AWS 101

아마존 웹서비스(AWS)와 함께하는 클라우드 컴퓨팅

윤석찬

AWS코리아, 테크에반젤리스트

© 2015, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

amazon web services

AWS와 함께 하는 4주 클라우드 보안 강의

- 5월 2일 **클라우드 컴퓨팅 및 AWS 소개**
- 5월 9일 **AWS 주요 서비스 사용 실습** (S3 및 CloudFront)
- 5월 23일 **AWS 보안 관리 서비스 소개**
- 5월 30일 **AWS 보안 관리 서비스 실습** (WAF, IAM)

amazon web services

목차

1. AWS IAM으로 사용자 및 그룹 만들기
2. Amazon S3 클라이언트 프로그램 사용해 보기
3. AWS WAF 설정해 보기
4. AWS WAF로 접근 제어 해 보기

amazon web services

10분 자습서

10분 자습서는 AWS를 체험할 수 있는 간단한 "Hello, World!" 기술 문서입니다.

10분 자습서

Linux 가상 머신 시작

Amazon EC2 사용

10분 자습서

Windows 가상 머신 시작

Amazon EC2 사용

10분 자습서

WordPress 웹 사이트 시작

Amazon EC2와 AWS Marketplace 사용

10분 자습서

도메인 이름 등

Amazon EC2 사용

10분 자습서

파일 저장 및 검색

Amazon S3 사용

10분 자습서

여러 파일 저장

AWS CLI를 사용해

10분 자습서

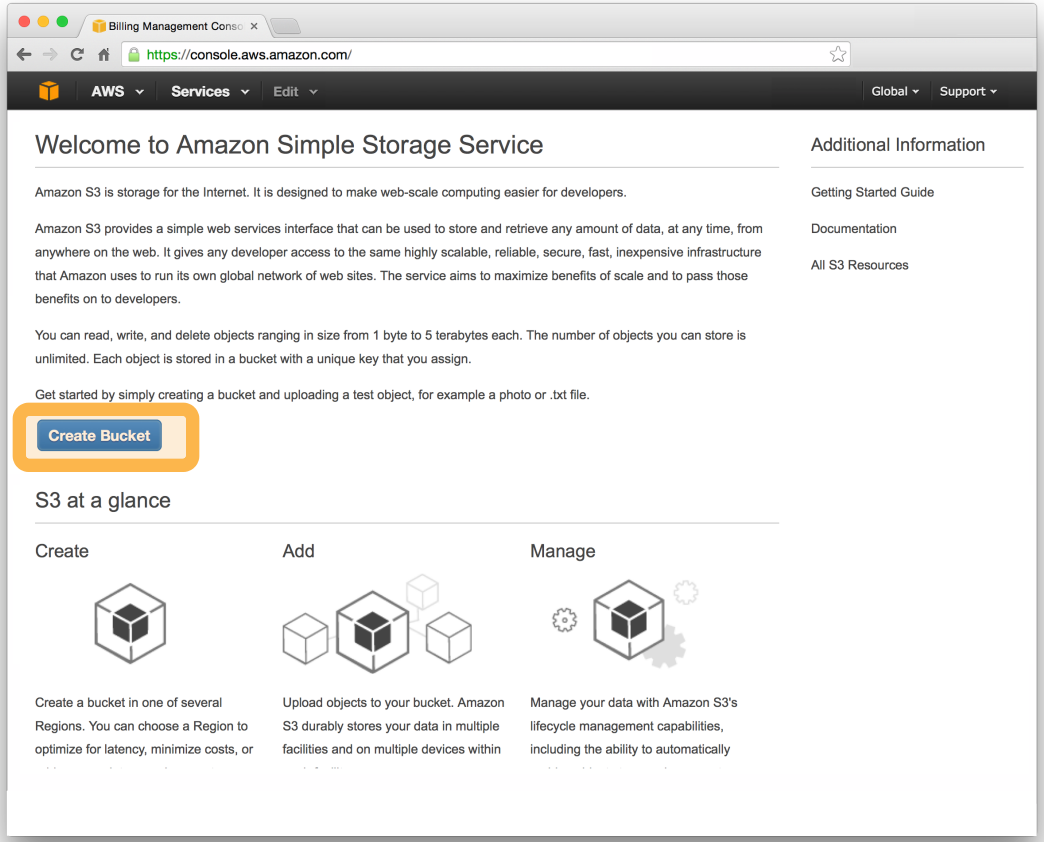
웹 애플리케이션 시작

10분 자습서

웹 애플리케이

업데이트

Amazon S3 시작하기



Amazon S3에 첫화면에서

Create Bucket

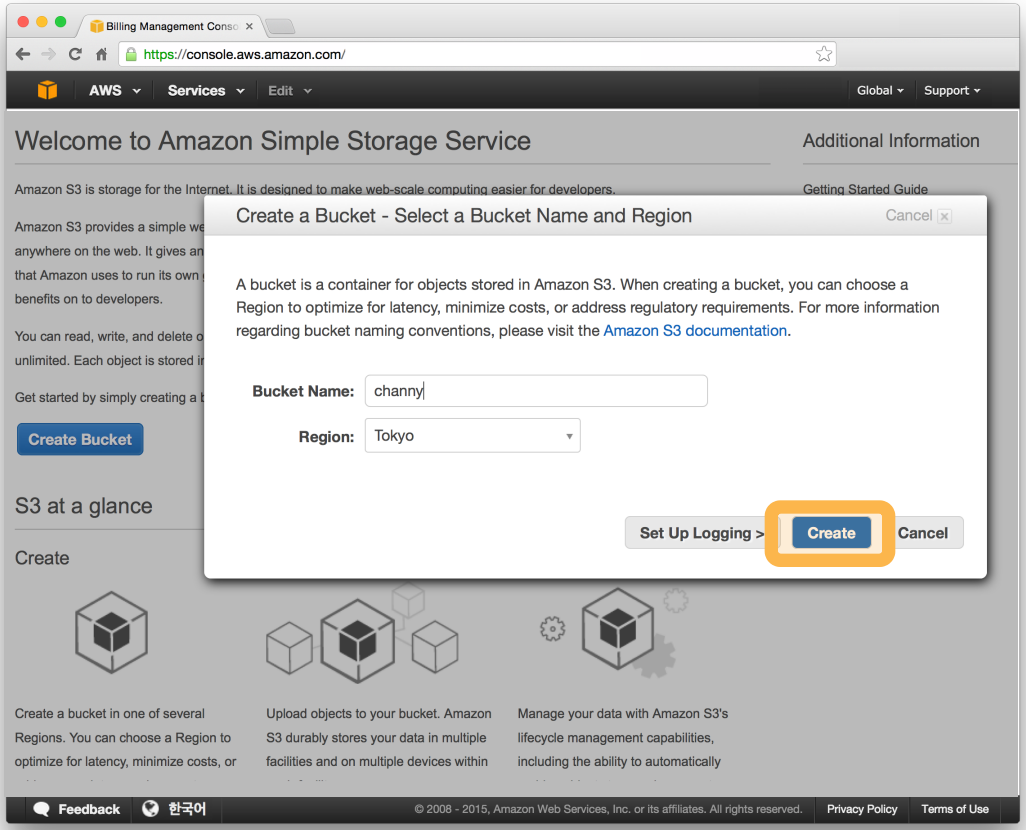
버튼을 누릅니다.

도움말: 버킷(Bucket)이란?

아이스버킷 챌린지에서 얼음이 든 양동이를 뒤집어 쓰던 IT업계 CEO들을 기억하십니까? 네... 바로 그 "양동이"입니다. 파일을 담는 폴더 개념으로 옆 아이콘이 버킷입니다.

amazon web services

단계 1. 버킷 생성하기



원하는 버킷이름을 선택합니다.

버킷 이름은 도메인 네임처럼 누가 미리 가지고 있을 수 있으니, 독특한 것으로 합니다.

파일이 저장될 리전(Region)을 선택합니다.

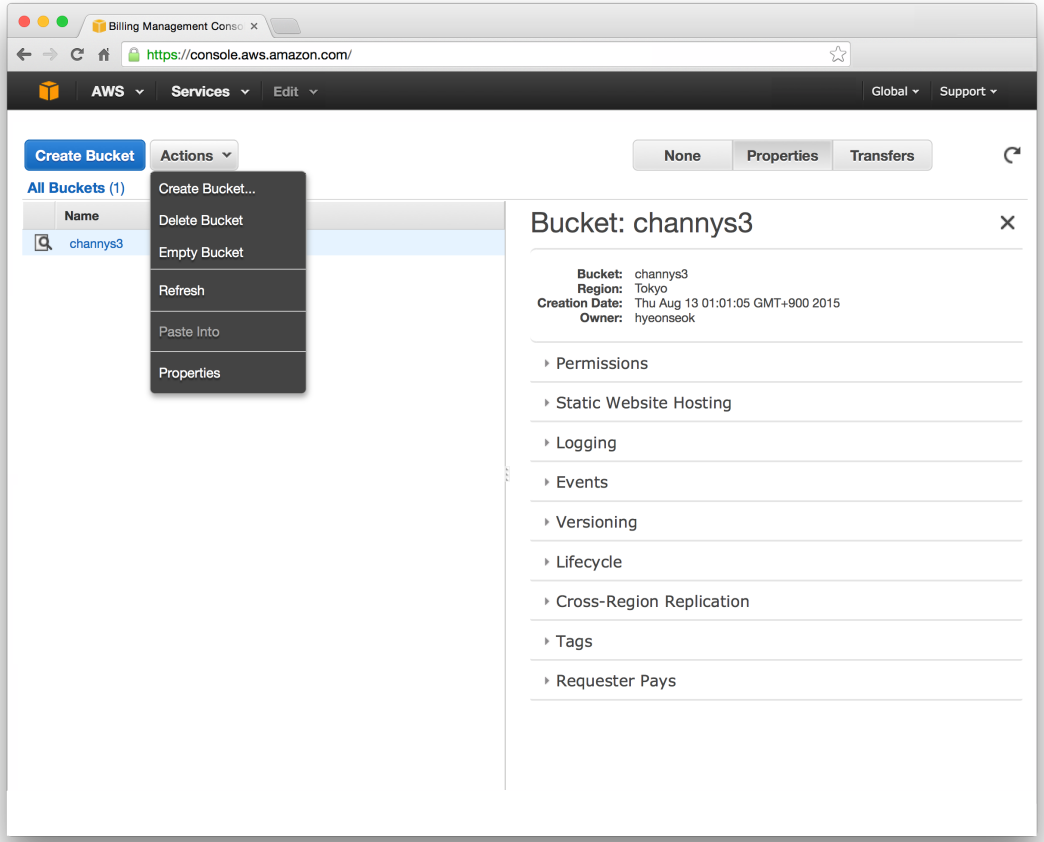
우리는 가까운 동경을 선택합니다.

도움말

Amazon S3에서 저장되는 파일은 어느 리전을 선택하더라도 모든 버킷과 파일이 한 곳에 모여서 나옵니다. 따라서, S3는 오른쪽 상단의 리전 위치를 선택할 필요는 없습니다.

amazon web services

단계 1. 버킷 생성하기



Action을 누르면, 버킷을 생성/삭제/비우기 등을 할 수 있습니다.

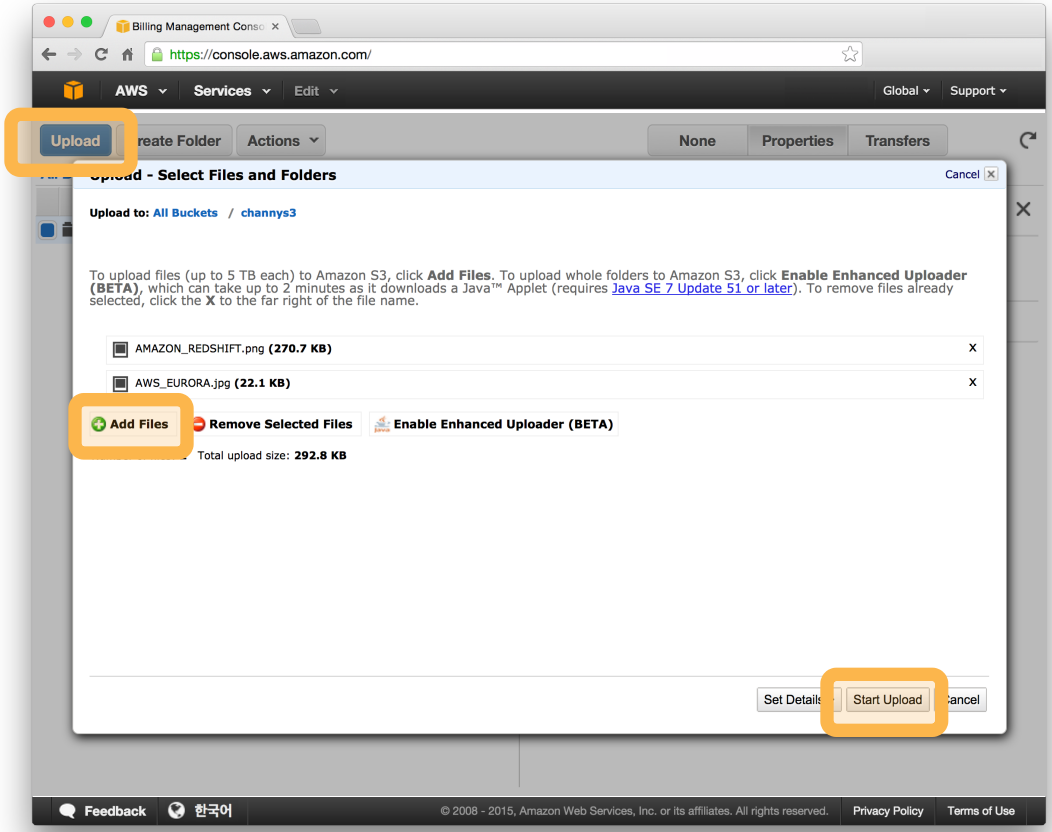
버킷은 파일의 종류를 구분하는 용도로 사용되며, 폴더처럼 한꺼번에 지우거나 할 수가 없습니다. 따라서, 버킷을 없애려면 버킷내 파일을 모두 삭제해야만 가능합니다.

도움말

Amazon S3는 객체(Object) 저장소입니다. 즉, 특정 객체만 담는 저장소입니다. 버킷은 폴더처럼 보이지만 단순히 파일 종류를 구분해 주는 용도로 사용자 편의상 폴더 인터페이스로 보입니다.

amazon web services

단계 2. 파일 업로드 하기



버킷 내에서 폴더를 만들 수도 있고, 파일을 업로드할 수도 있습니다.

Upload

Upload를 눌러 새로운 파일을 올려 볼까요?

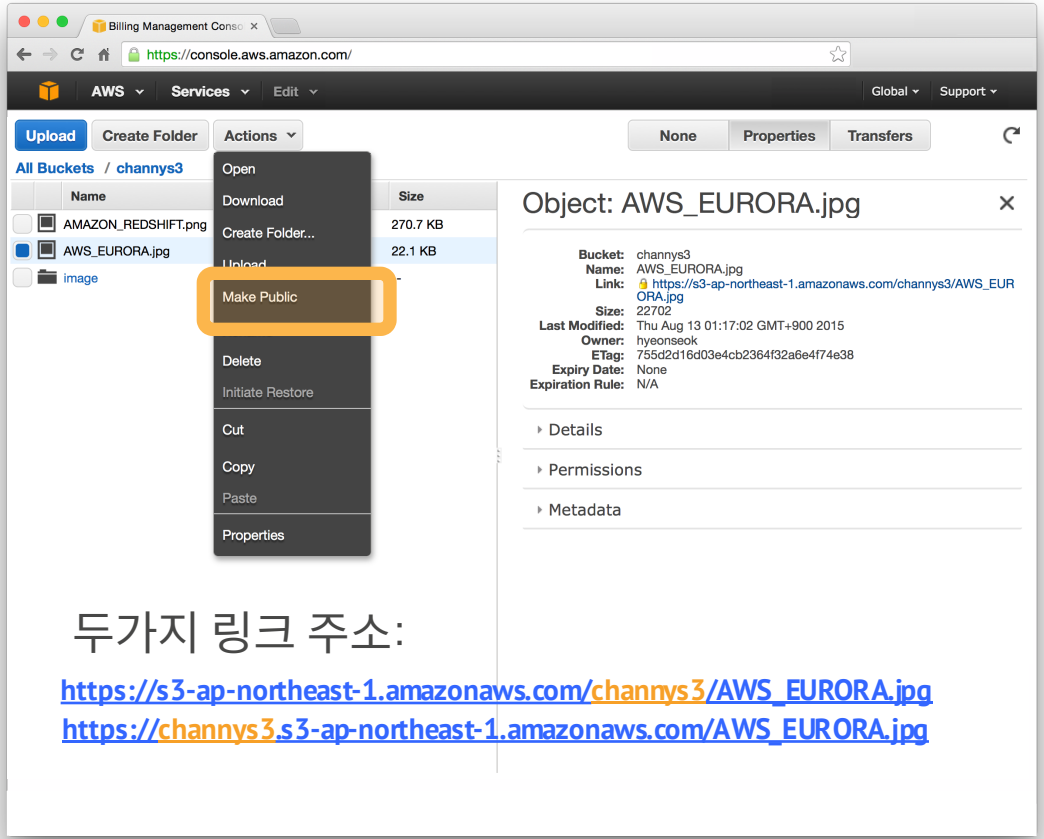
도움말

None | Properties | Transfers

오른쪽 상단의 None을 누르면, 목록만 보이며, Properties를 누르면 속성 정보 그리고 Transfers를 누르면 파일 전송 상태를 볼 수 있습니다.

amazon web services

단계 3. 파일 정보 보기



두가지 링크 주소:

https://s3-ap-northeast-1.amazonaws.com/channys3/AWS_EURORA.jpg
https://channys3.s3-ap-northeast-1.amazonaws.com/AWS_EURORA.jpg

파일을 선택하고 “Actions”를 누르면 원하는 기능을 수행할 수 있습니다. “Make Public”을 누르면, 누구나 Link 주소로 접속가능합니다.

열쇠 아이콘은 **비공개**, RSS아이콘이면 **공개**입니다.

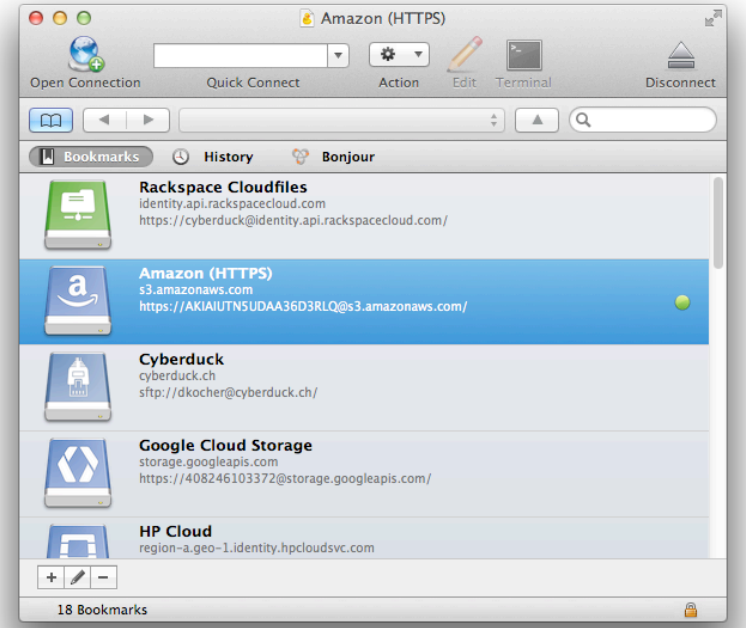
도움말

Amazon S3의 모든 객체는 정해진 URL을 가지며, 인터넷을 통해 접속할 수 있습니다. 기본적으로 비공개 상태로 파일이 저장되며, 공개를 하거나 또는 특정인 혹은 앱에게만 선별적으로 공개하는 기능을 제공합니다.

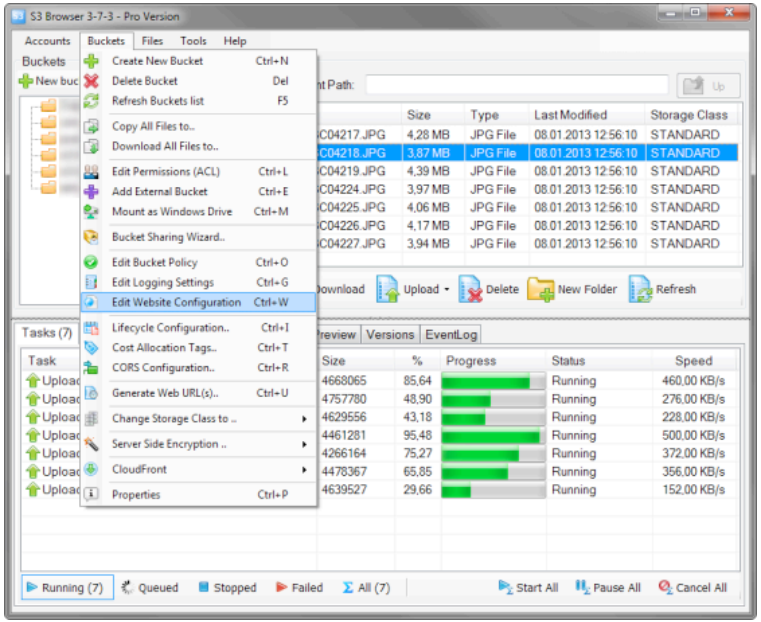
amazon web services

단계 4. 파일 업로드 프로그램

내 PC에서 손쉽게 파일 업로드 및 다운로드 가능합니다!



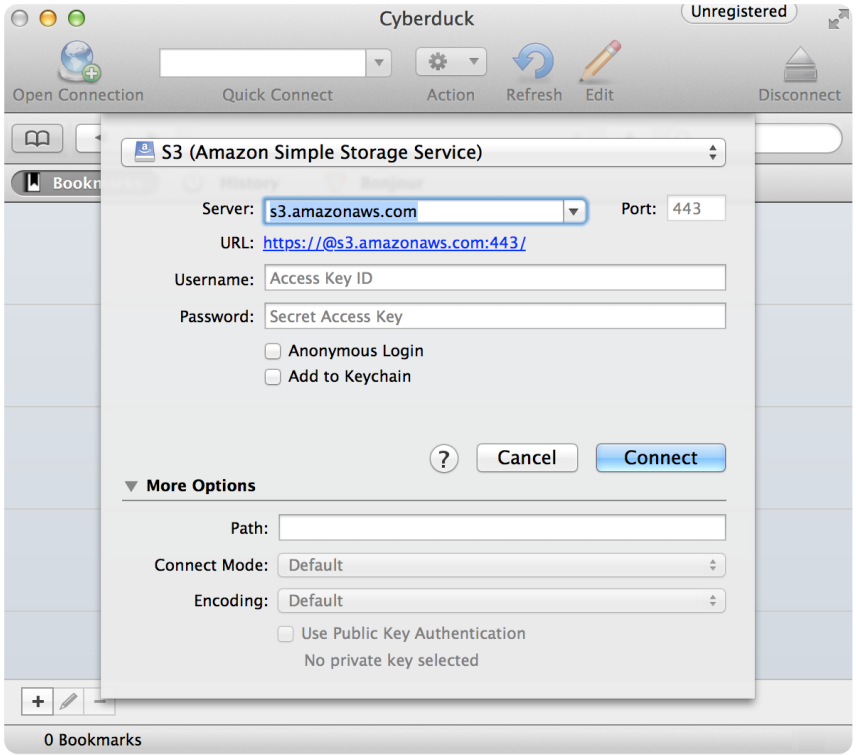
https://cyberduck.io/

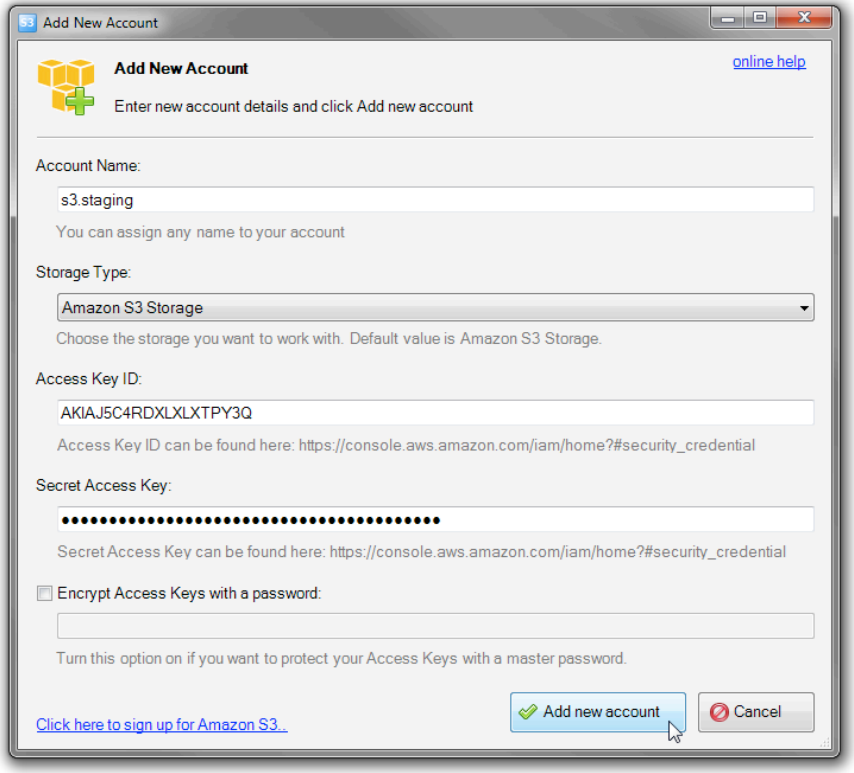


https://s3browser.com

amazon web services

앗! ID와 암호는 어떻게?

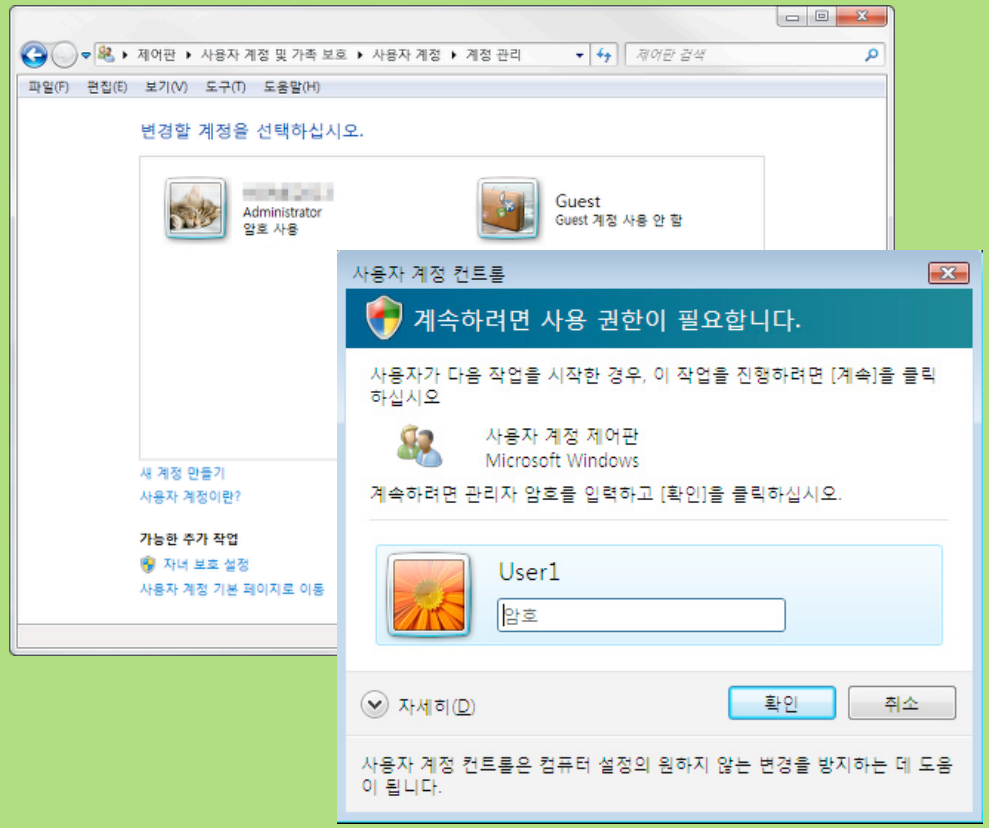




Access Key와 Secret Access Key를 필요로 합니다!

amazon web services

여러분 PC는 안전하십니까?

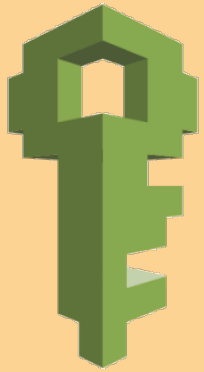


- 여러분의 PC에는 **"관리자"**와 **"일반 사용자"**가 있습니다.
- **"일반 사용자"**는 특정 권한만 가지고 있습니다.
- 만약, 모든 사람이 **"관리자"** 권한을 가지고 있으면 PC 보안에 취약합니다.

amazon web services

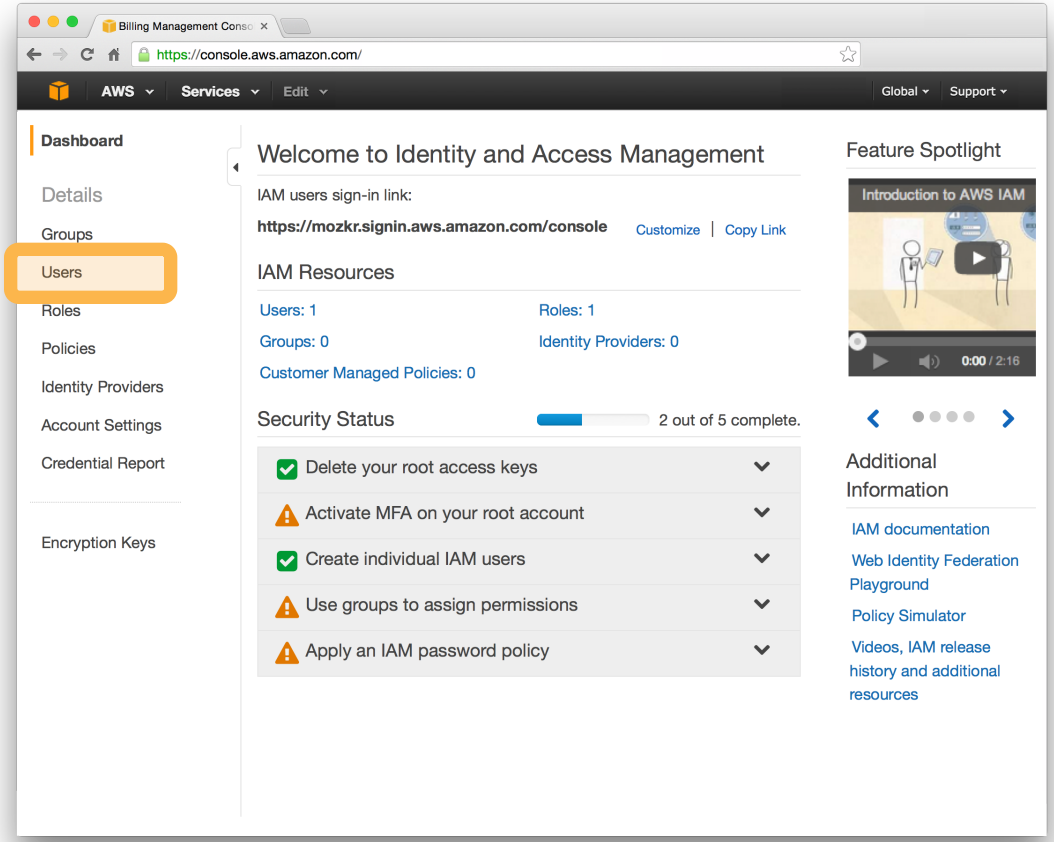
AWS Identity and Access Management (IAM)

- AWS 사용자 및 그룹을 만들고 관리 가능
- 각 AWS 서비스 및 자원별 사용 권한 지정
- 역할 및 정책을 통해 손쉽게 자세한 권한 관리
- 기업내 사용자 관리 시스템과도 연동 지원
- 오프라인 기기(MFA)를 통한 인증 가능



amazon web services

AWS IAM 시작하기



Amazon S3에 접근 가능한 사용자를 생성하고, S3 클라이언트 프로그램으로 접속하기 위한 사용자의 Access Key와 Secret을 얻어 보도록 하겠습니다.

도움말

AWS IAM을 잘 활용하면, 여러분은 안전하게 AWS 서비스를 이용할 수 있습니다. 특히 IAM 첫화면 중앙의 다섯 가지 "Security Status"를 눈여겨 보시고 모든 ✅이 체크가 되게 하세요.

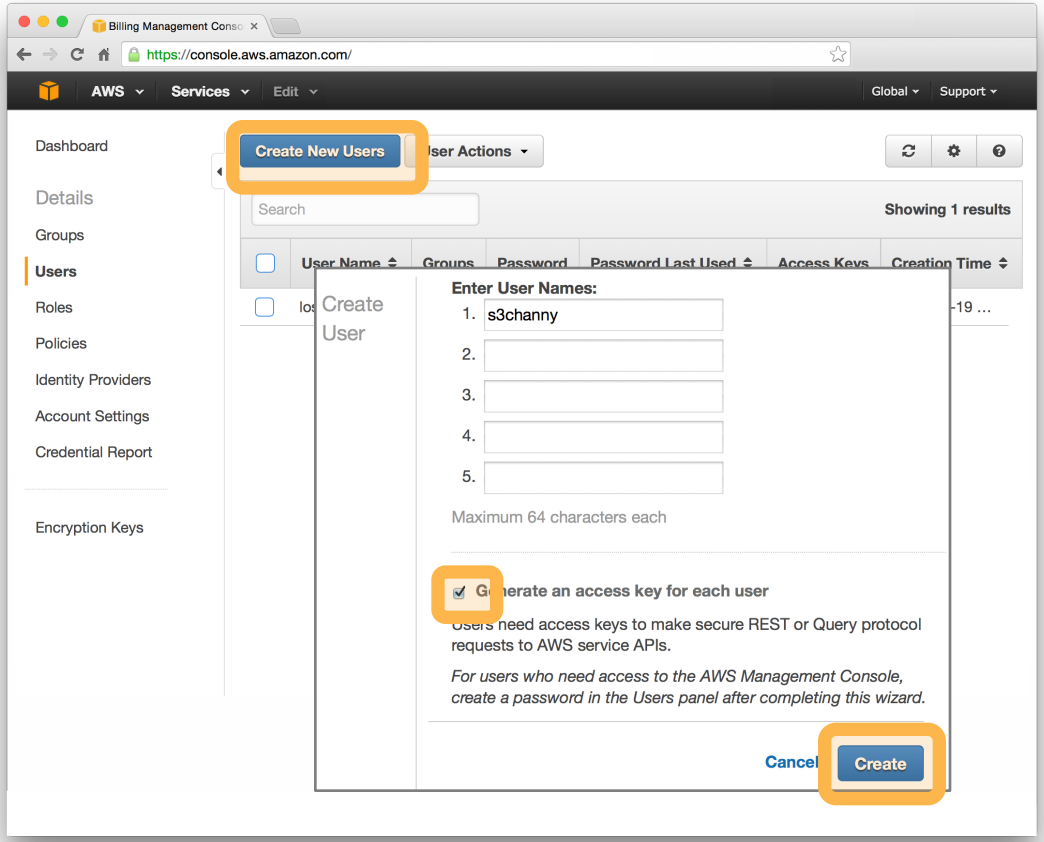
amazon web services

AWS의 다섯 가지 보안 팁

1. 루트 Access Key를 만들지도 쓰지도 맙시다!
   - 블로그나 책에 루트 AccessKey를 생성하는 예제 조심
2. 오프라인 기기 혹은 앱 인증을 꼭 사용합시다!
   - 중요 서비스일 경우, 꼭 모바일 앱 혹은 일회용 암호 생성기 이용
3. IAM 사용자를 생성하고 필요한 권한만 주세요!
   - 최소한의 권한을 주면 보안 위험도 낮아짐
4. IAM 그룹 생성을 통해 권한을 관리하세요!
   - 그룹을 통해 개발자, 관리자, 운영자 권한을 세분화
5. 암호 생성 조건을 꼭 설정하세요!
   - 탈취당하기 쉬운 암호 보다 좀 더 복잡한 암호를…

amazon web services

단계 1. IAM 사용자 생성



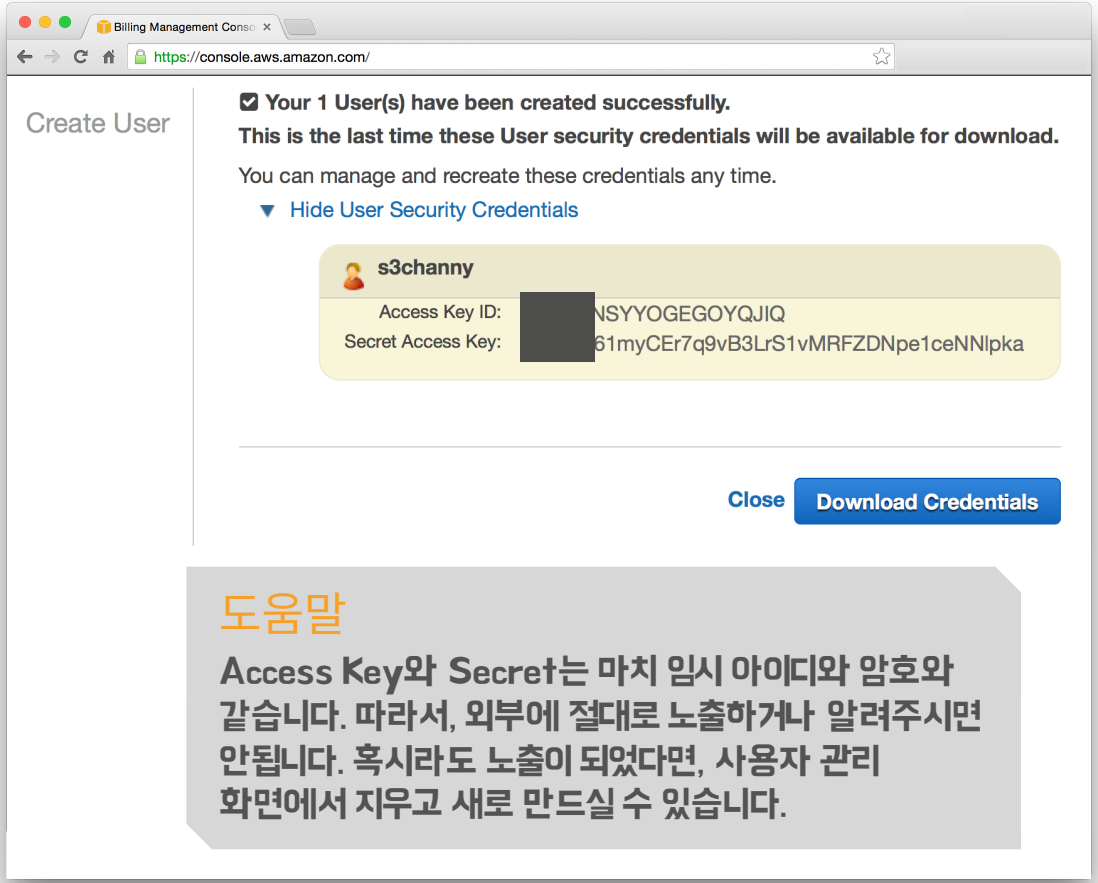
"Users"를 선택하고 "Create New Users"를 선택하면, 5개까지 일괄적으로 아이디를 만들 수 있습니다. S3 사용만 가능할 ID인 "s3channy"를 만듭니다.

도움말

아이디 생성 시 "Generate an access key for each user"를 체크하면, 각 사용자별로 랜덤 영문/숫자로 된 Access Key와 Secret을 만들 수 있습니다. S3 접속 프로그램 및 API 플러그인 사용등에 사용 가능합니다.

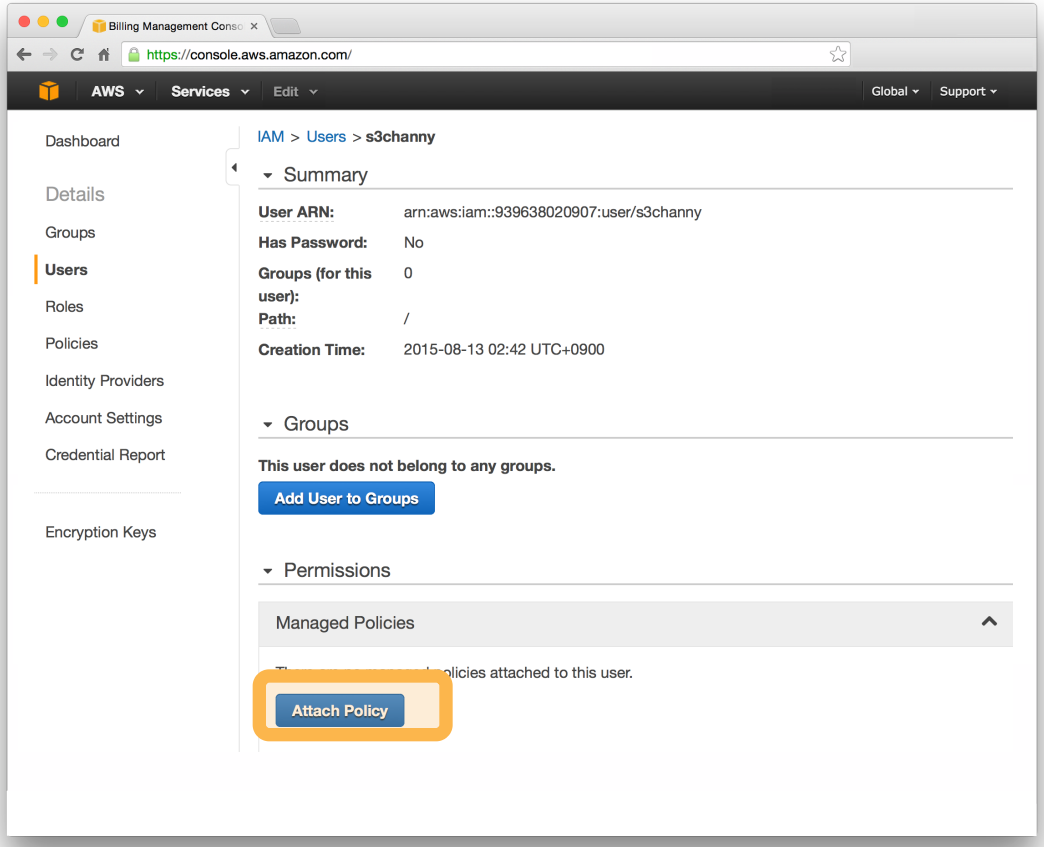
amazon web services

단계 2. 사용자 Credential 정보 받기



amazon web services

단계 3. 사용자 권한 지정



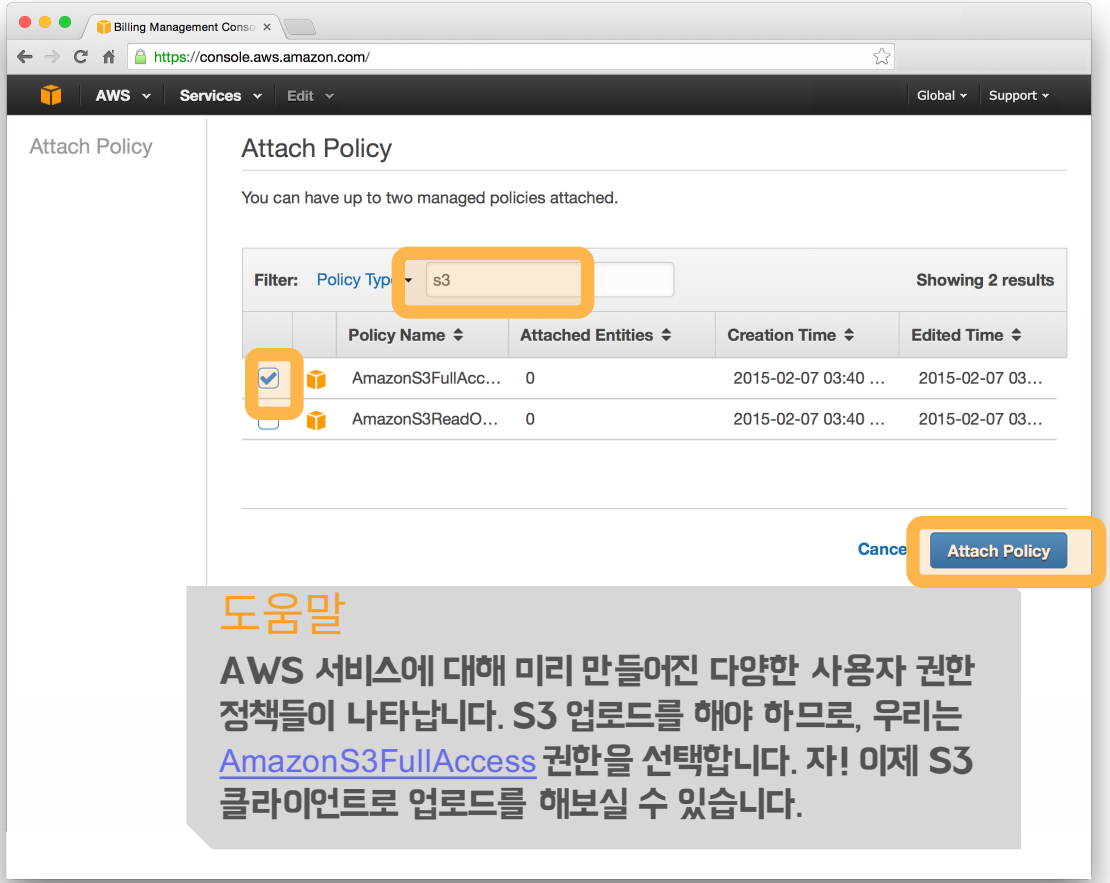
생성된 사용자를 선택하면, 그룹 추가, 권한 정책 설정, 키 관리, 암호 관리 등을 하실 수 있습니다. S3 접근 권한 관리를 위해 Attach Policy를 선택합니다.

도움말

아이디 생성 시 "Generate an access key for each user"를 체크하면, 각 사용자별로 랜덤 영문/숫자로 된 Access Key와 Secret을 만들 수 있습니다. S3 접속 프로그램 및 API 플러그인 사용등에 사용 가능합니다.

amazon web services

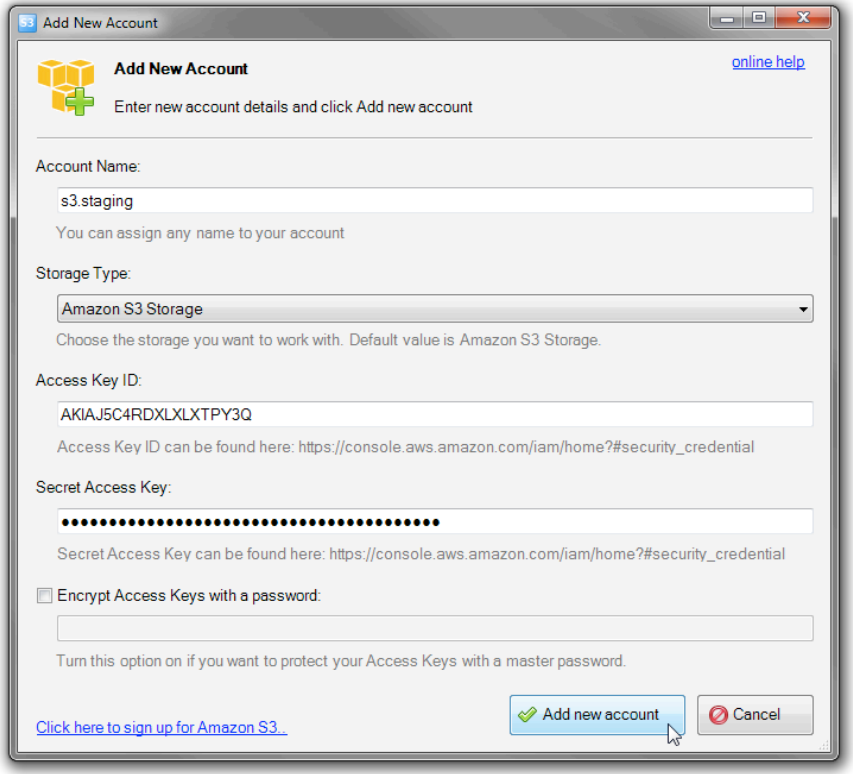
단계 4. 사용자 정책 검색 및 추가하기

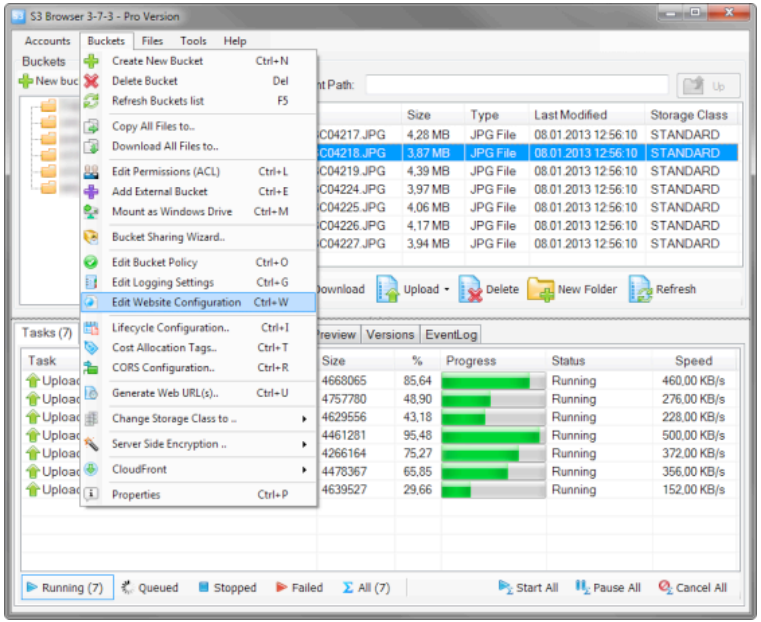


amazon web services

이제 S3에 파일을 업로드 해봅시다!

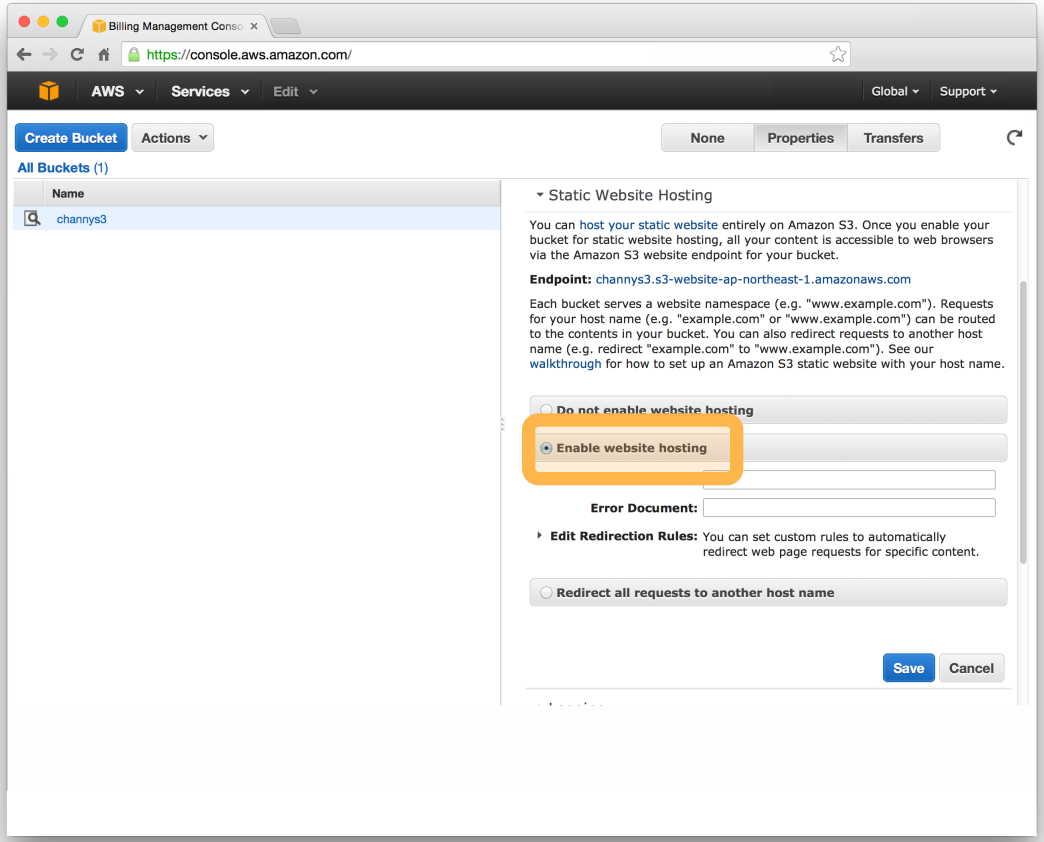
이제 여러분은 일년간 사용할 수 있는 **5GB짜리 무료 저장소**가 생겼습니다.





amazon web services

Amazon S3 정적 웹 사이트 호스팅



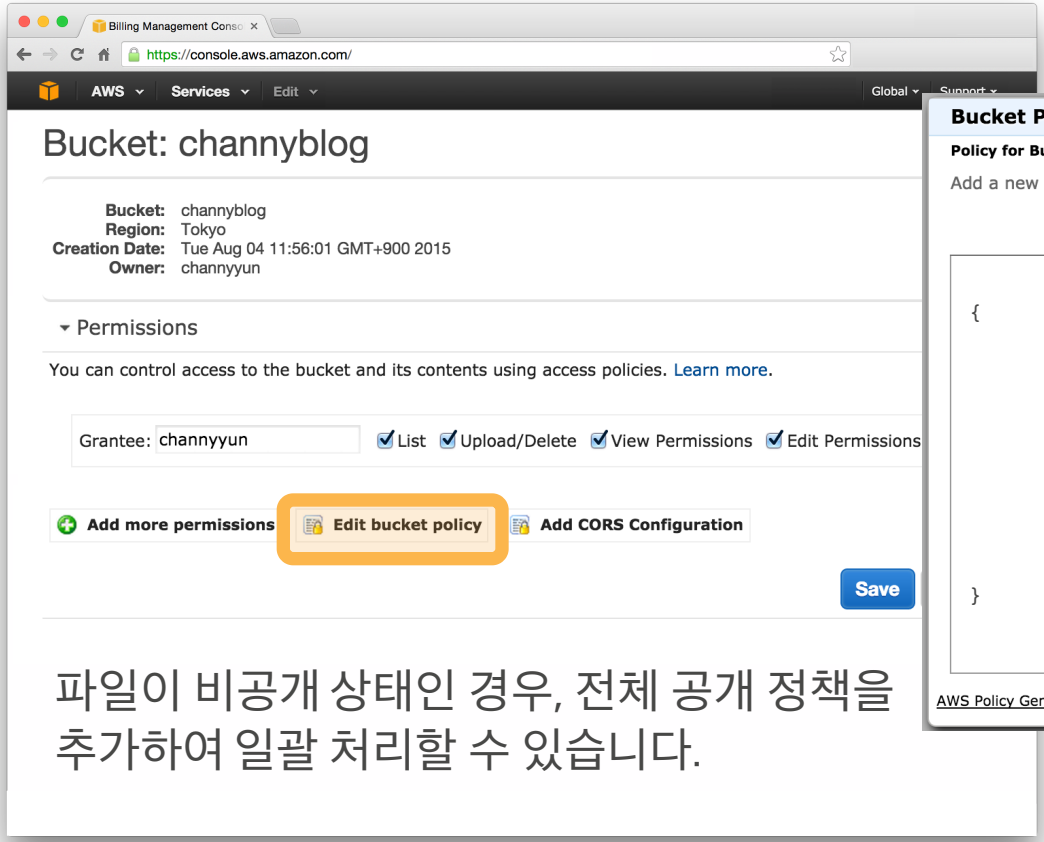
여러분의 버킷은 단순히 파일 저장 뿐만 아니라 간단한 웹 사이트 호스팅도 가능합니다. 이벤트 페이지나 간단한 개인 홈페이지를 서버 설정 없이도 제공 가능합니다.

도움말

버킷 Properties에서 “Static Web Site Hosting”을 선택하고 Enable을 시킵니다. 첫화면을 보여줄 index.html을 지정하면 됩니다. URL 접속시 바로 홈페이지가 나타납니다. 모든 파일은 공개 상태여야 합니다.

amazon web services

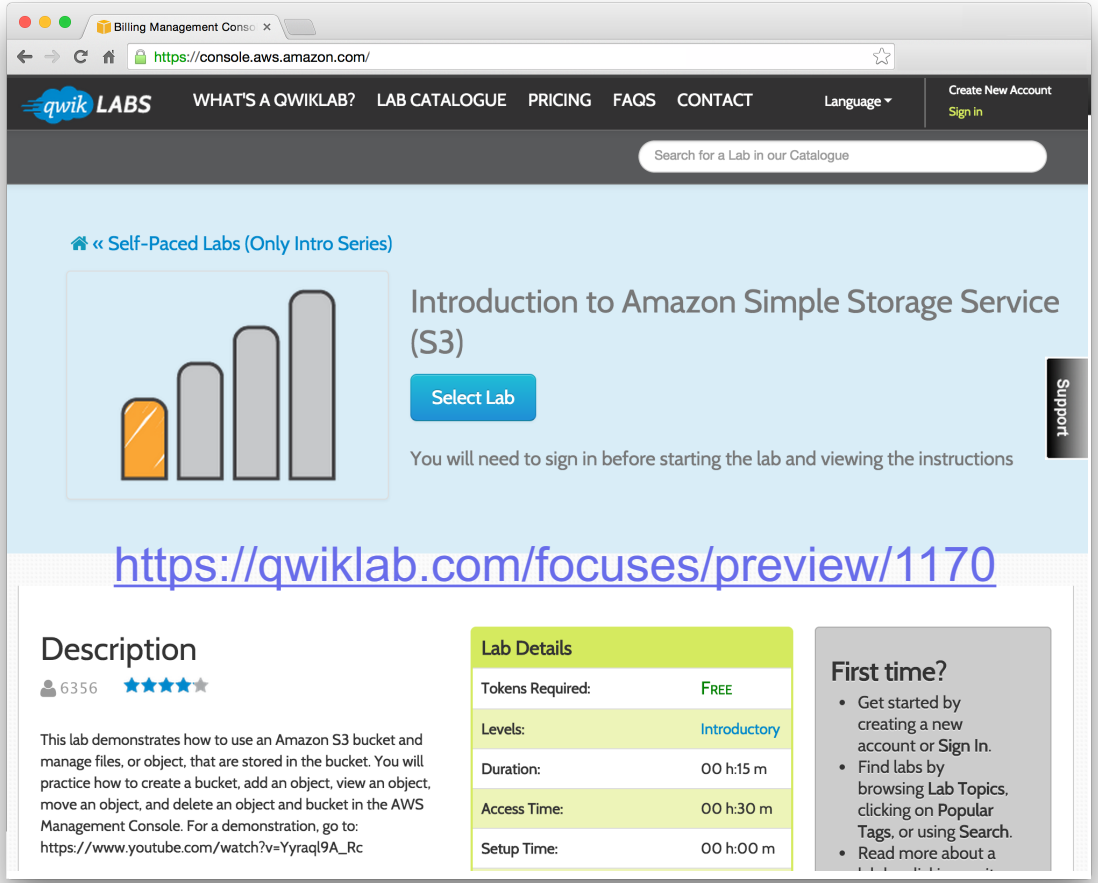
Tip1. 버킷 공개 정책 추가



파일이 비공개 상태인 경우, 전체 공개 정책을 추가하여 일괄 처리할 수 있습니다.

amazon web services

Tip2. qwikLABS에서 무료 S3 실습



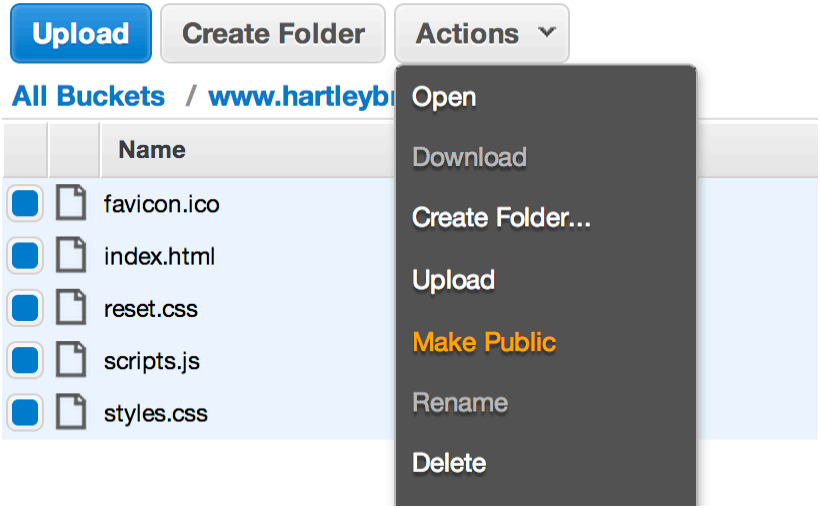
amazon web services

Tip3. S3 관련 유용한 문서

- S3 사용자 문서
  - http://docs.aws.amazon.com/ko_kr/AmazonS3/latest/gsg/GetStartedWithS3.html
- S3 콘솔 사용 설명서
  - http://docs.aws.amazon.com/ko_kr/AmazonS3/latest/UG/Welcome.html
- S3 개발자 문서
  - https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/dev/Welcome.html
- S3 Browser 정적 웹 호스팅 설명 문서
  - http://s3browser.com/how-to-host-static-website-on-amazon-s3.php

amazon web services

이제 여러분은 **무제한 웹 페이지 호스팅을** 받을 수 있습니다.



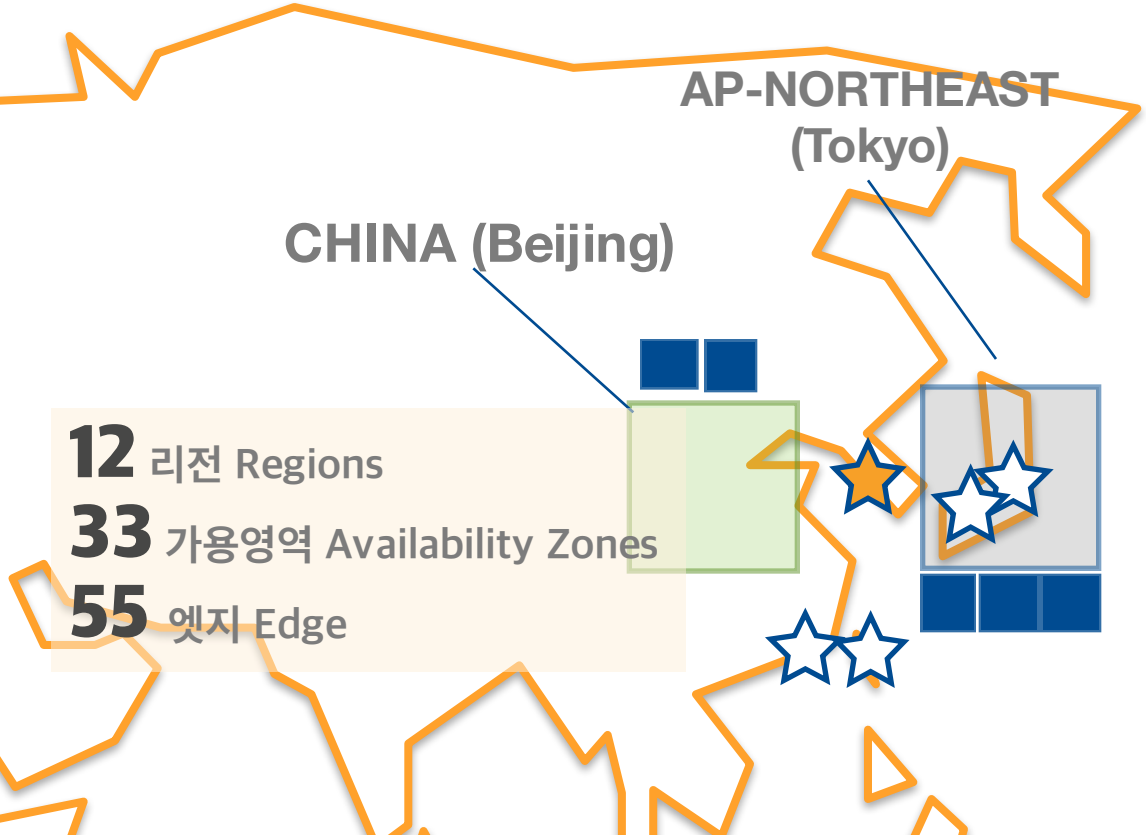
간단한 랜딩 페이지, 이벤트 웹 페이지를 제공하기 위해 서버 호스팅을 쓰시나요? Amazon S3로 서버 없이도 예상치 못한 대량 트래픽을 감당할 수 있습니다.

도움말

혹시 여러분이 Jekyll 같은 정적 블로그 도구를 사용하신다면, 손쉽게 S3에 업로드함으로서 쉽게 블로그 사이트 운영도 가능합니다.

amazon web services

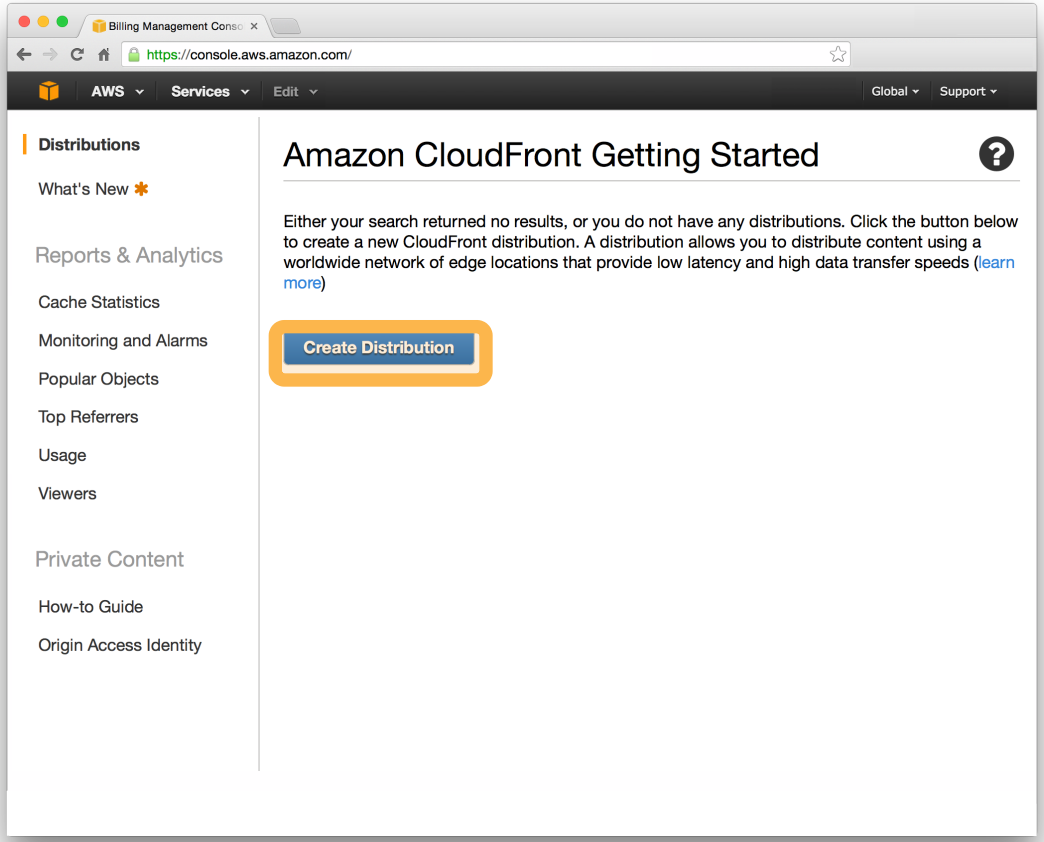
여러분의 홈페이지는 여전히 동경에…



그러나,
Amazon CloudFront를
활용하면, 여러분의
홈페이지를 더 빠르게
한국 혹은 전세계
고객에게 전달할 수
있습니다.

amazon web services

Amazon CloudFront 시작하기



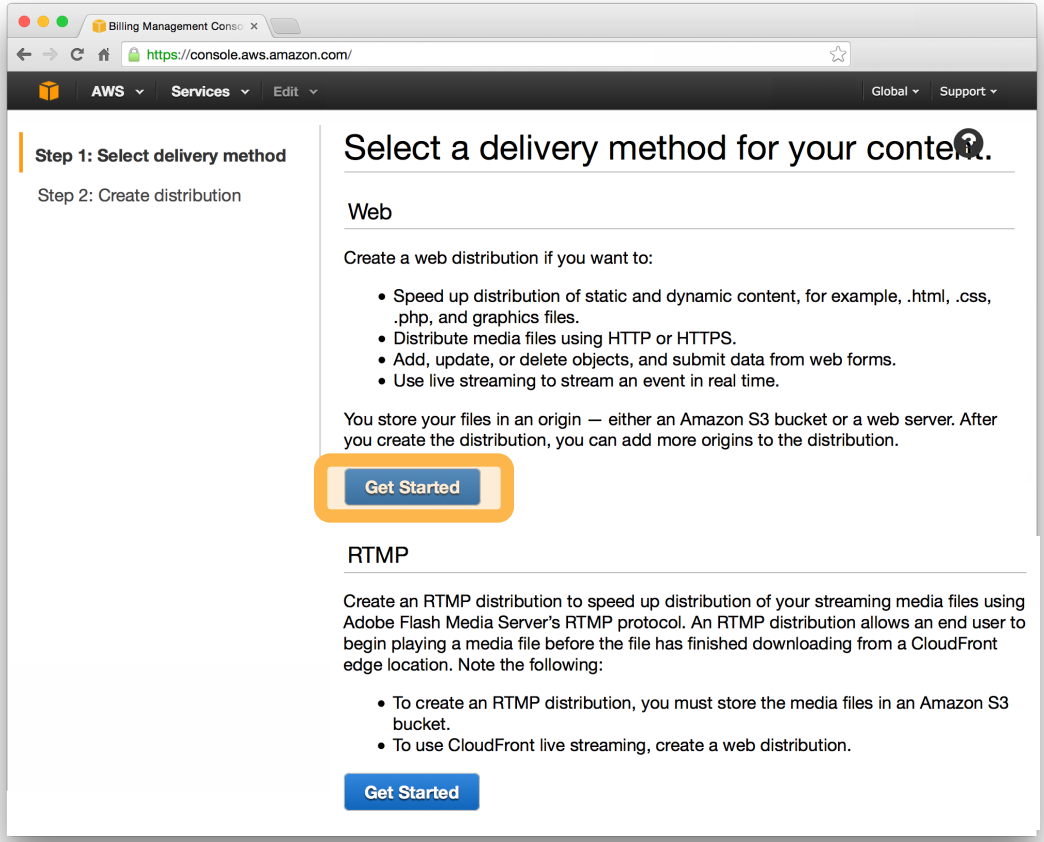
Amazon CloudFront는 정적 콘텐츠를 사용자 가까운 곳으로 전송하여 더 빠르게 이용하도록 도와 주는 서비스입니다. “Create Distribution”을 눌러 시작합니다.

도움말

Amazon CloudFront는 의외로 간단하고 사용하기가 쉽습니다. S3 버킷만 설정되어 있다면, 쉽게 콘텐츠 배포가 가능합니다.

amazon web services

단계 1. 배포 방식 결정



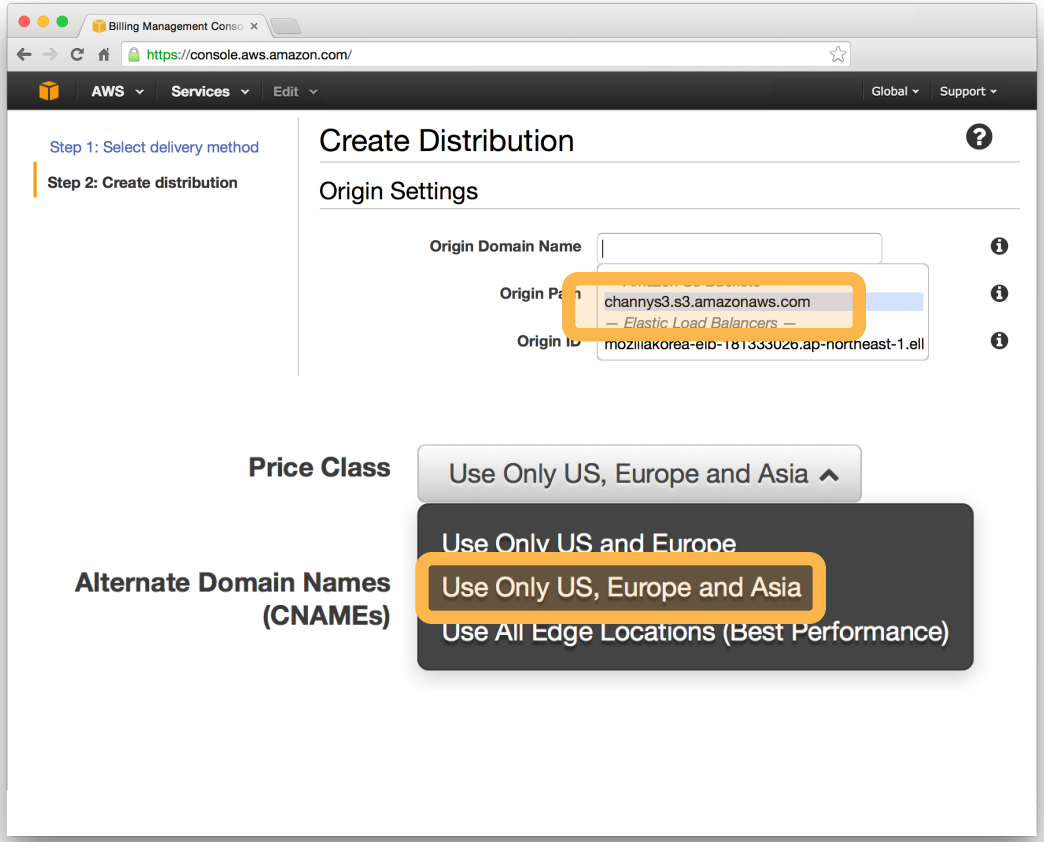
콘텐츠 배포 방식은 “Web”을 선택합니다. 미디어 파일이나 html, css, js와 같은 정적인 콘텐츠 뿐만 아니라 동적인 콘텐츠의 가속 기능도 제공합니다.

도움말

RMTP는 동영상 파일을 스트리밍으로 전달할 때 유용합니다. 여러분이 영상 파일을 Adobe 플래시의 스트리밍 방식으로 제공할 경우, S3에 미디어 파일을 담고 선택 하시면 됩니다.

amazon web services

단계 2. 소스 위치 및 배포 위치 결정



배포할 소스가 위치한 S3 버킷을 선택하고, 배포할 위치를 선택합니다. 엣지 위치는 세 가지 중에 선택 가능하며 금액에 차등이 있습니다.

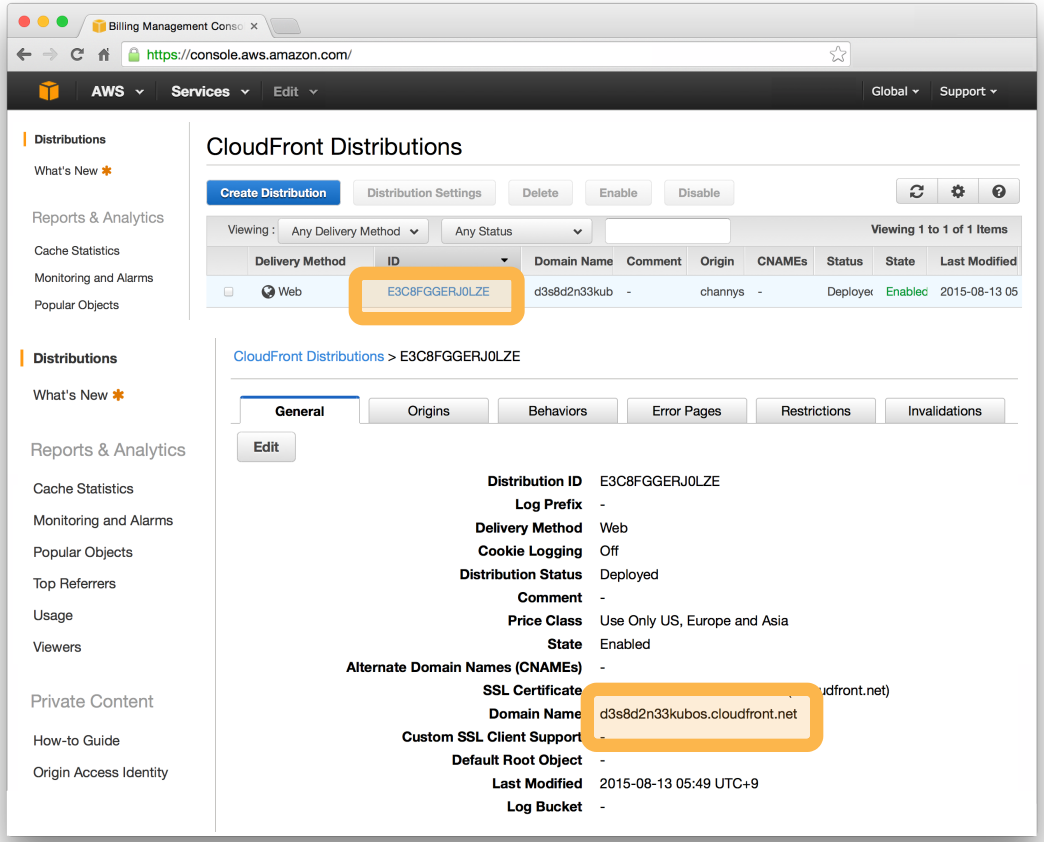
소스 위치는 S3 버킷 뿐만 아니라 웹 사이트 로드 밸런싱도 선택 가능합니다.

도움말

Origin Domain Name에는 AWS 서비스 뿐만 아니라 여러분의 외부 웹 사이트에 대한 콘텐츠 배포도 가능합니다. 즉, 국외에 더 빠르게 전송을 하기 위한 도메인을 별도로 세팅하실 수도 있습니다.

amazon web services

단계 3. 배포 확인 및 정보 수정



배포가 완료되면 “Deployed” 및 “Enabled” 표시가 됩니다. 이 때, **`xxxx.cloudfront.net`** 형식의 URL을 입력하면 확인 가능합니다.

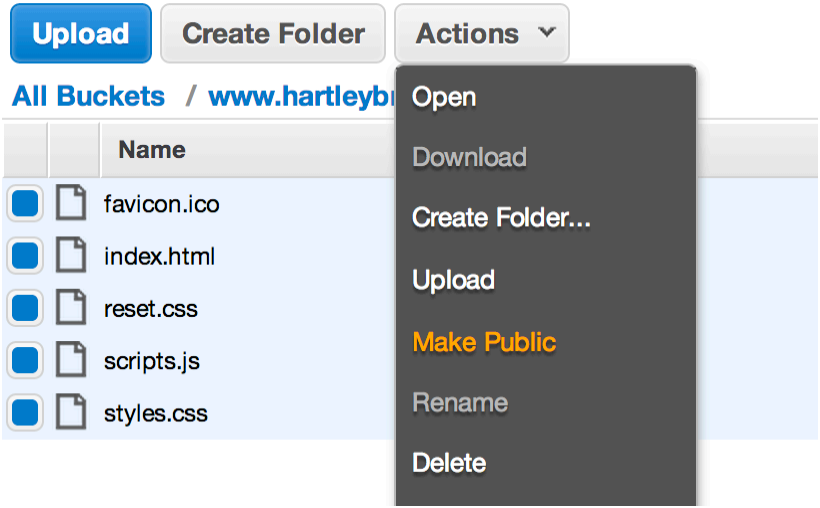
ID값을 누르시면, 각 설정 정보에 대한 변경을 손쉽게 하실 수 있습니다.

도움말

***.cloudfront.net 으로 설정된 도메인을 원하는 방식으로 바꾸고 싶으시면, 도메인 네임 서비스 설정에서 CNAME 변경을 통해 할 수 있습니다. 예를 들어, cdn.creation.net 을 CloudFront 배포 지점으로 지정 가능합니다.**

amazon web services

이제 여러분은 **전세계를 대상으로** **무제한 웹 페이지 호스팅을** 받을 수 있습니다.



간단한 랜딩 페이지, 이벤트 웹 페이지를 제공하기 위해 서버 호스팅을 쓰시나요? Amazon S3로 서버 없이도 예상치 못한 대량 트래픽을 감당할 수 있습니다.

도움말

혹시 여러분이 Jekell 같은 정적 블로그 도구를 사용하신다면, 손쉽게 S3에 업로드함으로서 쉽게 블로그 사이트 운영도 가능합니다.

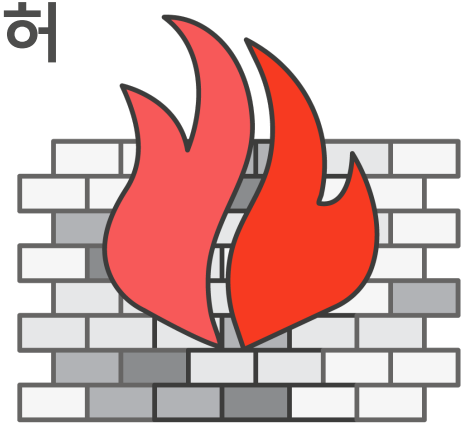
amazon web services

AWS WAF

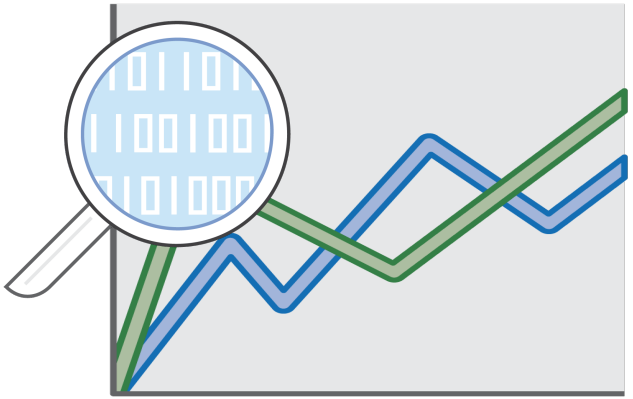
amazon web services

AWS WAF

- 웹 요청에 대한 허용 또는 불허



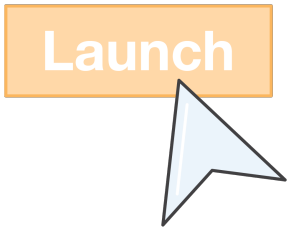
- 보안 이벤트 모니터링



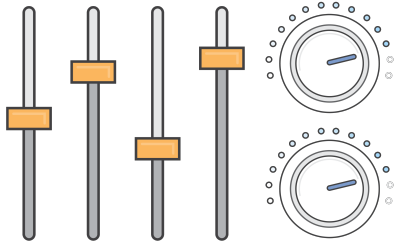
amazon web services

AWS WAF의 장점

- 쉽게 구성



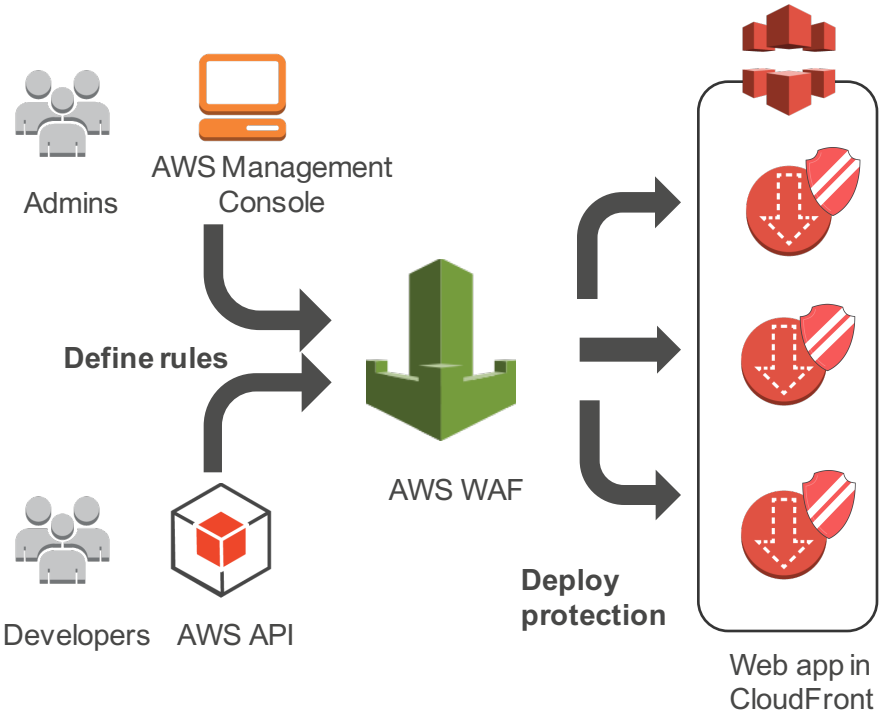
- 유연한 커스터마이징



- 개발과 통합

amazon web services

AWS WAF in Action



AWS WAF 구성 절차

- **1. web ACL 생성**

ALLOW requests by default, but…

- **2. Rule 추가**

- ***BLOCK if…***

- **3. Conditions 부여**

- ***the source IP matches this list…***

4. CloudFront 연계

for any request to d123.cloudfront.net.

amazon web services

매칭 조건

- IPSets

  CIDR notation on octet boundaries:

  - 192.0.0.0/8 – Matches 192.*.*.*
  - 192.168.0.0/16
  - 192.168.32.0/24
  - 92.168.32.64/32 – 단일 IP 주소 조건 부여

- Strings and bytes

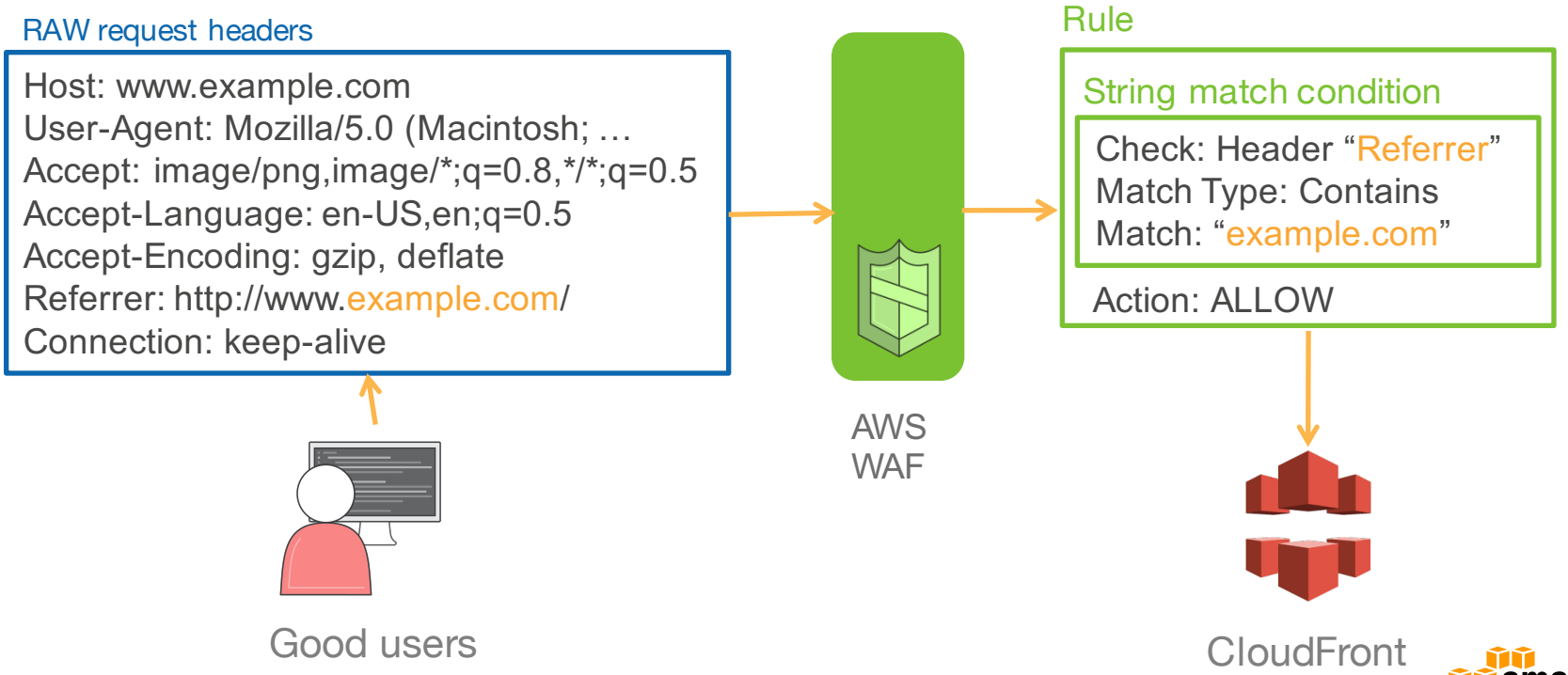
  웹 요청의 어느 부분에 대해서도 시그니쳐 탐색 가능

  적용 사례: Referrer whitelisting

amazon web services

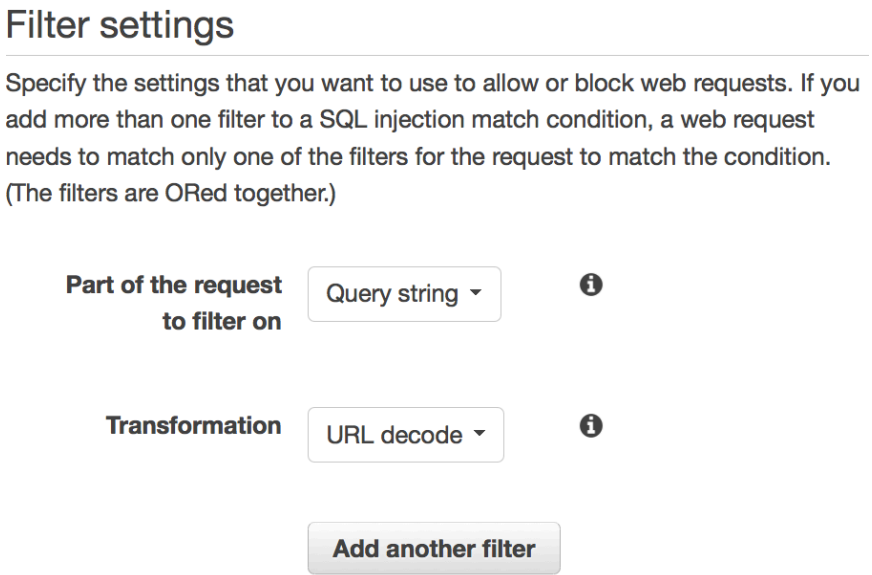
매칭 조건 : Strings and bytes

- 웹 요청의 어느 부분에 대해서도 시그니쳐 탐색 가능



매칭 조건 : SQLi

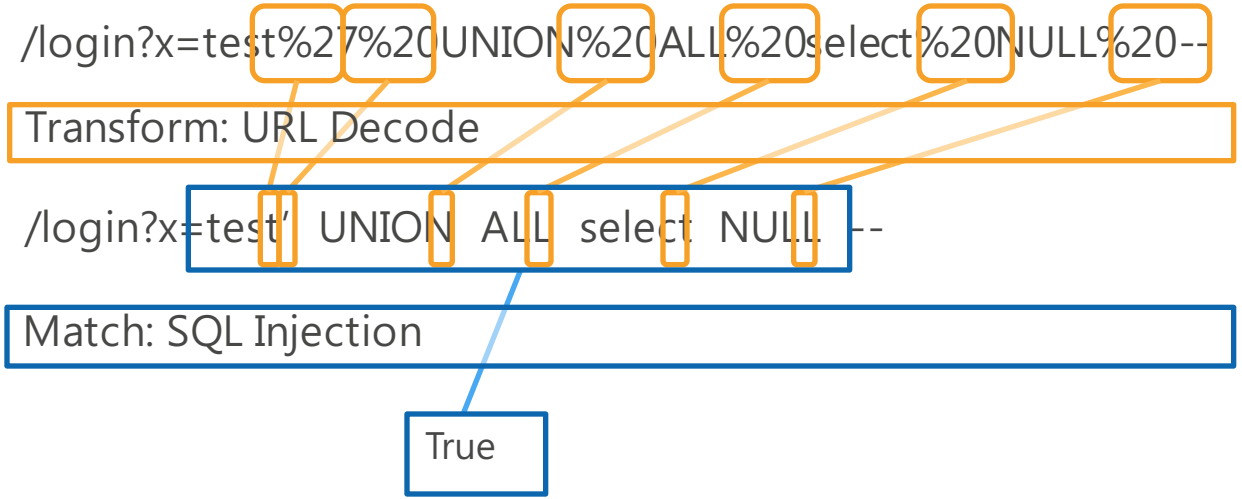
쿼리 스트링 검사, URL 디코딩



amazon web services

매칭 조건 : SQLi

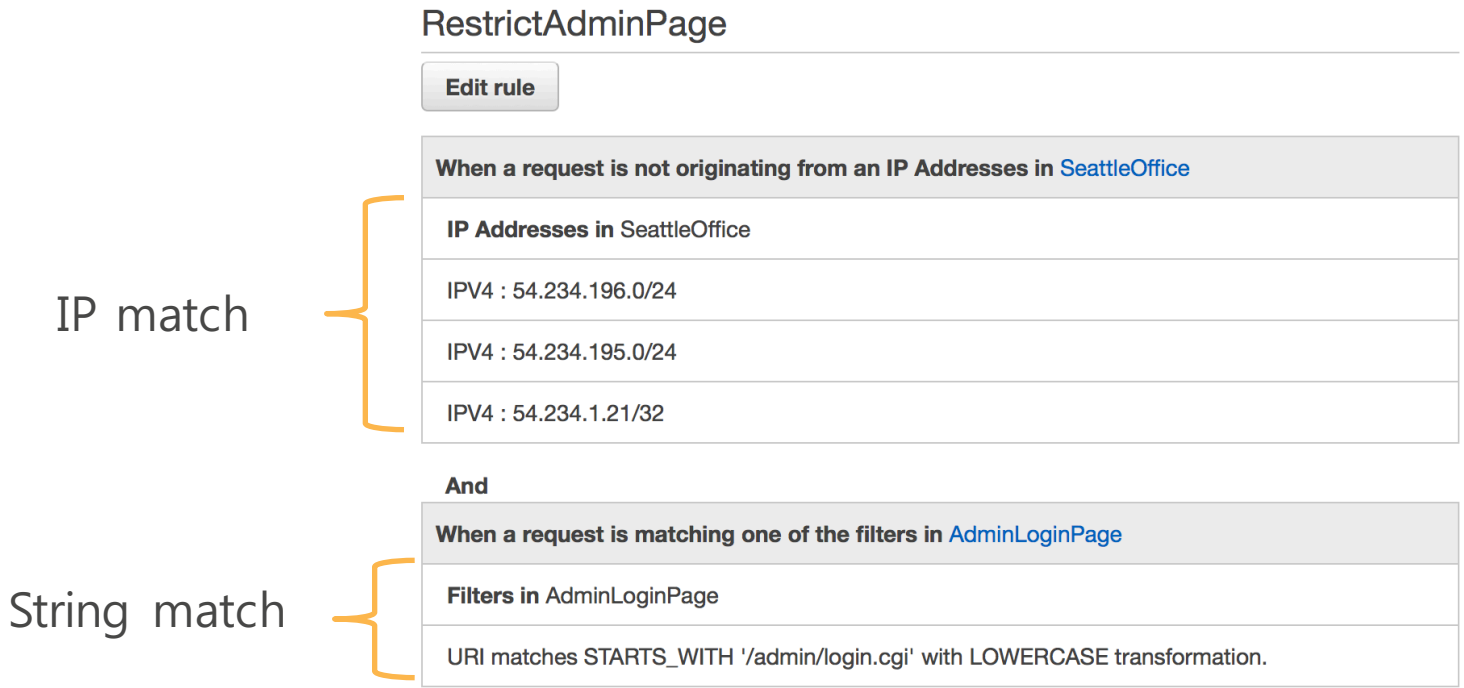
- 쿼리 스트링을 체크하려면, ‘URL decode’ Transform 활성화



amazon web services

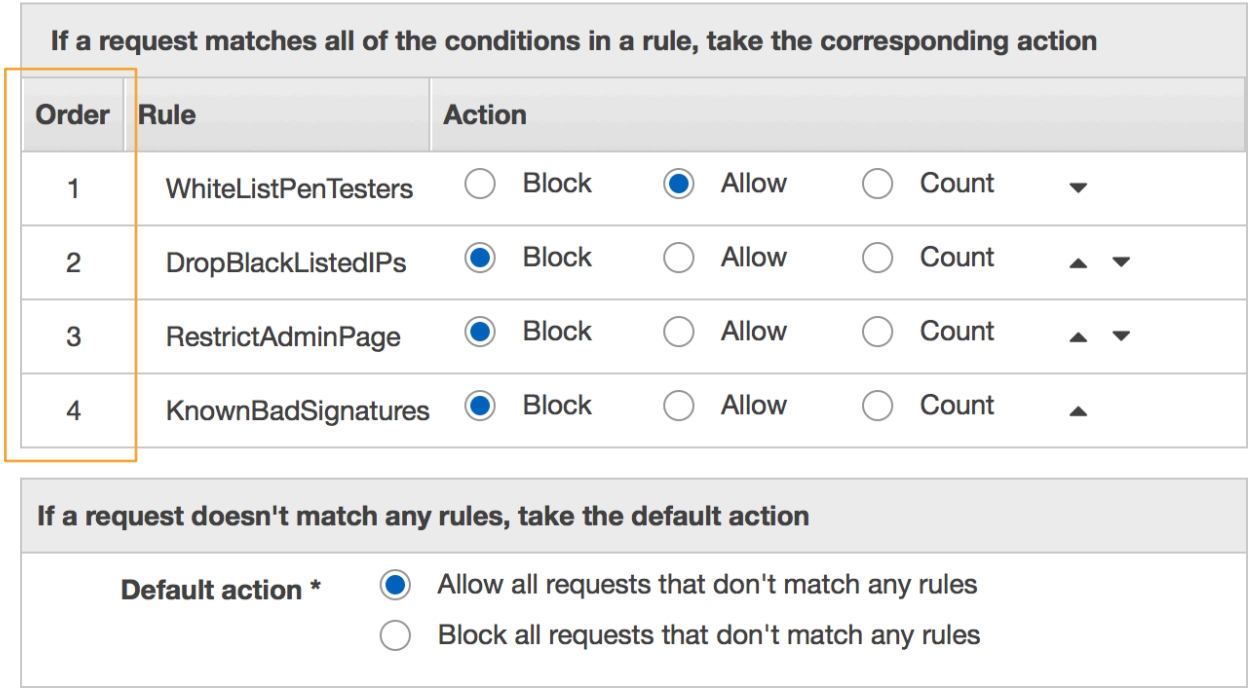
복합 conditions

- **로그인 페이지와 같이 특정 URIs에 대해 접근을 제한.**



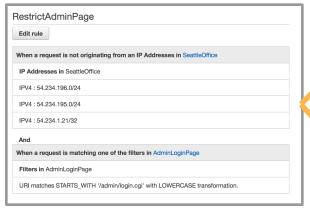
Rule Order

- **Rule 에 대한 우선순위 & 디폴트 Action.**

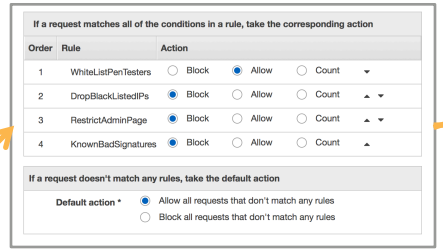


Conditions 재사용

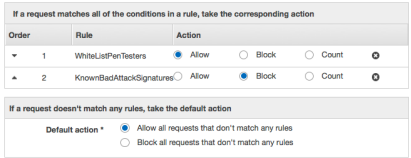
- **web ACL의 모든 부분을 재사용 가능.**



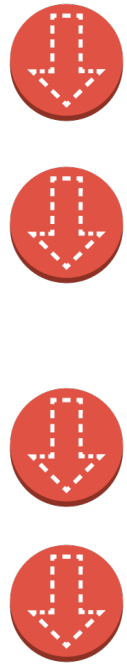
공유된 블랙리스트



Web ACL #1



Web ACL #2

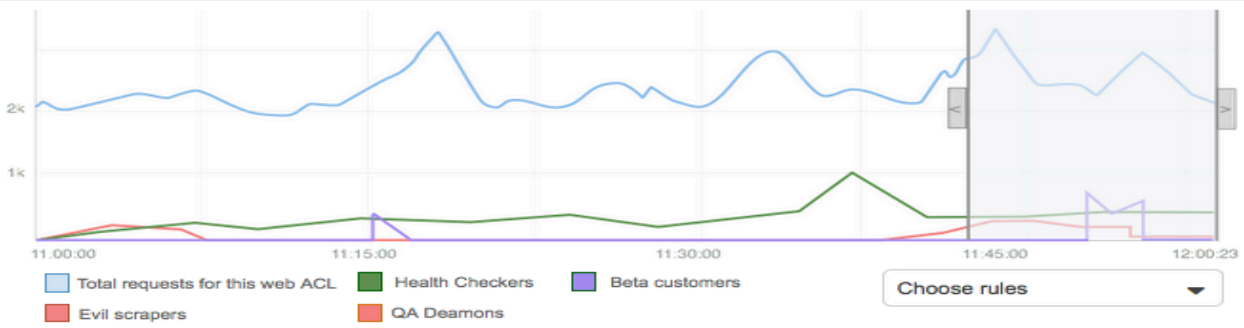


CloudFront distributions

amazon web services

Rule 적용 결과 확인

- **Rule의 실제 작동 결과를 용이하게 확인**



Sample requests

The following requests are sampled for the time period selected in the graph above. To view new samples, choose **Get new samples**, or change the time period in the graph.

Add to IP match condition **Add to string match condition**

Sample data from 11:45-12:00 pm UTC, matching all rules **Get new samples** << < 1-3 of 3 items > >>

IP Address	Host name	Matches rule	Action	Request time (UTC)
101.23.23.34	example.com/*	Health Checkers	Block	2015-11-23 12:00:23
92.23.45.67	example.com/*	Beta customer	Allow	2015-11-23 12:00:23
87.89.23.34	example.net/adm	Default	Allow	2015-11-23 12:00:23

amazon web services

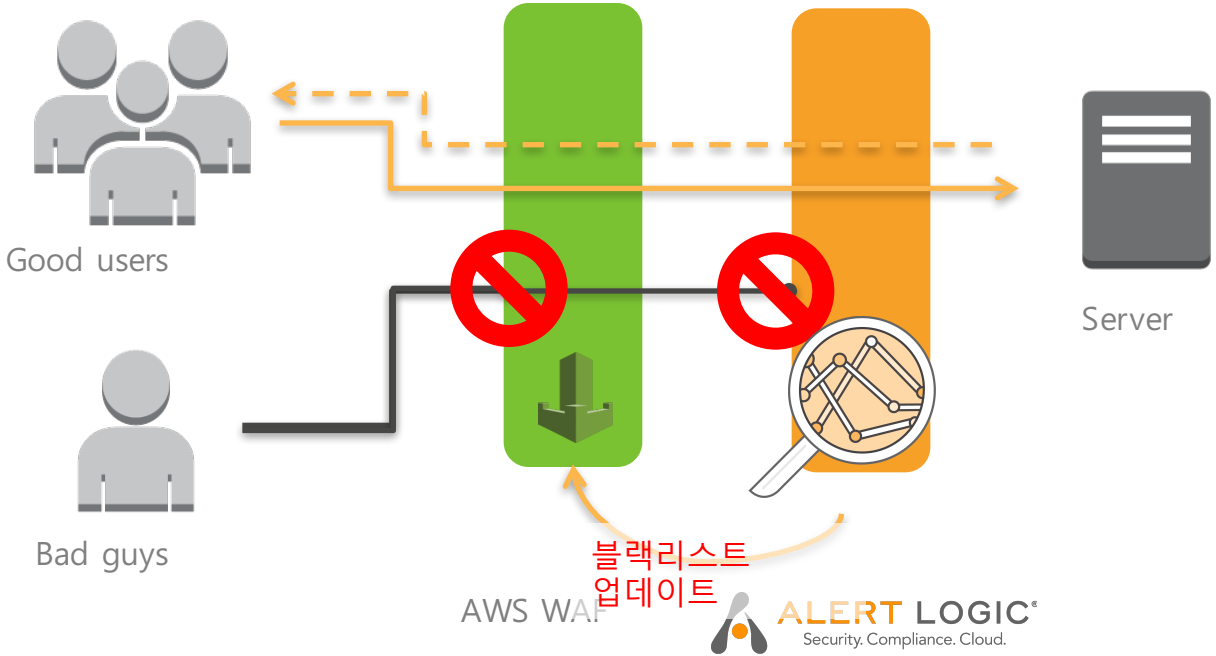
공격자 식별에 ‘count rule’ 활용하기

- Count mode
  - Amazon CloudWatch metric에 의한 경보
    - 샘플 요청 수집
      - 식별된 ‘bad IP’ 를 BlackList에 추가

amazon web services

행위 분석 자동 반영

- **Alert Logic (PoC 레벨)**



amazon web services

요금 체계

- 선수금 없음
- 한달 동안 web ACL 당 5$, rule 당 1$
- 백만 요청 당 $0.60
- 사례 :

  테스트 환경 (1 rule): $6 / 월

  작은 규모 (6 rules, 58M views): $46 / 월

  중간 규모 (6 rules, 260M views): $167 / 월

amazon web services

수업 과제

- Amazon CloudFront로 자신의 홈페이지를 배포
- 자신의 CF 배포 URL을 조교 이메일로 제출
    - xxxxx.cloudfront.net 형식

amazon web services