

* Multi-part Upload

- 오브젝트의 크기가 클 경우, 이를 조각내어 병렬적으로 처리하여 처리량을 개선하는 방법
- 보통 객체의 크기가 100MB 이상일 경우 사용하는 것을 권고하며 최대 가능 크기는 5TB
- 조각의 갯수는 최대 1만개까지 가능하며, 조각의 크기는 대개 5MB~5GM 정도임

* Version management(중요!)

- 동일한 객체에 대해 여러 버전을 가질 수 있도록 하는 기능
- 이미 S3에 존재하는 객체에 내용을 변경하여 업데이트할 경우 기존 버전이 사라지지 않고 이전 버전으로 존재할 수 있음
- 최신 버전과 이전 버전 모두 확인 가능
- 객체를 삭제하더라도 바로 삭제되는 것이 아닌 삭제 마커를 붙여 다시 복구할 수 있는 기능 제공

* Lifecycle management(중요!)

- S3에 있는 오브젝트를 일정 시간 후에 다른 타입으로 변경하는 것을 의미
- 예를 들어, 자주 사용하던 Standard Type의 오브젝트를 60일 이후 더 이상 사용하지 않을 경우 Glacier Type으로 변환하여 비용을 줄일 수 있음
- 현재 버전과 이전 버전에 대해 설정 가능
- 또한 완료되지 않은 멀티파트 업로드와 버전관리가 적용된 오브젝트의 삭제 마커를 정리할 수 있음
- 더 이상 사용하지 않은 오브젝트에 대해 만료기간을 설정하여 정한 기간 후 삭제하도록 설정 가능(만료 기간 설정)
- Standard-IA와 One Zone IA는 보관 후 30일 이후 이전 가능

* 정적 웹 사이트 호스팅

- S3로 하여금 정적 페이지를 제공할 수 있는 호스팅 기능을 제공하게 하는 것
- 활성화 후 특정 페이지를 지정하면 S3 접속시 해당 페이지를 띄움
- 굳이 서버를 이용하지 않고 S3를 이용하여 웹 호스팅을 할 수 있음
- 호스팅 뿐만 아니라 요청을 다른 버킷 혹은 도메인으로 리디렉션 가능

* 기본 암호화(중요!)

- 암호화는 Client side와 Server side로 나뉘며 Client side는 Client에서 S3로 전송될 때의 암호화(data at transit)을, Server side는 S3에 저장될 때의 암호화(data at rest)를 의미함

- Server Side Encryption

- SSE-S3 : S3의 고유한 키로 암호화를 실시하며 암호화 주체가 S3가 되는 방식. 암호 알고리즘은 AES-256.
- SSE-KMS : Key Management Service를 이용하여 객체를 암호화하는 방식으로 KMS 고객 마스터 키(CMK)를 활용함. SSE-S3와 달리 고객에 키를 제어할 수 있음
- SSE-C : 고객(Customer)가 제공하는 키로 암호화를 진행하는 방식으로 제공된 암호화 키를 사용하여 디스크를 쓰거나 해독할 때 객체에 액세스할 때의 모든 암호화를 관리함. 제공된 암호화키는 저장되지 않음

- Client Side Encryption

- S3로 데이터를 보내기 전의 암호화
- KMS에 저장된 고객 마스터키를 사용하여 암호화
- 애플리케이션 내 마스터 키를 사용하여 암호화

* 전송 속도 향상(Transfer Acceleration)

- Cloudfront의 Edge Location을 이용하여 파일 업로드를 보다 빠르게 하는 기능
- S3로 직접 업로드하는 것이 아닌 가장 가까운 Edge Location으로 전송하고 아마존 백본 네트워크를 통해 S3로 도달