트 Amplify

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 Amplify의 AWS 관리형 정책 업데이트에 대한 세부 정보를 확인하십시오. 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 에 대한 문서 기록 AWS Amplify 페이지에서 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
AmplifyBackendDeployFullAccess - 기존 정책에 대한 업데이트	Amplify가 고객 계정에서 CDK 부트스트랩 버전을 탐지할 수 있도록 `arn:aws:ssm:*:*:parameter/cdk-bootstrap/*` 리소스에 읽기 액세스 권한을 추가합니다.	2024년 5월 31일
AmplifyBackendDeployFullAccess-기존 정책 업데이트	리소스 및 계정 조건에 따라 범위가 지정된 Amazon RDS 및 Amazon EC2 읽기 전용 권한을 포함하는 새 `AmplifyDiscoverRDSVpcConfig` 정책 설명을 추가합니다. 이러한 권한은 고객이 기존 SQL 데이터베이스에서 Typescript 데이터 스키마를 생성할 수 있는 Amplify Gen 2 `npx amplify`	2024년 4월 17일

변경 사항	설명	날짜
	`generate schema-from-database` 명령을 지원합니다. `rds:DescribeDBProxies` ,, `rds:DescribeDBInstances` `rds:DescribeDBClusters` `rds:DescribeDBSubnetGroups` , 및 권한을 추가합니다. `ec2:DescribeSubnets` 이 `npx amplify generate schema-from-database` 명령에는 지정된 DB 호스트가 Amazon RDS에서 호스팅되는지 확인하고 SQL 데이터베이스에서 지원하는 AWS AppSync API를 설정하는 데 필요한 기타 리소스를 프로비저닝하는 데 필요한 Amazon VPC 구성을 자동 생성하려면 이러한 권한이 필요합니다.	

변경 사항	설명	날짜
AmplifyBackendDeployFullAccess-기존 정책 업데이트	`DeleteBranch` API 호출 시 스택 삭제를 지원하는 `cloudformation:DeleteStack` 정책 작업을 추가하십시오. 핫스왑 기능을 지원하는 `lambda:GetFunction` 정책 작업을 추가합니다. Lambda 함수에 업데이트를 지원하는 `lambda:UpdateFunctionConfiguration` 정책 작업을 추가합니다.	2024년 4월 5일
AdministratorAccess-증폭 — 기존 정책으로 업데이트	API 호출을 지원하는 `cloudformation:TagResource` 및 `cloudformation:UnTagResource` 권한을 추가합니다. AWS CloudFormation	2024년 4월 4일
AmplifyBackendDeployFullAccess-기존 정책 업데이트	AWS Cloud Development Kit (AWS CDK) 핫스왑을 지원하는 `lambda:InvokeFunction` 정책 작업을 추가합니다. Lambda 함수를 직접 호출하여 Amazon S3 자산 핫스왑을 수행합니다. AWS CDK 핫스왑 함수를 지원하는 `lambda:UpdateFunctionCode` 정책 작업을 추가합니다.	2024년 1월 2일

변경 사항	설명	날짜
AmplifyBackendDeployFullAccess-기존 정책 업데이트	`UpdateApiKey` 작업을 지원하는 정책 작업을 추가합니다. 리소스 삭제 없이 샌드박스를 종료하고 다시 시작한 후 앱을 성공적으로 배포할 수 있도록 하려면 이렇게 해야 합니다.	2023년 11월 17일
AmplifyBackendDeployFullAccess-기존 정책 업데이트	Amplify 앱 배포를 지원하는 `amplify:GetBackendEnvironment` 권한을 추가합니다.	2023년 11월 6일
AmplifyBackendDeployFullAccess - 새 정책	Amplify가 Amplify 백엔드 리소스를 배포하는 데 필요한 최소 권한이 포함된 새 정책을 추가했습니다.	2023년 10월 8일
AdministratorAccess-증폭 — 기존 정책으로 업데이트	Amplify 명령줄 인터페이스(CLI)에 필요한 `ecr:DescribeRepositories` 권한을 추가합니다.	2023년 6월 1일

변경 사항	설명	날짜
AdministratorAccess-증폭 — 기존 정책으로 업데이트	AWS AppSync 리소스에서 태그 제거를 지원하는 정책 작업을 추가합니다. Amazon Polly 리소스를 지원하는 정책 작업을 추가합니다. OpenSearch 도메인 구성 업데이트를 지원하는 정책 조치를 추가합니다. AWS Identity and Access Management 역할에서 태그 제거를 지원하는 정책 작업을 추가합니다. Amazon DynamoDB 리소스에서 태그 제거를 지원하는 정책 작업을 추가합니다. Amplify 게시 및 호스팅 워크플로를 지원하도록 `cloudfront:GetCloudFrontOriginAccessIdentity` 및 `cloudfront:GetCloudFrontOriginAccessIdentityConfig` 권한을 `CLISDKCalls` 명령문 블록에 추가합니다. AWS CLI 이(가) 내부 버킷에 Amazon S3 퍼블릭 액세스 차단 기능을 활성화하는 Amazon S3 보안 모범 사례를 지원할 수 있도록 `s3:PutBucketPublicAccessBlo`	2023년 2월 24일

변경 사항	설명	날짜
	ck 권한을 CLIManage viaCFNPolicy 명령문 블록에 추가합니다. Amplify 백엔드 프로세서에서 재시도 시 고객 AWS CloudFormation 스택을 검색할 수 있도록 CLISDKCalls 명령문 블록에 cloudform ation:DescribeStac ks 권한을 추가하여 스택이 업데이트되는 경우 중복 실행을 방지할 수 있습니다. CLICloudformationP olicy 명령문 블록에 cloudformation:Lis tStacks 권한을 추가합니다. 작업을 완전히 지원하려면 이 권한이 필요합니다. CloudFormation DescribeS tacks	
AdministratorAccess-증폭 — 기존 정책으로 업데이트	Amplify 서버 측 렌더링 기능을 통해 고객의 애플리케이션 메트릭을 푸시할 수 있도록 정책 조치를 추가합니다. CloudWatch AWS 계정	2022년 8월 30일
AdministratorAccess-증폭 — 기존 정책으로 업데이트	Amplify 배포 Amazon S3 버킷에 대한 퍼블릭 액세스를 차단하는 정책 작업을 추가합니다.	2022년 4월 27일

변경 사항	설명	날짜
AdministratorAccess-증폭 — 기존 정책으로 업데이트	고객이 서버 측 렌더링(SSR) 앱을 삭제하도록 허용하는 작업을 추가합니다. 이렇게 하면 해당 CloudFront 배포를 성공적으로 삭제할 수도 있습니다. 고객이 Amplify CLI를 사용하여 기존 이벤트 소스의 이벤트를 처리할 수 있도록 다른 Lambda 함수를 지정하는 것을 허용하는 작업을 추가합니다. 이러한 변경으로 작업을 수행할 수 있게 됩니다. AWS Lambda UpdateEventSourceMapping	2022년 4월 17일
AdministratorAccess-증폭 — 기존 정책으로 업데이트	모든 리소스에서 Amplify UI Builder 작업을 활성화하는 정책 작업을 추가합니다.	2021년 12월 2일
AdministratorAccess-증폭 — 기존 정책으로 업데이트	소셜 자격 증명 공급자를 사용하는 Amazon Cognito 인증 기능을 지원하는 정책 작업을 추가합니다. Lambda 계층을 지원하는 정책 작업을 추가합니다. Amplify 스토리지 범주를 지원하는 정책 작업을 추가합니다.	2021년 11월 8일

변경 사항	설명	날짜
AdministratorAccess-증폭 — 기존 정책으로 업데이트	Amplify Interactions 범주를 지원하는 Amazon Lex 작업을 추가합니다. Amplify Predictions 범주를 지원하는 Amazon Rekognition 작업을 추가합니다. Amazon Cognito 사용자 풀에서 MFA 구성을 지원하는 Amazon Cognito 작업을 추가합니다. 지원에 CloudFormation 조치를 추가하세요. AWS CloudFormation StackSets Amplify Geo 범주를 지원하는 Amazon Location Service 작업을 추가합니다. Amplify에서 Lambda 계층을 지원하는 Lambda 작업을 추가합니다. CloudWatch 이벤트를 지원하는 CloudWatch 로그 작업을 추가합니다. Amplify Storage 범주를 지원하는 Amazon S3 작업을 추가합니다. 서버 측 렌더링(SSR) 앱을 지원하는 정책 작업을 추가합니다.	2021년 9월 27일

변경 사항	설명	날짜
AdministratorAccess-증폭 — 기존 정책으로 업데이트	모든 Amplify 작업을 단일 `amplify:*` 작업으로 통합합니다. 고객 Amazon S3 버킷의 암호화를 지원하는 Amazon S3 작업을 추가합니다. 권한 경계가 활성화된 Amplify 앱을 지원하도록 IAM 권한 경계 작업을 추가합니다. 발신 전화번호 보기, 대상 전화번호 보기, 생성, 확인, 삭제를 지원하는 Amazon SNS 작업을 추가합니다. Amplify Studio: Amplify 콘솔 및 Amplify Studio에서 백엔드를 관리할 수 있도록 Amazon Cognito AWS Lambda, IAM AWS CloudFormation 및 정책 작업을 추가합니다. AWS Systems Manager (SSM) 정책 설명을 추가하여 Amplify 환경 비밀을 관리합니다. AWS CloudFormation `ListResources` Amplify 앱용 Lambda 계층을 지원하는 작업을 추가합니다.	2021년 7월 28일

변경 사항	설명	날짜
Amplify의 변경 내용 추적 시작	Amplify는 AWS 관리형 정책의 변경 사항을 추적하기 시작했습니다.	2021년 7월 28일

Amplify 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 Amplify 및 IAM에서 발생할 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다.

주제

- Amplify에서 작업을 수행할 권한이 없음
- 저는 IAM을 수행할 권한이 없습니다. PassRole
- 내 AWS 계정 외부의 사용자가 Amplify 리소스에 액세스할 수 있도록 허용하고 싶습니다.

Amplify에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 수신되면, 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 mateojacksonIAM 사용자가 콘솔을 사용하여 가상 *my-example-widget*리소스에 대한 세부 정보를 보려고 하지만 가상 amplify:*GetWidget*권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 amplify:GetWidget on resource: my-example-widget
```

이 경우 amplify:*GetWidget*작업을 사용하여 *my-example-widget*리소스에 액세스할 수 있도록 mateojackson사용자 정책을 업데이트해야 합니다.

도움이 필요하면 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

Amplify Studio가 릴리스됨에 따라 앱 또는 백엔드를 삭제하려면 amplify 및 amplifybackend 권한이 모두 필요합니다. 관리자가 amplify 권한만 제공하는 IAM 정책을 작성한 경우, 앱을 삭제하려고 하면 권한 오류가 발생합니다.

다음 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 가상 *example-amplify-app* 리소스를 삭제하려고 하지만 amplifybackend:*RemoveAllBackends* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 amplifybackend;:RemoveAllBackends on resource: example-amplify-app
```

이 경우 Mateo는 *example-amplify-app* 작업을 사용하여 amplifybackend:*RemoveAllBackends* 리소스에 액세스하도록 허용하는 정책을 업데이트하라고 관리자에게 요청합니다.

저는 IAM을 수행할 권한이 없습니다. PassRole

iam:PassRole 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 Amplify에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

새 서비스 역할 또는 서비스 연결 역할을 만드는 대신 기존 역할을 해당 서비스에 전달할 AWS 서비스 수 있는 기능도 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 marymajor라는 IAM 사용자가 콘솔을 사용하여 Amplify에서 태스크를 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우 Mary가 iam:PassRole작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 AWS 계정 외부의 사용자가 Amplify 리소스에 액세스할 수 있도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하십시오.

- Amplify에서 이러한 기능을 지원하는지 여부를 알아보려면 Amplify에서 IAM을 사용하는 방법 섹션을 참조하십시오.

- 소유한 리소스에 대한 액세스 권한을 AWS 계정 부여하는 방법을 알아보려면 IAM 사용 설명서의 다른 AWS 계정 IAM 사용자에게 액세스 권한 제공을 참조하십시오.
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정AWS 계정 소유에 대한 액세스 제공을 참조하십시오.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(자격 증명 연동)을 참조하세요.
- 크로스 계정 액세스를 위한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.

Amplify의 데이터 보호

AWS Amplify https://aws.amazon.com/compliance/shared-responsibility-model/ AWS 모든 AWS 서비스를 실행하는 글로벌 인프라를 보호할 책임이 있습니다. AWS 고객 콘텐츠 및 개인 데이터 처리를 위한 보안 구성 제어를 포함하여 이 인프라에서 호스팅되는 데이터에 대한 제어를 유지합니다. AWS 데이터 컨트롤러 또는 데이터 처리자 역할을 하는 고객 및 APN 파트너는 AWS 클라우드에 저장하는 모든 개인 데이터에 대한 책임을 집니다.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 AWS IAM Identity Center OR AWS Identity and Access Management (IAM) 를 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이러한 방식에서는 각 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 멀티 팩터 인증 설정(MFA)을 사용하세요.
- SSL/TLS를 사용하여 리소스와 통신할 수 있습니다. AWS
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다. AWS CloudTrail
- AWS 서비스 내의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오.
- Amazon S3에 저장된 개인 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다.

이름 필드와 같은 자유 형식 필드에 고객 계정 번호와 같은 중요 식별 정보를 절대 입력하지 마십시오. 여기에는 콘솔 AWS CLI, API 또는 SDK를 사용하여 Amplify 또는 기타 AWS 서비스를 사용하는 경우가 포함됩니다. AWS Amplify 또는 기타 서비스에 입력하는 모든 데이터를 진단 로그에 포함할 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명 정보를 URL에 포함시키지 마십시오.

데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하십시오.

저장 중 암호화

유휴 데이터 암호화는 저장된 데이터를 암호화하여 무단 액세스로부터 데이터를 보호하는 것을 의미합니다. Amplify는 에서 관리하는 AWS KMS keys Amazon S3를 사용하여 기본적으로 앱의 빌드 아티팩트를 암호화합니다. AWS Key Management Service

Amplify는 CloudFront Amazon을 사용하여 고객에게 앱을 제공합니다. CloudFront 엣지 로케이션 접속 지점 (POP) 용으로 암호화된 SSD를 사용하고 지역별 엣지 캐시 (REC) 에는 암호화된 EBS 볼륨을 사용합니다. Functions의 CloudFront 함수 코드와 구성은 엣지 로케이션 POP 및 에서 사용하는 기타 스토리지 위치의 암호화된 SSD에 항상 암호화된 형식으로 저장됩니다. CloudFront

전송 중 암호화

전송 중 데이터 암호화는 데이터가 통신 엔드포인트 간을 이동하는 동안 데이터를 가로채기에서 보호하는 것을 의미합니다. Amplify Hosting은 전송 중 데이터에 대한 암호화를 기본으로 제공합니다. 고객과 Amplify 간 및 Amplify와 다운스트림 종속성 간의 모든 통신은 서명 버전 4 서명 프로세스를 사용하여 서명된 TLS 연결을 통해 보호됩니다. 모든 Amplify 호스팅 엔드포인트는 AWS Certificate Manager 사설 인증 기관에서 관리하는 SHA-256 인증서를 사용합니다. 자세한 내용은 서명 버전 4 서명 프로세스 및 ACM PCA란 무엇입니까를 참조하십시오.

암호화 키 관리

AWS Key Management Service (KMS) 는 고객 데이터를 암호화하는 데 사용되는 암호화 키를 생성하고 제어하는 AWS KMS keys관리형 서비스입니다. AWS Amplify 고객을 대신하여 데이터 암호화를 위한 암호화 키를 생성하고 관리합니다. 관리할 암호화 키가 없습니다.

규정 준수 검증: AWS Amplify

제3자 감사자는 여러 규정 AWS 준수 프로그램의 AWS Amplify 일환으로 보안 및 규정 준수를 평가합니다. 여기에는 SOC, PCI, ISO, HIPAA, MTCS, C5, K-ISMS, ENS High, OSPAR, HITRUST CSF, 및 FINMA가 포함됩니다.

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램의 범위별, 규정 준수AWS 서비스 프로그램별 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 HIPAA 적격 애플리케이션을 만드는 AWS 데 사용할 수 있는 방법을 설명합니다.

> **Note**
>
> 모든 AWS 서비스 사람이 HIPAA 자격을 갖춘 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하십시오.

- AWS 규정 준수 리소스AWS — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (미국 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (PCI), 국제 표준화기구 (ISO) 등) 에서 보안 제어에 대한 지침을 매핑합니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하십시오.
- Amazon GuardDuty — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.
- AWS Audit Manager— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

의 인프라 보안 AWS Amplify

관리형 서비스로서 AWS 글로벌 네트워크 보안으로 AWS Amplify 보호됩니다. AWS 보안 서비스 및 인프라 AWS 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하십시오. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하십시오.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 Amplify에 액세스할 수 있습니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(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 주체와 관련된 비밀 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 인증을 생성하여 요청에 서명할 수 있습니다.

Amplify의 보안 이벤트 로깅 및 모니터링

모니터링은 Amplify 및 기타 AWS 솔루션의 신뢰성, 가용성 및 성능을 유지하는 데 있어 중요한 부분입니다. AWS 는 Amplify를 관찰하고, 문제 발생 시 보고하고, 적절한 경우 자동 조치를 취할 수 있는 다음과 같은 모니터링 도구를 제공합니다.

- Amazon은 실행 중인 AWS 리소스와 애플리케이션을 실시간으로 CloudWatch AWS모니터링합니다. 지표를 수집 및 추적하고, 사용자 지정 대시보드를 생성할 수 있으며, 특정 지표가 지정한 임계값에 도달하면 사용자에게 알리거나 조치를 취하도록 경보를 설정할 수 있습니다. 예를 들어 Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스의 CPU 사용량 또는 기타 지표를 CloudWatch 추적하고 필요할 때 새 인스턴스를 자동으로 시작할 수 있습니다. Amplify에서 CloudWatch 메트릭 및 경보를 사용하는 방법에 대한 자세한 내용은 을 참조하십시오. 모니터링
- Amazon CloudWatch Logs를 사용하면 Amazon EC2 인스턴스 및 기타 소스에서 로그 파일을 모니터링 AWS CloudTrail, 저장 및 액세스할 수 있습니다. CloudWatch 로그는 로그 파일의 정보를 모니터링하고 특정 임계값이 충족되면 알려줄 수 있습니다. 또한 매우 내구력 있는 스토리지에 로그 데이터를 저장할 수 있습니다. 자세한 내용은 Amazon CloudWatch Logs 사용 설명서를 참조하십시오.
- AWS CloudTrail계정에서 또는 AWS 계정을 대신하여 이루어진 API 호출 및 관련 이벤트를 캡처하고 지정한 Amazon Simple Storage Service (Amazon S3) 버킷으로 로그 파일을 전송합니다. 어떤 사

용자와 계정이 전화를 걸었는지 AWS, 어떤 소스 IP 주소에서 전화를 걸었는지, 언제 호출이 발생했는지 식별할 수 있습니다. 자세한 정보는 AWS CloudTrail를 사용하여 Amplify API 호출 로깅을 참조하세요.

- EventBridgeAmazon은 다양한 소스의 데이터에 애플리케이션을 쉽게 연결할 수 있게 해주는 서버리스 이벤트 버스 서비스입니다. EventBridge 자체 애플리케이션, oftware-as-a S-Service (SaaS) 애플리케이션 AWS 및 서비스의 실시간 데이터 스트림을 제공하고 해당 데이터를 다음과 같은 대상으로 라우팅합니다. AWS Lambda이 방법을 통해 서비스에서 발생하는 이벤트를 모니터링하고 이벤트 기반 아키텍처를 구축할 수 있습니다. 자세한 내용은 Amazon EventBridge 사용 설명서를 참조하십시오.

교차 서비스 혼동된 대리인 방지

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. 에서 AWS서비스 간 사칭으로 인해 대리인 문제가 발생할 수 있습니다. 교차 서비스 가장은 한 서비스(직접 호출하는 서비스)가 다른 서비스(직접 호출되는 서비스)를 직접 호출할 때 발생할 수 있습니다. 직접 호출하는 서비스는 다른 고객의 리소스에 대해 액세스 권한이 없는 방식으로 작동하게 권한을 사용하도록 조작될 수 있습니다. 이를 방지하기 위해 AWS 에서는 계정의 리소스에 대한 액세스 권한이 부여된 서비스 보안 주체를 사용하여 모든 서비스에 대한 데이터를 보호하는 데 도움이 되는 도구를 제공합니다.

리소스 정책에 `aws:SourceArn`및 `aws:SourceAccount`글로벌 조건 컨텍스트 키를 사용하여 리소스에 다른 서비스에 AWS Amplify 부여하는 권한을 제한하는 것이 좋습니다. 두 전역 조건 컨텍스트 키를 모두 사용하는 경우 `aws:SourceAccount` 값과 `aws:SourceArn` 값의 계정은 동일한 정책 문에서 사용할 경우 동일한 계정 ID를 사용해야 합니다.

`aws:SourceArn`의 값은 Amplify 앱의 브랜치 ARN이어야 합니다. `arn:`*`Partition`*`:amplify:`*`Region`*`:`*`Account`*`:apps/`*`AppId`*`/branches/`*`BranchName` 형식에서 이 값을 지정합니다.

혼동된 대리인 문제로부터 보호하는 가장 효과적인 방법은 리소스의 전체 ARN이 포함된 `aws:SourceArn` 글로벌 조건 컨텍스트 키를 사용하는 것입니다. 리소스의 전체 ARN을 모를 경우 또는 여러 리소스를 지정하는 경우, ARN의 알 수 없는 부분에 대해 와일드카드(*)를 포함한 `aws:SourceArn` 전역 조건 컨텍스트 키를 사용합니다. 예제: `arn:aws:`*`servicename`*`::`*`123456789012`*`:*`.

다음 예는 계정의 Amplify 앱에 대한 액세스를 제한하고 혼동된 대리자 문제가 발생하는 것을 방지하기 위해 적용할 수 있는 역할 신뢰 정책을 보여줍니다. 이 정책을 사용하려면 정책 예제의 빨간색 기울임꼴 텍스트를 본인의 정보로 대체하십시오.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": [
          "amplify.me-south-1.amazonaws.com",
          "amplify.eu-south-1.amazonaws.com",
          "amplify.ap-east-1.amazonaws.com",
          "amplifybackend.amazonaws.com",
          "amplify.amazonaws.com"
        ]
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:amplify:us-east-1:123456789012:apps/*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

다음 예는 계정의 지정된 Amplify 앱에 대한 액세스를 제한하고 혼동된 대리자 문제가 발생하는 것을 방지하기 위해 적용할 수 있는 역할 신뢰 정책을 보여줍니다. 이 정책을 사용하려면 정책 예제의 빨간색 기울임꼴 텍스트를 본인의 정보로 대체하십시오.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": [
          "amplify.me-south-1.amazonaws.com",
          "amplify.eu-south-1.amazonaws.com",
          "amplify.ap-east-1.amazonaws.com",
          "amplifybackend.amazonaws.com",
          "amplify.amazonaws.com"
```

```
        ]
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:amplify:us-east-1:123456789012:apps/d123456789/
branches/*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

Amplify의 보안 모범 사례

Amplify는 자체 보안 정책을 개발하고 구현할 때 고려해야 할 여러 보안 기능을 제공합니다. 다음 모범 사례는 일반적인 지침이며 완벽한 보안 솔루션을 나타내지는 않습니다. 이러한 모범 사례는 환경에 적절하지 않거나 충분하지 않을 수 있으므로 지침이라기보다는 권장 사항으로만 사용해 주십시오.

Amplify 기본 도메인에 쿠키 사용

Amplify를 사용하여 웹 앱을 배포하는 경우, Amplify는 기본 `amplifyapp.com` 도메인에서 웹 앱을 대신 호스팅합니다. `https://branch-name.d1m7bkiki6tdw1.amplifyapp.com`와(과) 같은 형식의 URL에서 앱을 볼 수 있습니다.

Amplify 애플리케이션의 보안을 강화하기 위해 amplifyapp.com 도메인은 공개 접미사 목록(PSL)에 등록되어 있습니다. 보안 강화를 위해 Amplify 애플리케이션의 기본 도메인 이름에 민감한 쿠키를 설정해야 하는 경우, `__Host-` 접두사가 있는 쿠키를 사용하는 것이 좋습니다. 이렇게 쿠키를 설정하면 교차 사이트 요청 위조 시도(CSRF)로부터 도메인을 보호하는 데 도움이 됩니다. 자세한 내용은 Mozilla 개발자 네트워크의 Set-Cookie 페이지를 참조하십시오.

Amplify Hosting 서비스 할당량

다음은 호스팅 서비스 할당량입니다. AWS Amplify 서비스 할당량(과거에는 제한이라고도 함)은 AWS 계정의 최대 서비스 리소스 또는 작업 수입니다.

신규 앱과 동시 작업 AWS 계정 할당량이 줄어들었습니다. AWS 사용량에 따라 할당량을 자동으로 올립니다. 할당량 증가 요청을 할 수도 있습니다.

Service Quotas 콘솔이 계정의 할당량에 관한 정보를 제공합니다. Service Quotas 콘솔을 사용하면 기본 할당량을 확인하고 조정 가능한 할당량에 대한 할당량 증가를 요청할 수 있습니다. 자세한 내용은 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하십시오.

명칭	기본값	조정 가능	설명
앱	지원되는 각 리전: 25개	예	현재 지역의 이 계정에서 AWS Amplify Console에서 만들 수 있는 최대 앱 수입니다.
앱당 브랜치 수	지원되는 각 리전: 50	아니요	현재 리전의 이 계정에서 생성할 수 있는 앱당 최대 브랜치 수.
빌드 아티팩트 크기	지원되는 각 리전: 5기가바이트	아니요	앱 빌드 아티팩트의 최대 크기(GB). 빌드 아티팩트는 빌드 후 AWS Amplify 콘솔에서 배포됩니다.
캐시 아티팩트 크기	지원되는 각 리전: 5기가바이트	아니요	캐시 아티팩트의 최대 크기(GB)입니다.
동시 작업	지원되는 각 리전: 5	예	현재 리전의 이 계정에서 생성할 수 있는 동시 작업의 최대 수입니다.

명칭	기본값	조정 가능	설명
앱당 도메인 수	지원되는 각 리전: 5	예	현재 리전의 이 계정에서 생성할 수 있는 앱당 도메인 최대 수.
환경 캐시 아티팩트 크기	지원되는 각 리전: 5기가바이트	아니요	환경 캐시 아티팩트의 최대 크기(GB)
수동 배포 ZIP 파일 크기	지원되는 각 리전: 5기가바이트	아니요	수동 배포 ZIP 파일의 최대 크기(GB).
시간당 최대 앱 생성 수	지원되는 각 리전: 25개	아니요	현재 지역의 이 계정에서 AWS Amplify Console에서 시간당 생성할 수 있는 최대 앱 수입니다.
초당 요청 토큰	지원되는 각 리전: 20개,000	예	앱의 초당 최대 요청 토큰 수. Amplify Hosting은 요청이 소비하는 리소스 양(처리 시간 및 데이터 전송) 을 기반으로 요청에 토큰을 할당합니다.
도메인당 하위 도메인 수	지원되는 각 리전: 50	아니요	현재 리전의 이 계정에서 생성할 수 있는 도메인당 최대 하위 도메인 수.
앱당 웹훅 수	지원되는 각 리전: 50	예	현재 리전의 이 계정에서 생성할 수 있는 앱당 웹훅 최대 수.

Amplify 서비스 할당량에 대한 자세한 내용은 AWS 일반 참조의 AWS Amplify 엔드포인트 및 할당량을(를) 참조하십시오.

Amplify 호스팅 문제 해결

Amplify Hosting을 사용할 때 오류 또는 배포 문제가 발생하는 경우 이 섹션의 항목을 참조하십시오.

주제

일반적인 Amplify 문제 해결

다음 정보는 Amplify 호스팅과 관련된 일반적인 문제를 해결하는 데 도움이 될 수 있습니다.

주제

HTTP 429 상태 코드 (요청이 너무 많음)

Amplify는 수신 요청이 소비하는 처리 시간 및 데이터 전송을 기반으로 웹 사이트에 대한 초당 요청 수 (RPS) 를 제어합니다. 애플리케이션이 HTTP 429 상태 코드를 반환하는 경우, 들어오는 요청이 애플리케이션에 할당된 처리 시간 및 데이터 전송량을 초과한 것입니다. 이 애플리케이션 한도는 Amplify의 `REQUEST_TOKENS_PER_SECOND` 서비스 할당량에 의해 관리됩니다. 할당량에 대한 자세한 내용은 Amplify Hosting 서비스 할당량 섹션을 참조하세요.

이 문제를 해결하려면 애플리케이션을 최적화하여 요청 기간을 줄이고 데이터 전송을 줄여 앱의 RPS를 높이는 것이 좋습니다. 예를 들어 동일한 20,000개의 토큰을 사용하는 경우 100밀리초 이내에 응답하는 고도로 최적화된 SSR 페이지는 지연 시간이 200밀리초 이상인 페이지와 비교하여 더 높은 RPS를 지원할 수 있습니다.

마찬가지로 1MB 응답 크기를 반환하는 애플리케이션은 250KB의 응답 크기를 반환하는 애플리케이션보다 더 많은 토큰을 소비합니다.

또한 주어진 응답이 캐시에 보관되는 시간을 최대화하는 CloudFront 캐시 제어 헤더를 구성하여 Amazon 캐시를 활용하는 것이 좋습니다. CloudFront 캐시에서 제공되는 요청은 속도 제한에 포함되지 않습니다. 각 CloudFront 배포는 초당 최대 250,000개의 요청을 처리할 수 있으므로 캐시를 사용하여

앱을 매우 높게 확장할 수 있습니다. 캐시에 대한 자세한 내용은 Amazon CloudFront 개발자 안내서의 CloudFront 캐싱 및 가용성 최적화를 참조하십시오.

아마존 리눅스 2023 빌드 이미지 문제 해결

다음 정보는 Amazon Linux 2023 (AL2023) 빌드 이미지 관련 문제를 해결하는 데 도움이 될 수 있습니다.

주제

- Python 런타임으로 Amplify 함수를 실행하려면 어떻게 해야 합니까?
- 수퍼유저 또는 루트 권한이 필요한 명령을 실행하려면 어떻게 해야 하나요?

Python 런타임으로 Amplify 함수를 실행하려면 어떻게 해야 합니까?

Amplify 호스팅은 이제 새 애플리케이션을 배포할 때 기본적으로 Amazon Linux 2023 빌드 이미지를 사용합니다. AL2023 에는 Python 버전 3.8, 3.9, 3.10, 3.11이 사전 설치되어 있습니다.

Amazon Linux 2 이미지와의 이전 버전과의 호환성을 위해 AL2023 빌드 이미지에는 이전 버전의 Python에 대한 심볼릭 링크가 사전 설치되어 있습니다. 따라서 Amplify Hosting GitHub FAQ의 지침을 사용하여 애플리케이션의 빌드 사양에 있는 빌드 명령을 더 이상 업데이트할 필요가 없습니다.

기본적으로 Python 버전 3.10은 전역적으로 사용됩니다. 특정 Python 버전을 사용하여 함수를 빌드하려면 애플리케이션의 빌드 사양 파일에서 다음 명령을 실행합니다.

```
version: 1
backend:
  phases:
    build:
      commands:
        # use a python version globally
        - pyenv global 3.11
        # verify python version
        - python --version
        # install pipenv
        - pip install --user pipenv
        # add to path
        - export PATH=$PATH:/root/.local/bin
        # verify pipenv version
        - pipenv --version
```

```
        - amplifyPush --simple
```

수퍼유저 또는 루트 권한이 필요한 명령을 실행하려면 어떻게 해야 하나요?

Amazon Linux 2023 빌드 이미지를 사용 중이고 수퍼유저 또는 루트 권한이 필요한 시스템 명령을 실행할 때 오류가 발생하는 경우 Linux sudo 명령을 사용하여 이러한 명령을 실행해야 합니다. 예를 `yum install -y gcc` 들어 실행 중에 오류가 발생하면 를 사용하십시오`sudo yum install -y gcc`.

Amazon Linux 2 빌드 이미지는 루트 사용자를 사용했지만 Amplify의 AL2023 이미지는 `amplify` 사용자 지정 사용자와 함께 코드를 실행합니다. Amplify는 이 사용자에게 Linux sudo 명령을 사용하여 명령을 실행할 수 있는 권한을 부여합니다. 수퍼유저 권한이 sudo 필요한 명령에 사용하는 것이 가장 좋습니다.

사용자 지정 도메인 문제 해결

사용자 지정 도메인을 Amplify 애플리케이션에 연결할 때 문제가 발생하는 경우 지원을 사용자 지정 도메인 문제 해결 참조하십시오.

서버 측 렌더링 응용 프로그램 문제 해결

Amplify에 SSR 앱을 배포하는 데 문제가 발생하는 경우 지원을 참조하십시오. SSR 배포 문제 해결

AWS Amplify Hosting 참조

이 섹션의 주제를 통해 AWS Amplify에 대한 자세한 참조 자료를 찾아보세요.

주제

AWS CloudFormation 지원

AWS CloudFormation 템플릿을 사용하여 Amplify 리소스를 프로비저닝하고 반복 가능한 안정적인 웹 앱 배포를 활성화합니다. AWS CloudFormation은(는) 클라우드 환경 내 모든 인프라 리소스를 설명하고 프로비저닝하는 공통 언어를 제공하며, 몇 번의 클릭만으로도 여러 AWS 계정 및/또는 리전 전체에 대한 배포 작업이 가능해집니다.

Amplify Hosting은 Amplify CloudFormation 설명서를 참조하세요. Amplify Studio는 Amplify UI Builder CloudFormation 설명서를 참조하세요.

AWS Command Line Interface 지원

AWS Command Line Interface을(를) 사용하여 명령줄에서 프로그래밍 방식으로 Amplify 앱을 생성할 수 있습니다. 자세한 내용은 AWS CLI 설명서을(를) 참조하세요.

리소스 태그 지정 지원

AWS Command Line Interface을(를) 사용하여 Amplify 리소스에 태그를 지정할 수 있습니다. 자세한 내용은 AWS CLI 태그-리소스 설명서을(를) 참조하세요.

Amplify Hosting API

이 참조는 Amplify Hosting API의 작업과 데이터 유형에 대한 설명을 제공합니다. 자세한 내용은 Amplify API 참조 문서를 참조하세요.

에 대한 문서 기록 AWS Amplify

다음 표에는 의 마지막 릴리스 이후 설명서에서 변경된 주요 내용이 설명되어 있습니다 AWS Amplify.

- 최신 설명서 업데이트: 2024년 5월 31일

변경 사항	설명	날짜
업데이트된 관리형 정책 항목	Amplify의 AWS 관리형 정책에 대한 최근 변경 사항을 설명하도록 AWS 관리형 정책은 다음과 같습니다. AWS Amplify 항목을 업데이트했습니다.	2024년 5월 31일
업데이트된 관리형 정책 항목	Amplify의 AWS 관리형 정책에 대한 최근 변경 사항을 설명하도록 AWS 관리형 정책은 다음과 같습니다. AWS Amplify 항목을 업데이트했습니다.	2024년 4월 17일
시작하기 챕터 업데이트	튜토리얼에서 Next.js 예제 애플리케이션을 사용하도록 Amplify Hosting 시작하기 챕터를 업데이트했습니다.	2024년 4월 12일
업데이트된 관리형 정책 항목	Amplify의 AWS 관리형 정책에 대한 최근 변경 사항을 설명하도록 AWS 관리형 정책은 다음과 같습니다. AWS Amplify 항목을 업데이트했습니다.	2024년 4월 5일
업데이트된 관리형 정책 항목	Amplify의 AWS 관리형 정책에 대한 최근 변경 사항을 설명하도록 AWS 관리형 정책은 다음과 같습니다. AWS Amplify 항목을 업데이트했습니다.	2024년 4월 4일

변경 사항	설명	날짜
새 문제 해결 장	Amplify Hosting에 배포된 응용 프로그램에서 발생하는 문제를 해결하는 방법을 설명하는 Amplify 호스팅 문제 해결 장을 추가했습니다.	2024년 4월 2일
사용자 지정 SSL/TLS 인증서에 대한 새로운 지원	앱을 사용자 지정 도메인에 연결할 때 사용자 지정 SSL/TLS 인증서에 대한 Amplify 지원을 설명하는 SSL/TLS 인증서 사용 항목이 사용자 지정 도메인 설정 장에 추가되었습니다.	2024년 2월 20일
업데이트된 관리형 정책 항목	Amplify의 AWS 관리형 정책에 대한 최근 변경 사항을 설명하도록 AWS 관리형 정책은 다음과 같습니다. AWS Amplify 항목을 업데이트했습니다.	2024년 1월 2일
SSR 프레임워크를 위한 새로운 지원	오픈 소스 어댑터를 사용하는 JavaScript 기반 SSR 프레임워크를 위한 Amplify 지원을 설명하는 SSR 프레임워크를 위한 Amplify 지원 주제를 추가했습니다.	2023년 11월 19일
이미지 최적화 기능 시작을 위한 새로운 지원	서버 측에서 렌더링한 앱의 이미지 최적화에 기본적으로 제공되는 지원을 설명하는 SSR 앱을 위한 이미지 최적화 주제를 추가했습니다.	2023년 11월 19일

변경 사항	설명	날짜
업데이트된 관리형 정책 항목	Amplify의 AWS 관리형 정책에 대한 최근 변경 사항을 설명하도록 AWS 관리형 정책은 다음과 같습니다. AWS Amplify 항목을 업데이트했습니다.	2023년 11월 17일
업데이트된 관리형 정책 항목	Amplify의 AWS 관리형 정책에 대한 최근 변경 사항을 설명하도록 AWS 관리형 정책은 다음과 같습니다. AWS Amplify 항목을 업데이트했습니다.	2023년 11월 6일
새 와일드카드 하위 도메인 항목	사용자 지정 도메인의 와일드카드 하위 도메인 지원을 설명하는 Wildcard 하위 도메인 항목이 추가되었습니다.	2023년 11월 6일
새로운 관리형 정책	AWS 관리형 정책은 다음과 같습니다. AWS AmplifyAmplify의 새 AmplifyBackendDeployFullAccess AWS 관리형 정책을 설명하도록 항목을 업데이트했습니다.	2023년 10월 8일
모노레포 프레임워크 기능 출시에 대한 새로운 지원	npm 작업 공간, pnpm 작업 공간, Yarn 작업 공간, Nx 및 Turborepo를 사용하여 만든 모노리포지토리에 앱을 배포하기 위한 지원을 설명하도록 모노레포 빌드 설정 항목을 업데이트했습니다.	2023년 6월 19일

변경 사항	설명	날짜
업데이트된 관리형 정책 항목	Amplify의 AWS 관리형 정책에 대한 최근 변경 사항을 설명하도록 AWS 관리형 정책은 다음과 같습니다. AWS Amplify 항목을 업데이트했습니다.	2023년 6월 1일
업데이트된 관리형 정책 항목	Amplify의 AWS 관리형 정책에 대한 최근 변경 사항을 설명하도록 AWS 관리형 정책은 다음과 같습니다. AWS Amplify 항목을 업데이트했습니다.	2023년 2월 24일
서버 측 렌더링 챕터 업데이트	Next.js 버전 12 및 13에 대한 Amplify 지원의 최근 변경 사항을 설명하도록 Amplify Hosting을 통해 서버 측 렌더링 앱 배포 장을 업데이트했습니다.	2022년 11월 17일
업데이트된 관리형 정책 항목	Amplify의 AWS 관리형 정책에 대한 최근 변경 사항을 설명하도록 AWS 관리형 정책은 다음과 같습니다. AWS Amplify 항목을 업데이트했습니다.	2022년 8월 30일
업데이트된 관리형 정책 항목	Amplify Studio를 사용하여 백엔드를 배포하는 방법을 설명하도록 애플리케이션을 위한 백엔드 구축 항목을 업데이트했습니다.	2022년 8월 23일
업데이트된 관리형 정책 항목	Amplify의 AWS 관리형 정책에 대한 최근 변경 사항을 설명하도록 AWS 관리형 정책은 다음과 같습니다. AWS Amplify 항목을 업데이트했습니다.	2022년 4월 27일

변경 사항	설명	날짜
업데이트된 관리형 정책 항목	Amplify의 AWS 관리형 정책에 대한 최근 변경 사항을 설명하도록 AWS 관리형 정책은 다음과 같습니다. AWS Amplify 항목을 업데이트했습니다.	2022년 4월 17일
새 GitHub 앱 기능 출시	리포지토리에 대한 Amplify 액세스를 승인하기 GitHub 위한 새 GitHub 앱을 설명하는 GitHub 리포지토리에 대한 Amplify 액세스 설정 항목이 추가되었습니다.	2022년 4월 5일
Amplify Studio의 새로운 기능 출시	백엔드 데이터에 연결할 수 있는 UI 구성 요소를 만들 수 있는 비주얼 디자이너를 제공하는 Amplify Studio 업데이트를 설명하도록 AWS Amplify 호스팅에 오신 것을 환영합니다 항목을 업데이트했습니다.	2021년 12월 2일
업데이트된 관리형 정책 항목	Amplify Studio를 지원하기 위한 Amplify의 AWS 관리형 정책에 대한 최근 변경 사항을 설명하도록 AWS 관리형 정책은 다음과 같습니다. AWS Amplify 항목을 업데이트했습니다.	2021년 12월 2일
업데이트된 관리형 정책 항목	Amplify의 AWS 관리형 정책에 대한 최근 변경 사항을 설명하도록 AWS 관리형 정책은 다음과 같습니다. AWS Amplify 항목을 업데이트했습니다.	2021년 11월 8일

변경 사항	설명	날짜
업데이트된 관리형 정책 항목	Amplify의 AWS 관리형 정책에 대한 최근 변경 사항을 설명하도록 AWS 관리형 정책은 다음과 같습니다. AWS Amplify 항목을 업데이트했습니다.	2021년 9월 27일
새로운 관리형 정책 항목	Amplify의 AWS 관리형 정책과 해당 정책의 최근 변경 사항을 설명하는 AWS 관리형 정책은 다음과 같습니다. AWS Amplify 항목이 추가되었습니다.	2021년 7월 28일
서버측 렌더링 챕터가 업데이트되었습니다.	Next.js 버전 10.x. x 및 Next.js 버전 11에 대한 새로운 지원을 설명하도록 Amplify Hosting을 통해 서버 측 렌더링 앱 배포 장을 업데이트했습니다.	2021년 7월 22일
빌드 설정 구성 챕터 업데이트	Amplify를 사용하여 monorepo 앱을 배포할 때 빌드 설정 및 새로운 `AMPLIFY_MONOREPO_APP_ROOT` 환경 변수를 구성하는 방법을 설명하는 모노레포 빌드 설정 항목이 추가되었습니다.	2021년 7월 20일

변경 사항	설명	날짜
기능 브랜치 배포 챕터가 업데이트되었습니다.	빌드 시 `aws-exports.js` 파일을 자동 생성하는 방법을 설명하는 Amplify 구성의 자동 빌드 타임 생성 (1세대 앱만 해당) 항목이 추가되었습니다. 조건부 백엔드 빌드를 활성화하는 방법을 설명하는 조건부 백엔드 빌드 (1세대 앱만 해당) 항목이 추가되었습니다. 새 앱을 만들거나, 새 브랜치를 기존 앱에 연결하거나, 다른 백엔드 환경을 가리키도록 기존 프론트엔드를 업데이트할 때 기존 백엔드를 재사용하는 방법을 설명하는 여러 앱에서 Amplify 백엔드 사용 (1세대 앱만 해당) 항목이 추가되었습니다.	2021년 6월 30일
업데이트된 보안 장	공동 책임 모델을 적용하는 방법과 Amplify가 암호화를 사용하여 저장된 데이터와 전송 중인 데이터를 보호하는 방법을 설명하는 Amplify의 데이터 보호 항목을 추가했습니다.	2021년 6월 3일
SSR 기능 출시에 대한 새로운 지원	서버 사이드 렌더링(SSR)을 사용하고 Next.js로 만든 웹 앱에 대한 Amplify 지원을 설명하는 Amplify Hosting을 통해 서버 측 렌더링 앱 배포 장을 추가했습니다.	2021년 5월 18일

변경 사항	설명	날짜
새로운 보안 장	Amplify를 사용할 때 공동 책임 모델을 적용하는 방법과 보안 및 규정 준수 목표를 충족하도록 Amplify를 구성하는 방법을 설명하는 Amplify의 보안 장을 추가했습니다.	2021년 3월 26일
업데이트된 사용자 지정 빌드 항목	Amazon Elastic Container Registry Public에서 호스팅되는 사용자 지정 빌드 이미지를 구성하는 방법을 설명하기 위해 사용자 지정 빌드 이미지 및 라이브 패키지 업데이트 항목을 업데이트했습니다.	2021년 3월 12일
모니터링 항목 업데이트	Amazon CloudWatch 지표 데이터에 액세스하고 경보를 설정하는 방법을 설명하도록 모니터링 주제를 업데이트했습니다.	2021년 2월 2일
새 CloudTrail 로깅 주제	AWS Amplify 콘솔 API 참조 및 AWS Amplify 관리자 UI API 참조에 대한 모든 API 작업을 AWS CloudTrail 캡처하고 기록하는 방법을 설명하는 AWS CloudTrail주제를 사용하여 Amplify API 호출 로깅을 추가했습니다.	2021년 2월 2일

변경 사항	설명	날짜
새 관리자 UI 기능 출시	프런트엔드 웹 및 모바일 개발자가 AWS Management Console외부에서 앱 백엔드를 만들고 관리할 수 있는 시각적 인터페이스를 제공하는 새로운 관리 UI를 설명하도록 AWS Amplify 호스팅에 오신 것을 환영합니다 항목을 업데이트했습니다.	2020년 12월 1일
새 성능 모드 기능 출시	성능 모드를 활성화하여 더 빠른 호스팅 성능을 위해 최적화하는 방법을 설명하도록 앱 성능 관리 항목을 업데이트했습니다.	2020년 11월 4일
사용자 지정 헤더 항목을 업데이트했습니다.	콘솔을 사용하거나 YML 파일을 편집하여 Amplify 앱의 사용자 지정 헤더를 정의하는 방법을 설명하도록 사용자 지정 헤더 항목을 업데이트했습니다.	2020년 10월 28일
새로운 자동 하위 도메인 기능 출시	Amazon Route 53 사용자 지정 도메인에 연결된 앱에 패턴 기반 기능 분기 배포를 사용하는 방법을 설명하는 Route 53 사용자 지정 도메인의 자동 하위 도메인 설정 항목을 추가했습니다. 하위 도메인에서 액세스할 수 있도록 pull 요청의 웹 미리 보기를 설정하는 방법을 설명하는 하위 도메인을 통한 웹 미리 보기 액세스 항목을 추가했습니다.	2020년 6월 20일

변경 사항	설명	날짜
새 알림 항목	빌드의 성공 또는 실패 시 이해 관계자 또는 팀 구성원에게 알리도록 Amplify 앱에 이메일 알림을 설정하는 방법을 설명하는 알림 항목이 추가되었습니다.	2020년 6월 20일
사용자 지정 도메인 항목을 업데이트했습니다.	Amazon Route 53 및 Google 도메인에 사용자 지정 도메인을 추가하는 절차를 개선하도록 사용자 지정 도메인 설정 주제를 업데이트했습니다. GoDaddy 이 업데이트에는 사용자 지정 도메인 설정을 위한 새로운 문제 해결 정보도 포함되어 있습니다.	2020년 5월 12일
AWS Amplify 릴리스	이번 릴리스에서 Amplify가 도입되었습니다.	2018년 11월 26일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.