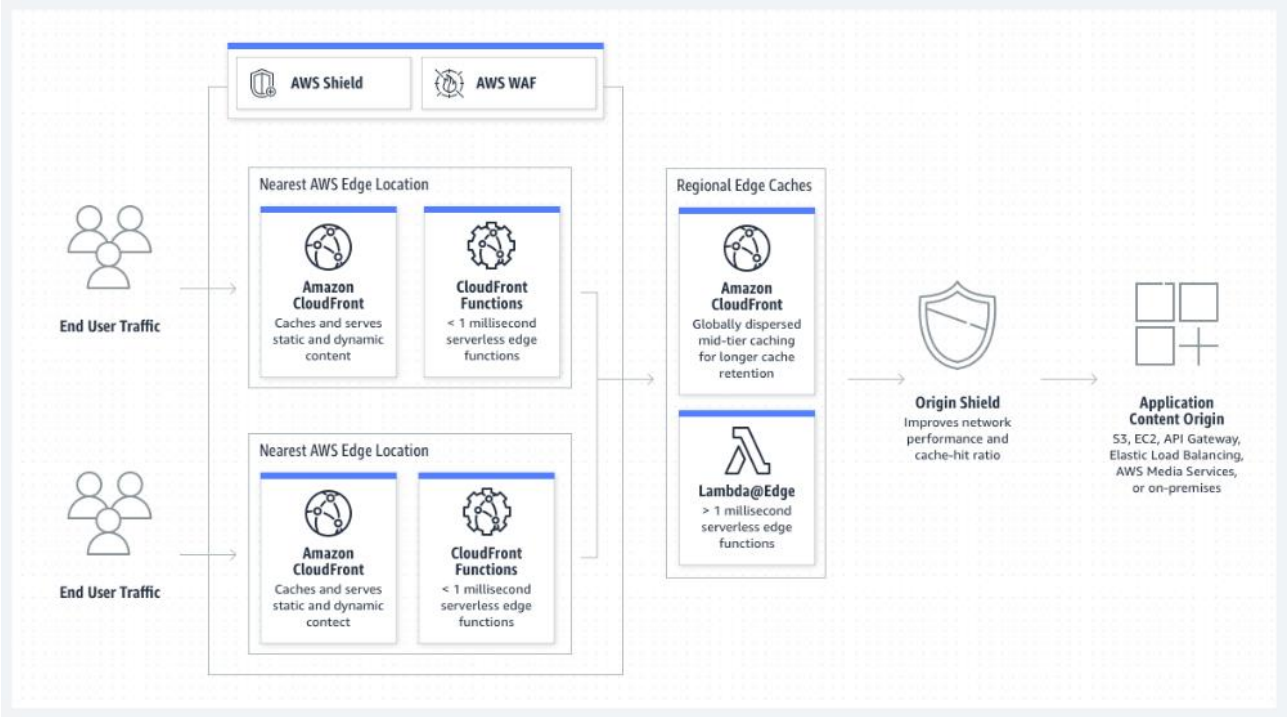
AWS CloudFront

1. 콘텐츠 전송 네트워크(CDN : Contents Delivery Network)

서비스 사용자에게 보다 빠른 자료(동영상, 이미지, 문서, 웹 문서 등) 전송을 위하여 사용자와 가장 인접한 엣지 포인트에 데이터를 보관(캐싱)하고 있다가 재 요청이 있을 경우 해당 요청자료를 사용자에게 전송해 주는 역할을 수행한다. 2022년 현재 이를 위해 AWS에서는 410개 이상의 접속지점(POP: Points of Presence)를 두고 있다.



1) 사용 목적

① 고속 콘텐츠 전송

② 실시간 스트리밍

③ 다중 사용자 확장

2) 장점

- 웹사이트 로딩 속도의 개선

- 인터넷 회선 비용 절감

- 컨텐츠 제공의 안정성

- 웹 사이트 보안 개선

2. AWS CloudFront Service

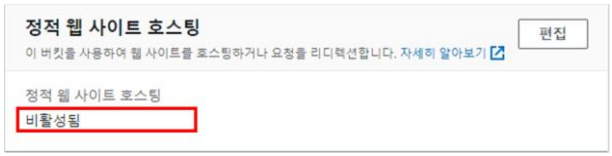
Amazon CloudFront 서비스 Amazon의 CDN 서비스로 웹 문서 및 이미지 파일과 같이 정적 및 동적 웹 콘텐츠를 사용자에게 보다 빨리 배포할 수 있도록 지원하는 서비스로 엣지 로케이션 데이터 센터의 글로벌 네트워크를 통해 사용자가 요청한 콘텐츠의 배포 지연 시간이 가장 낮은 엣지 로케이션으로 요청이 라우팅 되어 보다 빠르게 콘텐츠를 배포 할 수 있도록 한다.

1) S3 정적 웹 사이트와 CloudFront 연결

CloudFront를 사용하여 정적 웹 사이트를 구현하고자 할 경우에는 S3에서의 정적 웹 사이트 설정 및 권한 설정을 할 필요가 없다.

오히려 보안을 좀더 강화하면서 정적 웹 사이트를 구현하고자 할 경우에는 CloudFront 배포 생성을 통해 서비스를 하는 것이 구현도 간단하고 서비스 속도도 향상되며, 보안도 강화할 수 있는 방법이 된다.

CloudFront 배포 생성 프로세스

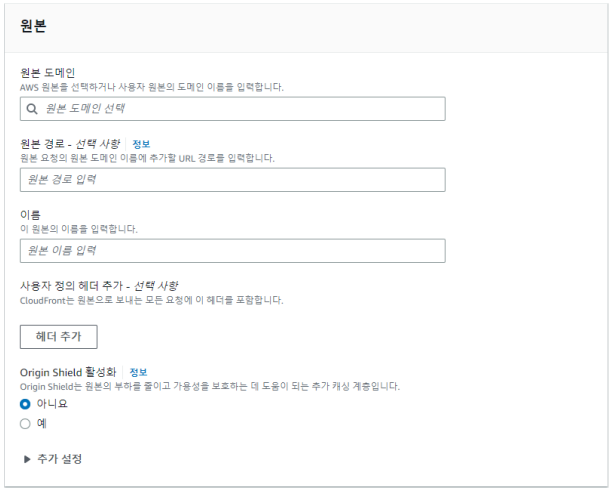


- 권한 탭 ➔ Bucket 정책(코드) : 필요 없음(삭제)
- Bucket 정책의 경우 CloudFront 배포 생성시 자동 부여됨. 오히려 작성을 해 놓았을 경우 CloudFront 배포 생성시 코드 수정이 되지 않는 경우가 발생함.

S3 Bucket 생성시 불필요한 작업

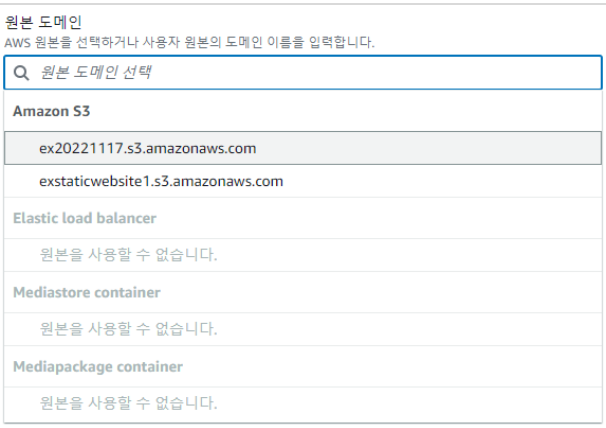
① 배포 페이지의 상단 오른쪽에 있는 "배포 생성"을 클릭하여 배포 생성 페이지로 이동한다.

② 배포 페이지 : 원본



- **원본 도메인(Origin Domain Name) :** 연결하고자 하는 서비스의 도메인(URL)을 선택 또는 기재
- **원본경로(Origin Path) :** 원본 도메인에 지정된 도메일의 하위 경로
- **이름 :** CloudFront에서 사용될 이름, OAI에 사용 됨. 원본 도메인을 선택하면 자동으로 기재됨.
- **Origin Shield 활성화 :** CloudFront에서 캐싱 계층
- **추가설정**
  연결 시도 : 원본에 연결을 시도하는 횟수
  연결 시간 초과 : 원본에서의 응답을 기다리는 시간(초)

원본

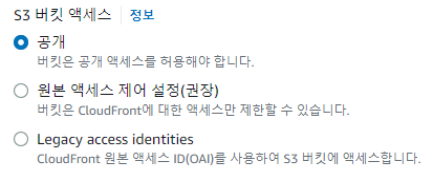


- CloudFront와 연결하고자 하는 S3를 찾아 선택
  입력 칸을 클릭하면 현재 선택할 수 있는 AWS서비스들이 나오며 이 중 연결할 S3서비스 선택
- API Gateway의 배포명(URL)을 연결하고자 할 경우엔 API Gateway의 배포명을 기재
- 정적 웹 사이트로 지정된 Amazon S3의 Bucket의 URL을 선택해주면 됨.
- S3 도메인을 원본으로 지정하게 될 경우 기존에 없던 S3 Bucket 액세스가 추가됨.

원본 도메인(Origin Domain Name)

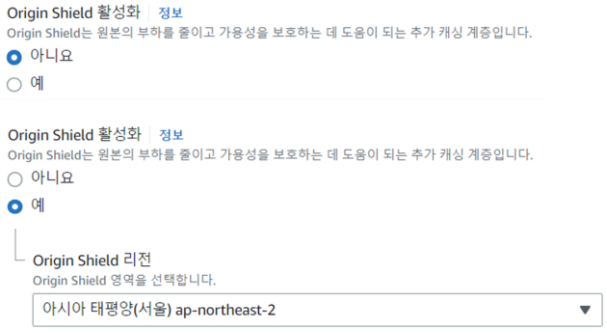
- 선택한 S3 정적 웹사이트에 하위 폴더(디렉터리)가 있을 경우 이를 지정하면

원본경로(Origin Path)



- **공개 :** S3 Bucket 액세스를 사용하지 않음. 즉, 접근 제어를 하지 않게 됨.
- **원본 액세스 제어 설정(권장) :**
  S3 Bucket 액세스 제어는 S3에서 직접 제한하게 됨. CloudFront에 대한 액세스 권한 부여 등을 S3 권한 정책을 통해 코드로 직접 삽입을 해주어야 함.
- **Legacy access identities :**
  S3 Bucket 액세스 제어를 CloudFront에서 OAI를 사용하여 S3 권한 정책에 대한 수정을 할 수 있음. 자동으로 권한 정책을 수정하기 위하여 "Legacy access identities"를 선택한 후 제어대상 S3 Bucket을 선택하고 Bucket 정책은 "예. Bucket 정책 업데이트"를 선택해주면 S3 Bucket의 권한 정책이 자동으로 수정됨.

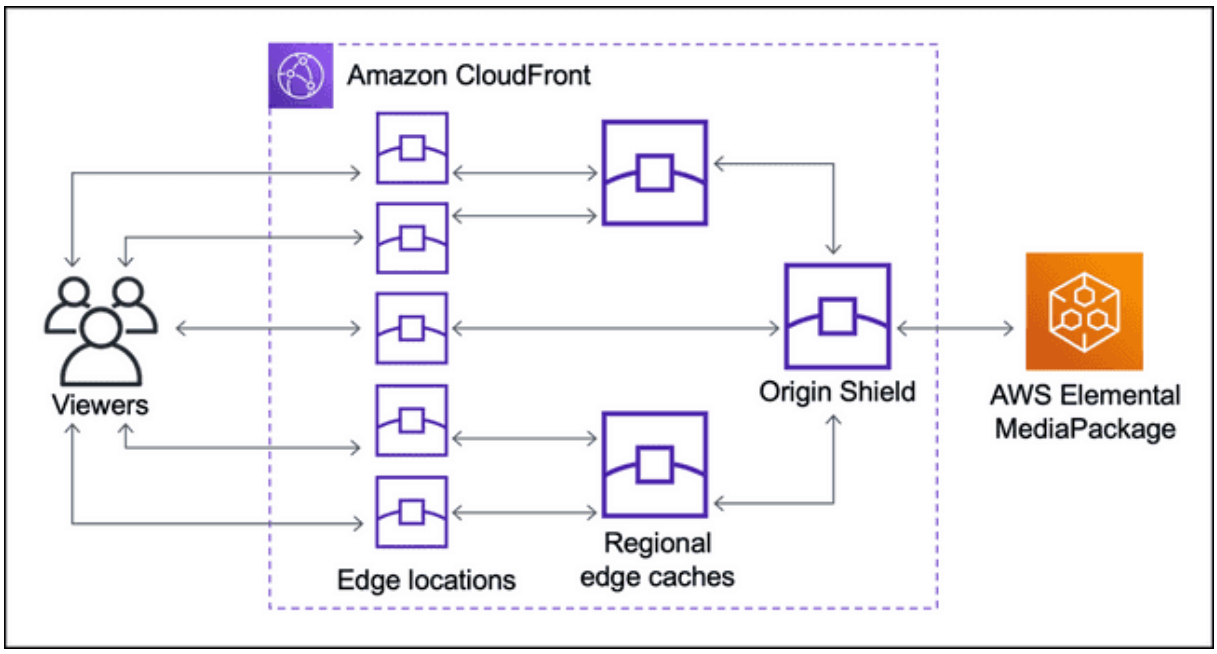
S3 Bucket Access



CloudFront Origin Shield는 CloudFront 캐싱 인프라의 추가 계층으로 오리진의 부하를 최소화하고 가용성을 높이며 운영 비용을 절감하는 데 도움이 됩니다.

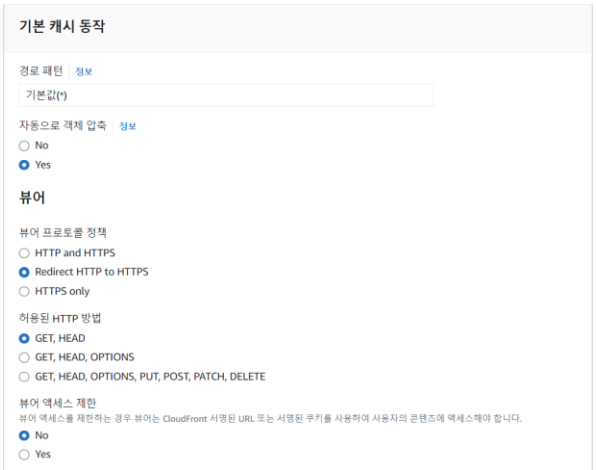
- 향상된 캐시 적중률
- 오리진 부하 감소
- 향상된 네트워크 성능

CloudFront Origin Shield에 대한 요청은 10,000개당 비용이 책정된다. ➔ CloudFront 요금



Origin Shield 활성화

③ 배포 페이지 : 기본 캐시 동작

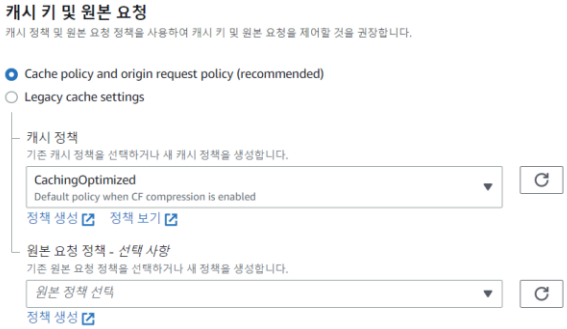


- **자동으로 객체 압축** : Yes
  요청할 리소스의 파일 크기를 비약적으로 줄여줄 수 있다.

- **뷰어 프로토콜 정책** : Redirect HTTP to HTTPS
  HTTP 프로토콜로 접속 시 자동으로 HTTPS로 리다이렉트된다.

- **허용된 HTTP 방법 :** GET, HEAD
  정적 리소스를 배포할 것이기 때문에 다른 HTTP Method를 허용하지 않아도 된다.

기본 캐시 동작

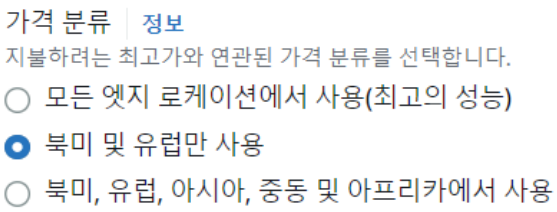


- Cache policy and origin request policy (권장)

정책이름	설명
Amplify	AWS Amplify 웹 앱인 원본과 함께 사용
CachingDisabled	**캐싱 비활성화**
CachingOptimized	**CloudFront가 캐시 키에 포함된 값을 최소화하여 캐시 효율성을 최적화**
CachingOptimizedForUncompressedObjects	압축을 사용할 수 없는 경우의 기본 정책
Elemental-MediaPackage	AWS Elemental Media Package End-Point인 원본과 함께 사용하도록 설계

캐시 키 및 원본 요청 정책

④ 배포 페이지 : 설정

<table>
<tr><td> 
</td><td>· 보통 “모든 엣지 로케이션에서 사용(최고의 성능)”을 사용하면 되지만, 비용을 절약해야 하는 상황이거나 서비스 지역 타겟이 정해져 있을 때 적절한 항목을 선택하면 된다.</td></tr>
<tr><td colspan="2">기본 캐시 동작</td></tr>
<tr><td> 
</td><td>· 기본값 루트 객체에 인덱스 페이지의 파일명을 입력한다.
· /는 입력하면 안 된다.</td></tr>
<tr><td colspan="2">캐시 키 및 원본 요청 정책</td></tr>
</table>