BESPIN GLOBAL

[매뉴얼] AWS Certificate Manager에서 SSL 설정하는 방법

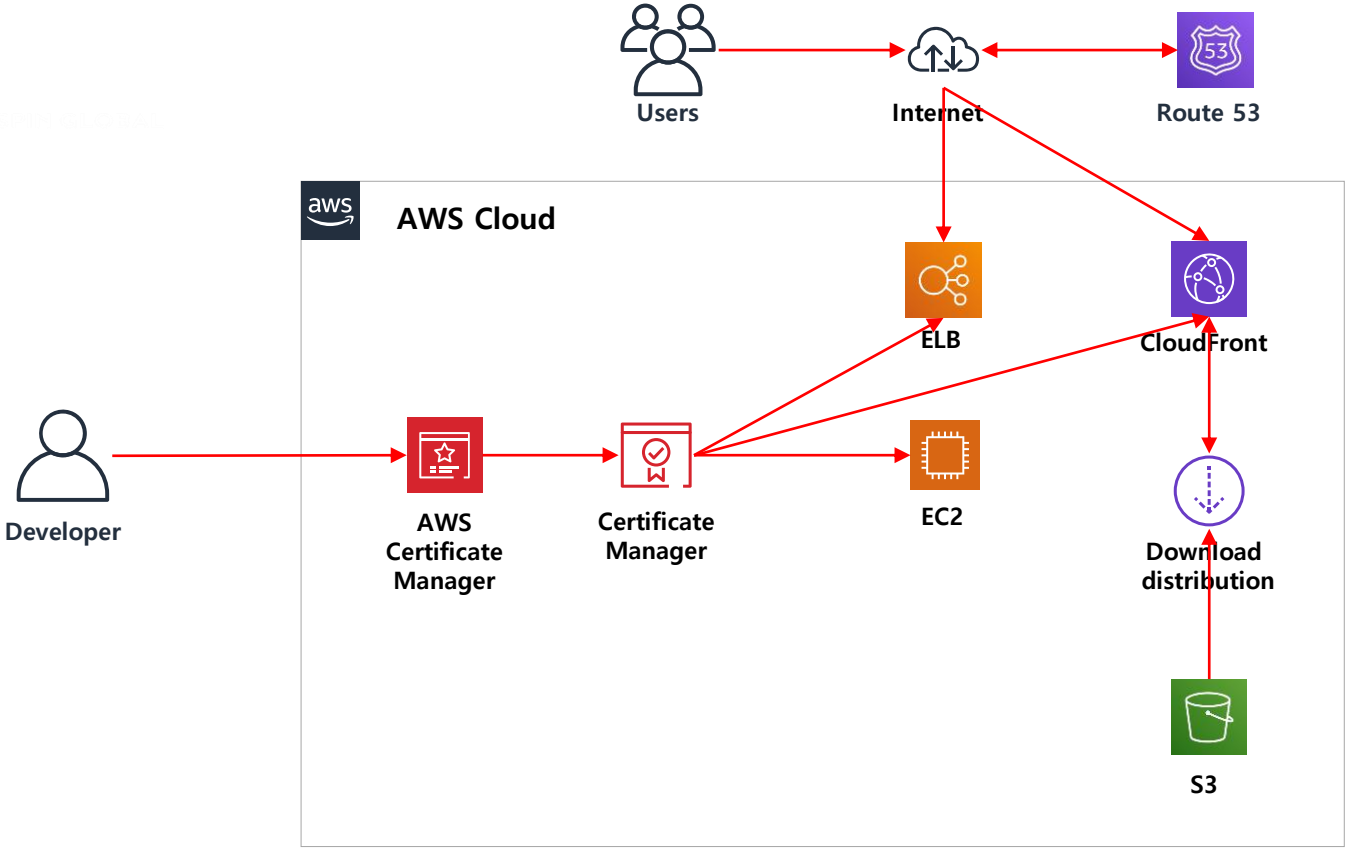
AGENDA

1. AWS Certificate Manager (ACM) 소개
2. AWS ACM 에서 무료 인증서 가져오기
3. CloudFront 에 AWS ACM 사용하기

AWS Certificate Manager (ACM) 소개

- SSL인증서를 Amazon Trust Services (ATS)에서 AWS 서비스 내에서 사용이 가능하도록 무료로 발급해주는 서비스
- SSL인증서를 구매할 필요 없음
- 자동으로 인증서를 정기적으로 업데이트 진행
- 매년 재발급 및 인증서 재설치의 작업 필요

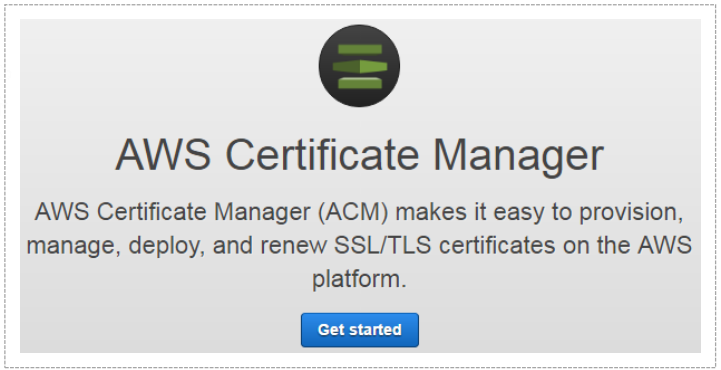
AWS ACM Architecture

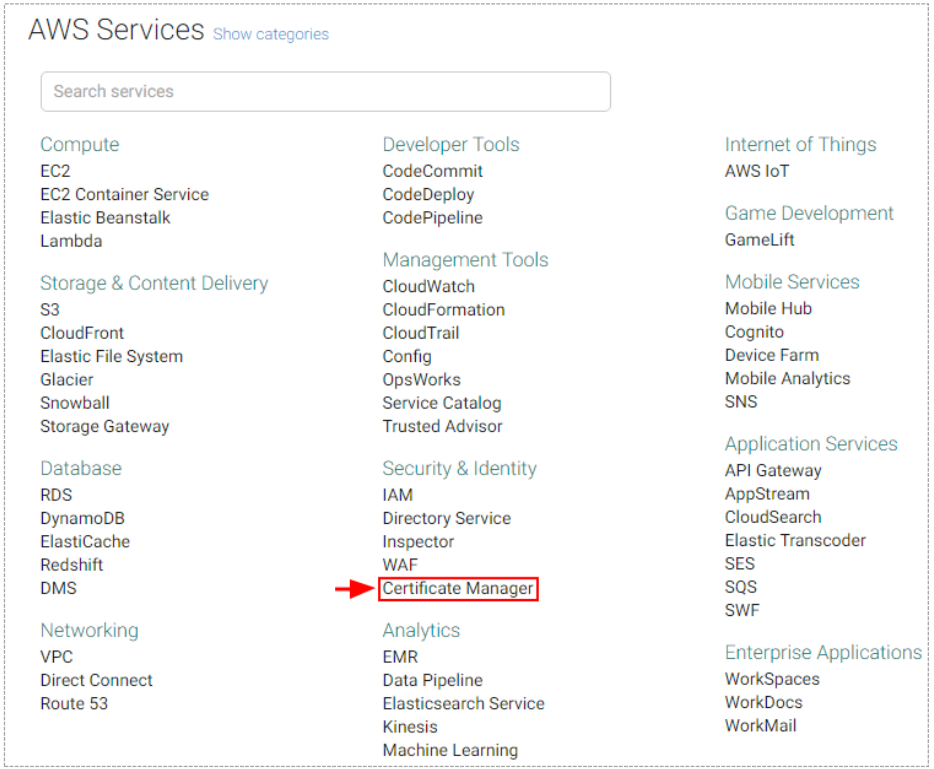


AGENDA

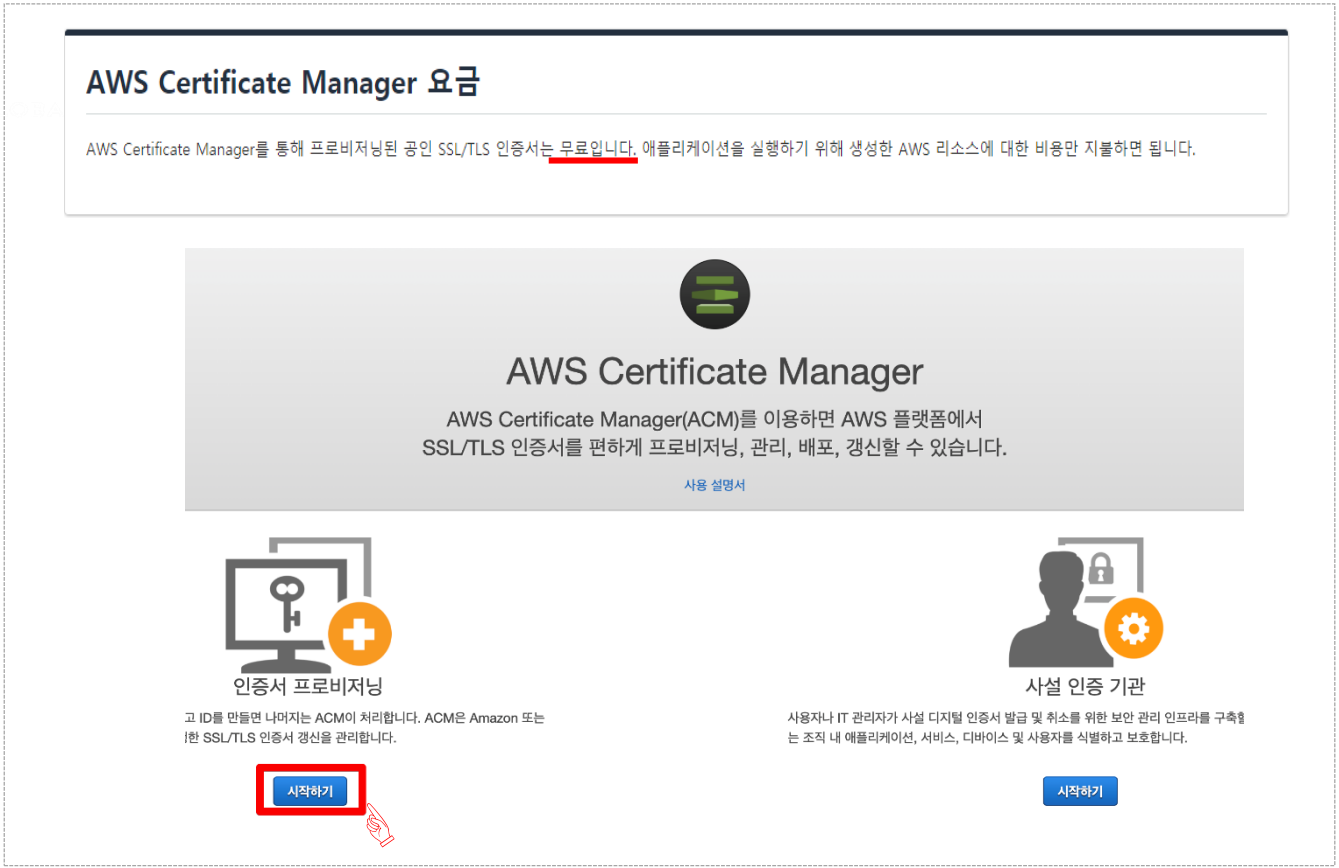
1. AWS Certificate Manager (ACM) 소개
2. AWS ACM 에서 무료 인증서 가져오기
3. CloudFront 에 AWS ACM 사용하기

AWS Certificate Manager(ACM) 무료 인증서

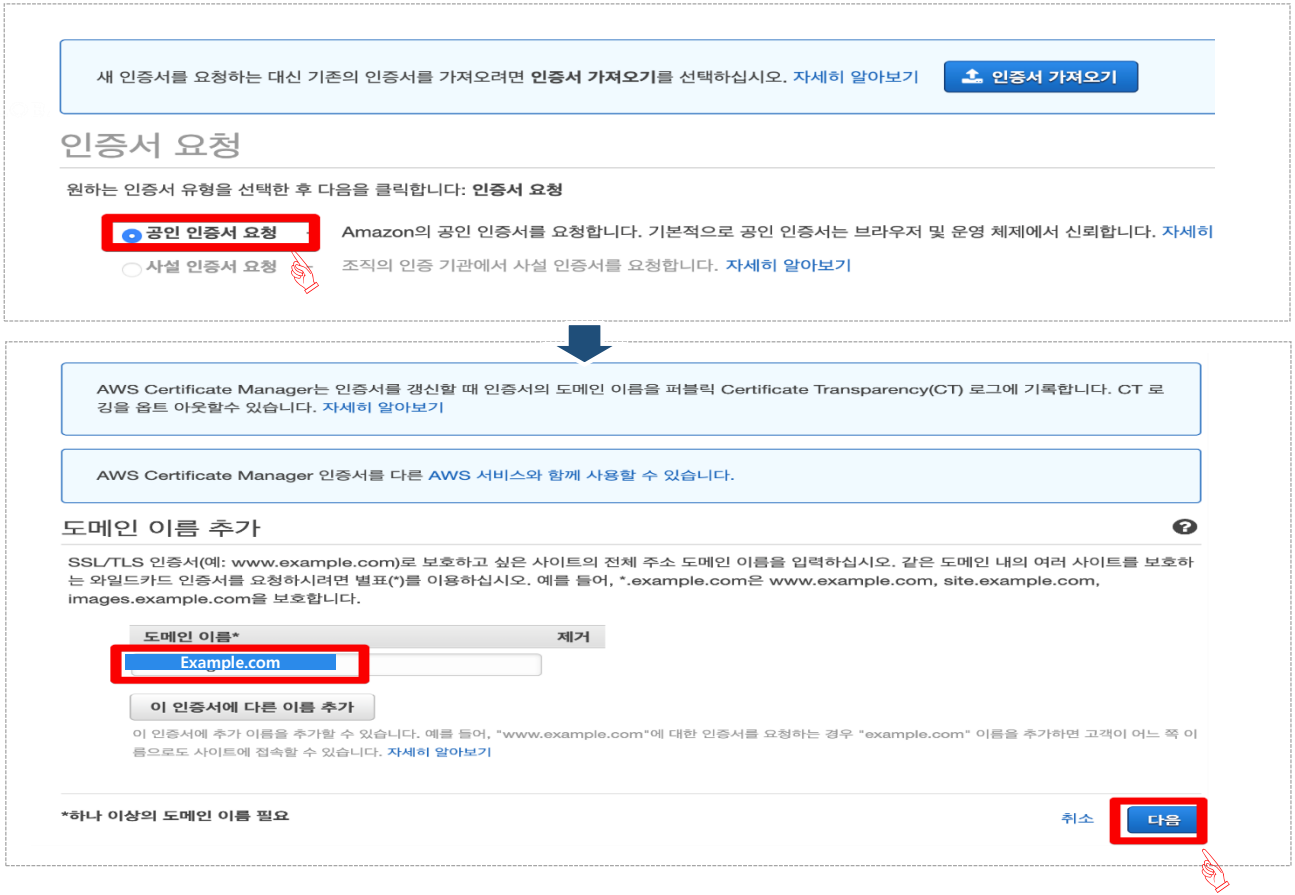




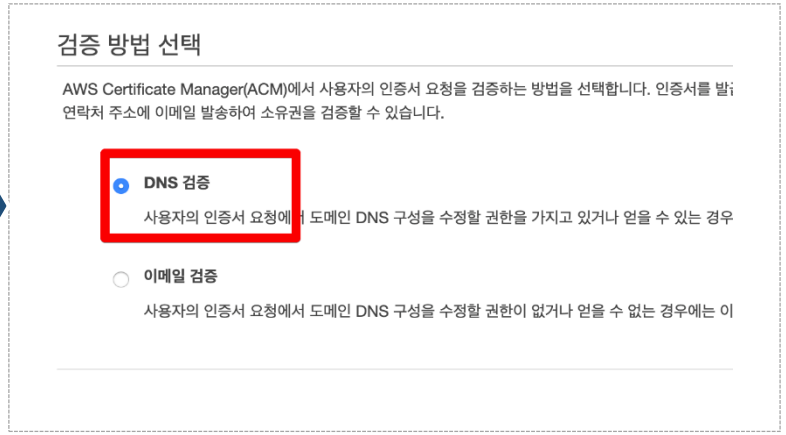
AWS Certificate Manager(ACM) 무료 인증서

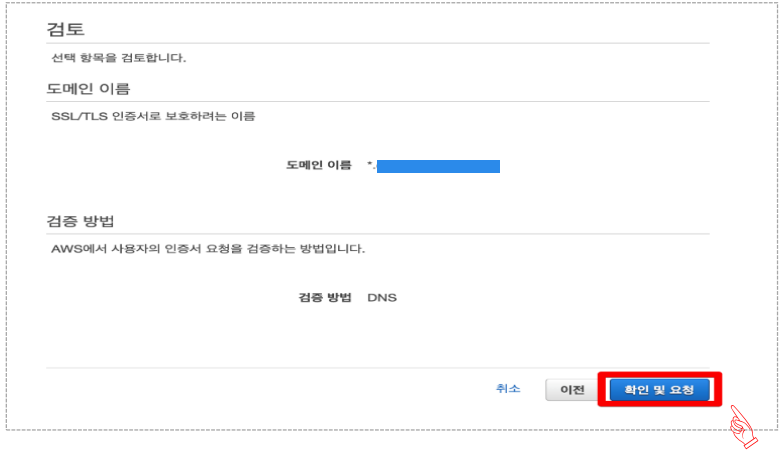


AWS Certificate Manager(ACM) 무료 인증서

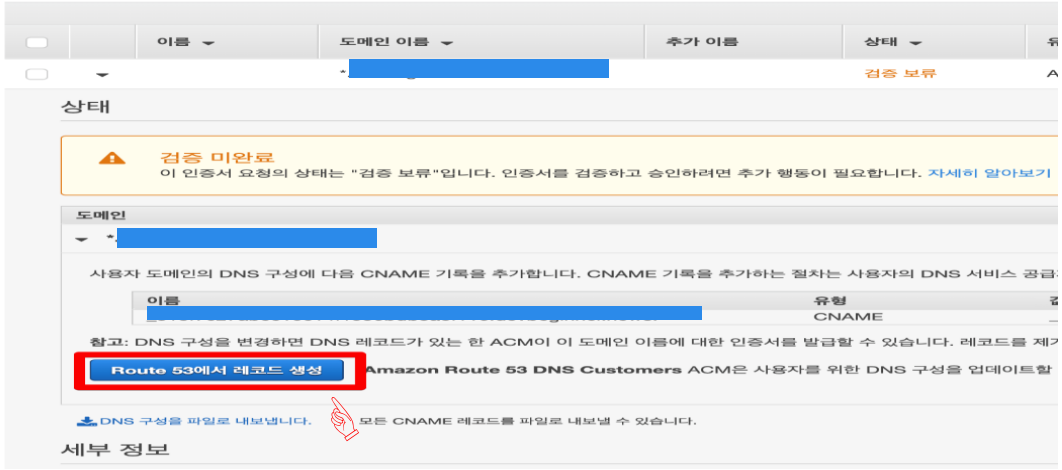


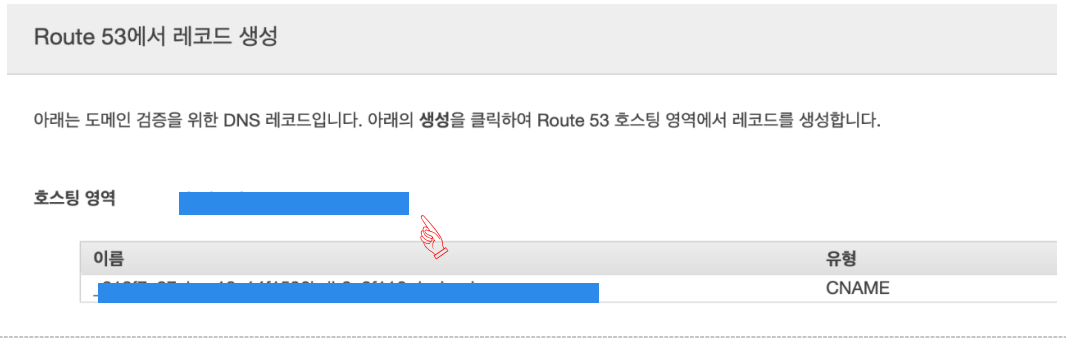
AWS Certificate Manager(ACM) 무료 인증서



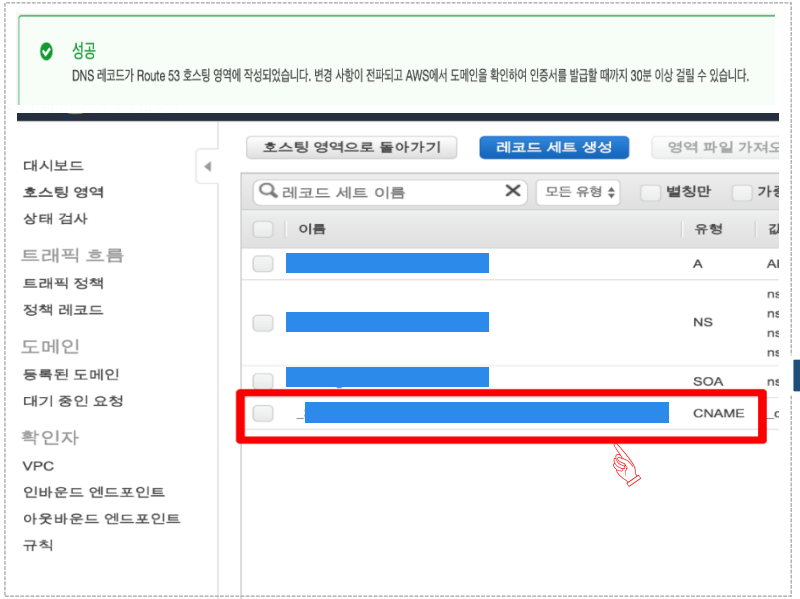


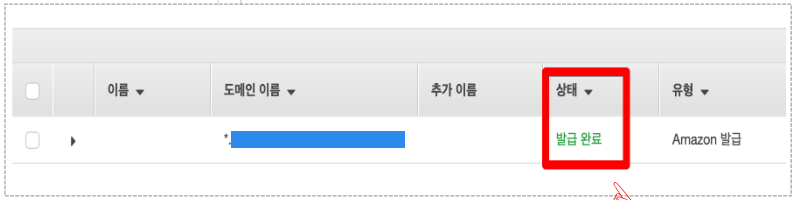
AWS Certificate Manager(ACM) 무료 인증서

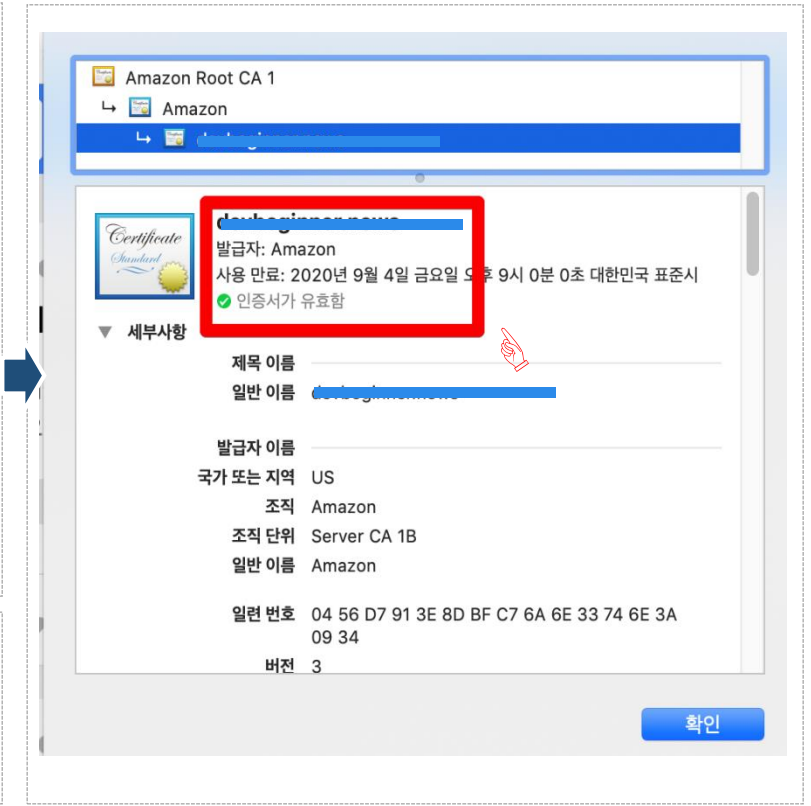




AWS Certificate Manager(ACM) 무료 인증서



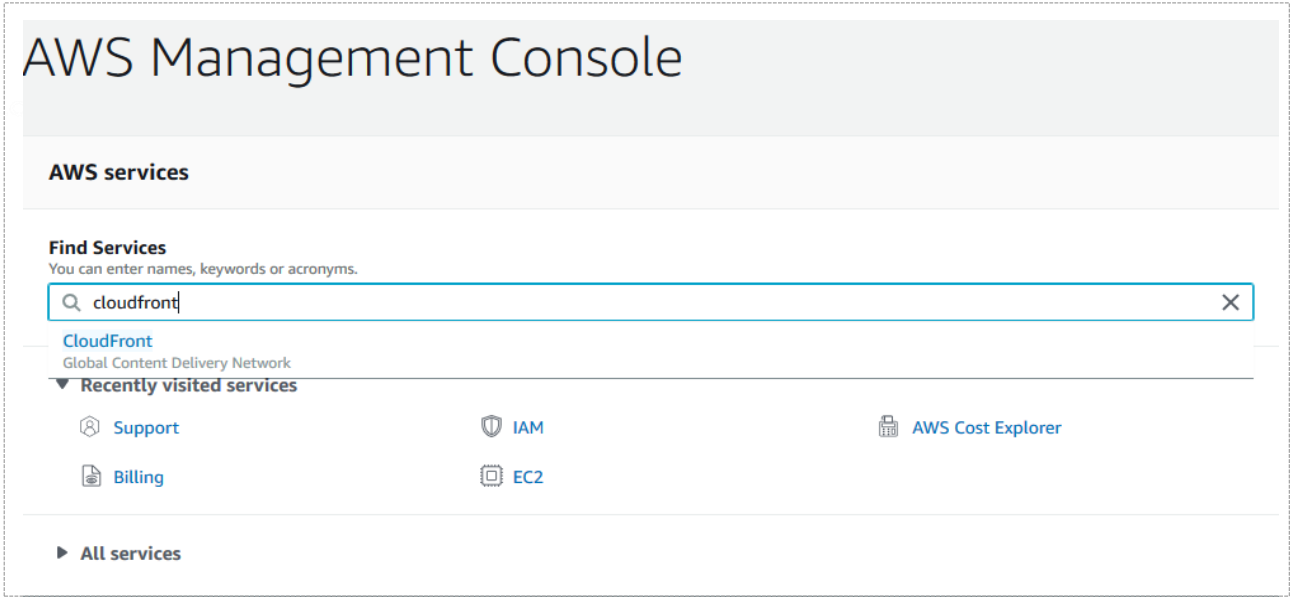




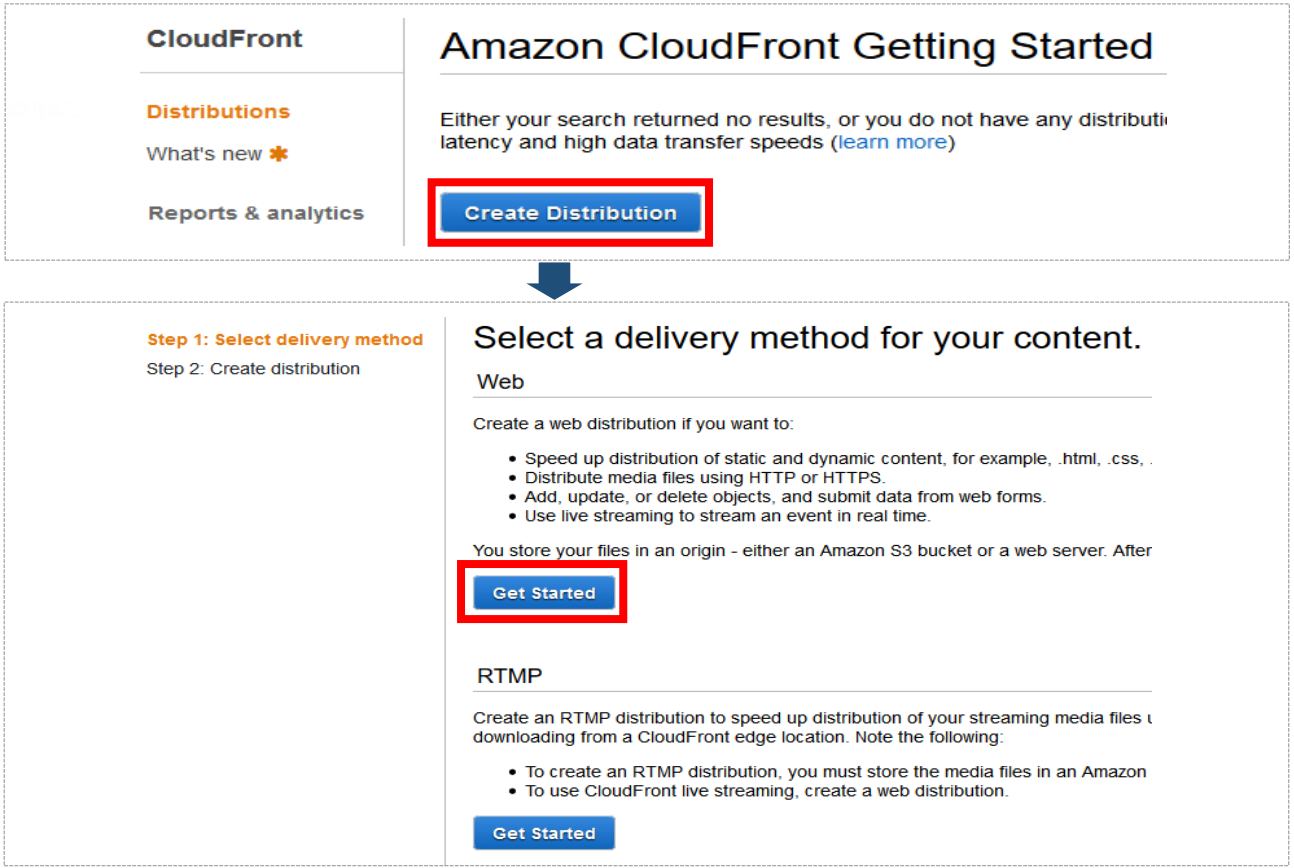
AGENDA

1. AWS Certificate Manager (ACM) 소개
2. AWS ACM 에서 무료 인증서 가져오기
3. **CloudFront 에 AWS ACM 사용하기**

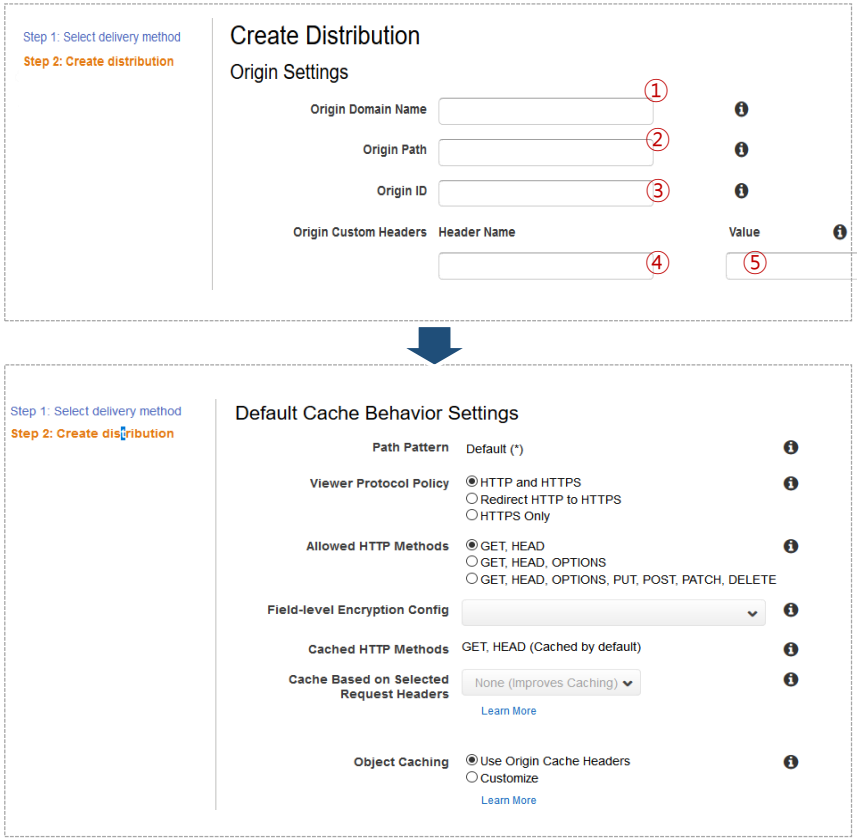
CloudFront 에 AWS ACM 사용하기



CloudFront 에 AWS ACM 사용하기



CloudFront 에 AWS ACM 사용하기



① • Origin Domain Name : 필드를 클릭하고 오리진의 도메인 이름 (Amazon S3 버킷, AWS MediaPackage 채널 엔드 포인트, AWS MediaStoreContainer 엔드 포인트 또는 CloudFront이 웹 컨텐츠를 가져올 웹 서버)을 지정하십시오. 예를 들어 Amazon S3 버킷의 경우 이름을 bucketname.s3.amazonaws.com 형식으로 입력하십시오. 오리진의 파일은 공개적으로 읽을 수 있어야합니다.

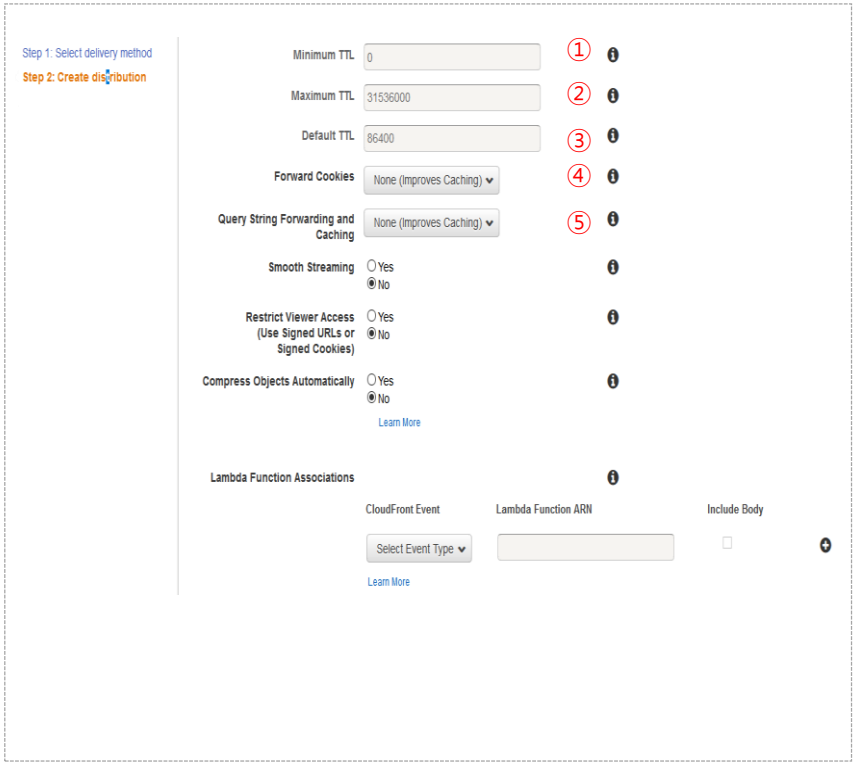
② • Origin Path : CloudFront가 Amazon S3 버킷의 디렉토리 또는 사용자 지정 오리진에서 컨텐츠를 요청하도록하려면 /로 시작하는 디렉토리 이름을 여기에 입력하십시오. CloudFront는 요청을 오리진 (예 : myawsbucket / production)에 전달할 때 디렉토리 이름을 오리진 도메인 이름 값에 추가합니다. 디렉토리 이름 끝에 /를 포함하지 마십시오.

③ • Origin ID : 원점에 대한 설명을 입력하십시오. 이 값을 사용하면 동일한 분포의 여러 원점을 서로 구별 할 수 있습니다. 각 원점에 대한 설명은 분포 내에서 고유해야합니다.

④ • Origin Custom Headers Header Name : 여기에 지정하는 모든 사용자 지정 헤더 키와 값은이 원본에 대한 모든 요청에 포함됩니다. 클라이언트 요청에 헤더가 이미 제공된 경우 대체됩니다.

⑤ • 기본 값으로 설정

CloudFront 에 AWS ACM 사용하기



① • Minimum TTL : CloudFront가 객체가 업데이트되었는지 여부를 확인하기 위해 다른 요청을 오리진에 전달하기 전에 객체가 CloudFront 캐시에 머무르기를 원하는 최소 시간 (초)입니다. Minimum TTL은 Cache-Control max-age, Cache-Control s-maxage 및 Expires와 같은 HTTP 헤더와 기본 TTL 및 Maximum TTL과 상호 작용합니다.

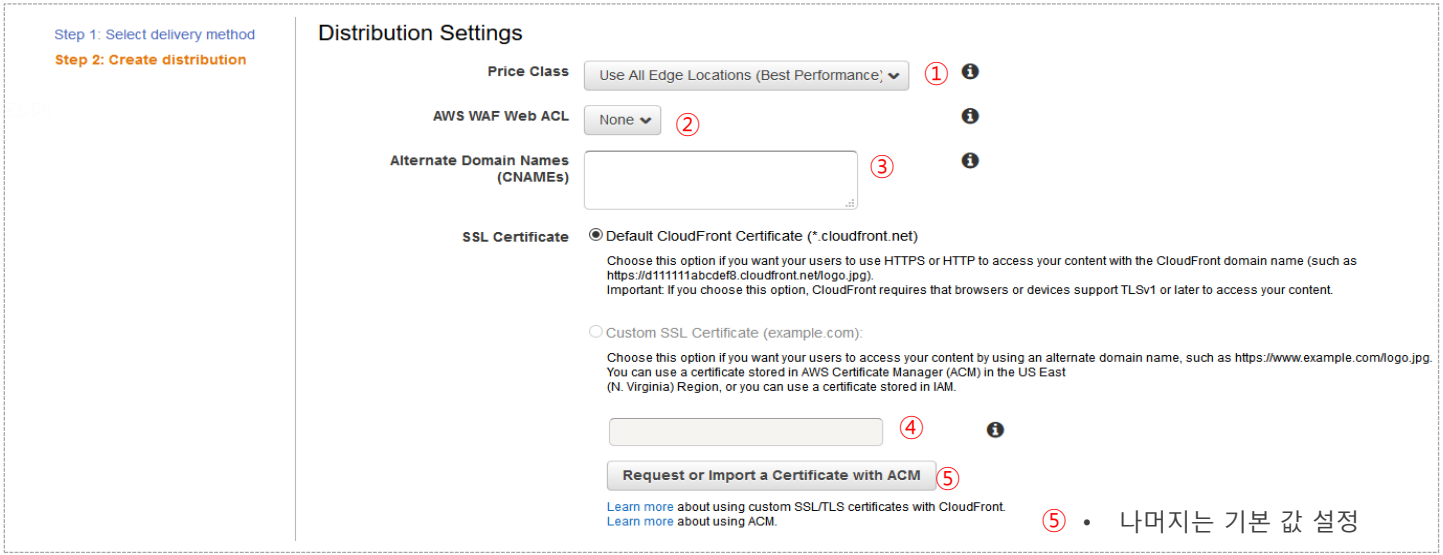
② • Maximum TTL : CloudFront가 객체가 업데이트되었는지 여부를 확인하기 위해 다른 요청을 오리진에 전달하기 전에 객체가 CloudFront 캐시에 머무르기를 원하는 최대 시간 (초)입니다. 지정하는 값은 원본이 Cache-Control max-age, Cache-Control s-maxage 및 Expires와 같은 HTTP 헤더를 객체에 추가 할 때만 적용됩니다.

③ • Default TTL : CloudFront가 객체가 업데이트되었는지 여부를 확인하기 위해 다른 요청을 오리진에 전달하기 전에 객체가 CloudFront 캐시에 유지되기를 원하는 기본 시간 (초)입니다. 지정하는 값은 원본이 Cache-Control max-age, Cache-Control s-maxage 및 Expires와 같은 HTTP 헤더를 객체에 추가하지 않는 경우에만 적용됩니다.

④ • Forword Cookies : CloudFront가 요청 URL에 오리진 (모두), 선택한 쿠키만 (허용 목록) 또는 쿠키 없음 (없음)으로 전달하는 요청 URL에 모든 사용자 쿠키를 포함 시킬지 여부를 선택합니다. 화이트리스트를 선택한 경우 쿠키 이름을 화이트리스트 쿠키 필드에 추가하십시오. Amazon S3 및 일부 HTTP 서버는 쿠키를 처리하지 않습니다.

⑤ • Query String Forwarding and Caching : CloudFront가 오리진으로 전달할 쿼리 문자열 파라미터 (모두 또는 없음)와 CloudFront가 캐싱을 기반으로 할 파라미터 (파라미터의 화이트리스트 또는 모두)를 선택합니다. CloudFront가 오리진에 전달해야하는 요청 수를 줄이려면 가능한 최소 값 조합이있는 매개 변수를 기반으로 캐시하도록 CloudFront를 구성하는 것이 좋습니다. Amazon S3 및 일부 HTTP 서버는 쿼리 문자열 파라미터를 처리하지 않습니다.

CloudFront 에 AWS ACM 사용하기



⑤ • 나머지는 기본 값 설정

① • Price Class : CloudFront 서비스에 대해 지불하려는 최대 가격과 관련된 가격 등급을 선택하십시오. 모두 이외의 가격 등급을 선택하면 일부 사용자의 대기 시간이 길어질 수 있습니다.

② • AWS WAF Web ACL : AWS WAF를 사용하여 지정한 기준에 따라 요청을 허용 또는 차단하려면 이 배포와 연결할 웹 ACL을 선택하십시오.

③ • Alternate Domain Names (CNAMEs) : 파일의 URL에 대해 CloudFront 도메인 이름 (예 : d1234.CloudFront.net) 외에 사용하는 모든 사용자 지정 도메인 이름 (예 : www.example.com)을 나열해야 합니다. 쉼표로 구분하여 최대 100 개의 CNAME을 지정하거나 각각을 새 줄에 입력하십시오. 또한 www.example.com에 대한 쿼리를 d1234.CloudFront.net으로 라우팅하려면 DNS 서비스로 CNAME 레코드를 만들어야 합니다. 자세한 내용은 도움말을 참조하십시오.

④ • SSL Certificate : HTTPS 프로토콜 사용을 위한 인증서 설정이다. Default CloudFront Certificate를 선택하면 CloudFront의 인증서를 기본으로 사용한다. Custom SSL Certificate를 선택할 경우 자신이 가지고 있는 인증서를 사용할 수 있습니다.

APPENDIX

참고 사항

- **AWS Certificate Manager(ACM)란 무엇입니까?**

  ✓ AWS Certificate Manager는 AWS 서비스 및 연결된 내부 리소스에 사용할 공인 및 사설 SSL/TLS(Secure Sockets Layer/전송 계층 보안) 인증서를 손쉽게 프로비저닝, 관리 및 배포할 수 있도록 지원하는 서비스입니다. SSL/TLS 인증서는 네트워크 통신을 보호하고 인터넷상에서 웹 사이트의 자격 증명과 프라이빗 네트워크상에서 리소스의 자격 증명을 설정하는 데 사용됩니다. AWS Certificate Manager는 SSL/TLS 인증서를 구매, 업로드 및 갱신하는 데 드는 시간 소모적인 수동 프로세스를 대신 처리합니다. AWS Certificate Manager에서는 사용자가 신속하게 인증서를 요청하고, Elastic Load Balancer, Amazon CloudFront 배포, API Gateway 기반 API와 같은 AWS 리소스에 배포한 후, AWS Certificate Manager가 인증서 갱신을 처리하도록 할 수 있습니다. 또한, 내부 리소스에 대한 사설 인증서를 생성하고 중앙에서 인증서 수명 주기를 관리할 수도 있습니다. AWS Certificate Manager를 통해 프로비저닝되고 ACM 통합 서비스(Elastic Load Balancing, Amazon CloudFront, Amazon API Gateway 등)에만 전용으로 사용되는 공인 및 사설 SSL/TLS 인증서는 무료입니다. 사용자는 애플리케이션을 실행하기 위해 생성한 AWS 리소스에 대한 비용을 지불합니다. 고객은 각 사설 CA의 운영에 대해 해당 CA를 삭제할 때까지 그리고 발급한 사설 인증서 중 ACM 통합 서비스 이외 다른 서비스에서도 사용된 인증서에 대해 월별 요금을 지불합니다.

참고 사항

- **SSL/TLS?**
  - ✓ SSL/TLS 인증서는 SSL/TLS(Secure Sockets Layer/전송 계층 보안) 프로토콜을 사용하여 웹 브라우저가 웹 사이트에 대해 암호화된 네트워크 연결을 확인하고 설정할 수 있게 해줍니다. 인증서는 퍼블릭 키 인프라(PKI)로 알려진 암호화 시스템 내에서 사용됩니다. 양쪽 모두가 인증 기관으로 알려진 타사를 신뢰하는 경우, PKI는 한쪽에서 인증서를 사용하여 다른 쪽의 자격 증명을 설정할 수 있는 방법을 제공합니다. ACM 사용 설명서의 개념 항목에 추가 배경 정보와 정의가 나와 있습니다.

- **사설 인증서란?**
  - ✓ 사설 인증서는 애플리케이션, 서비스, 디바이스 및 사용자와 같은 조직 내 리소스를 식별합니다. 암호화된 보안 통신 채널을 구성할 때 각 엔드포인트가 인증서와 암호화 기법을 사용하여 다른 엔드포인트에 자격 증명을 제공합니다. 내부 API 엔드포인트, 웹 서버, VPN 사용자, IoT 디바이스 및 다른 많은 애플리케이션에서 사설 인증서를 사용하여 보안 작업에 필요한 암호화된 통신 채널을 구성합니다.

참고 사항

- **공인 인증서와 사설 인증서의 차이점은?**

  ✓ 공인 인증서와 사설 인증서 모두 고객이 네트워크상의 리소스를 식별하고 이러한 리소스 간 통신을 보호하는 데 도움이 됩니다. 공인 인증서는 퍼블릭 인터넷상의 리소스를 식별하고 사설 인증서는 프라이빗 네트워크상의 리소스를 식별합니다. 큰 차이점 하나는 기본적으로 애플리케이션과 브라우저에서는 공인 인증서를 자동으로 신뢰하는 반면, 사설 인증서의 경우 애플리케이션에서 신뢰하도록 관리자가 명시적으로 구성해야 합니다. 공인 인증서를 발급하는 엔터티인 공인 CA는 엄격한 규칙을 준수하고, 운영 가시성을 제공하고, 브라우저 및 운영 체제가 자동으로 신뢰할 CA를 결정하는 브라우저 및 운영 체제 공급업체가 도입한 보안 표준을 충족해야 합니다. 사설 CA는 사설 조직에서 관리하며, 사설 CA 관리자는 인증서 발생에 대한 사례, 인증서에 포함할 수 있는 정보를 비롯하여 사설 인증서 발급에 대한 자체 규칙을 생성할 수 있습니다. 사설 인증서와 사설 CA에 대해 자세히 알아보려면 아래 ACM 사설 인증 기관을 참조하십시오.