Amazon Simple Storage Service

콘솔 사용 설명서

Amazon Simple Storage Service: 콘솔 사용 설명서

Table of Contents

Amazon S3 콘솔 사용 설명서 시작

Amazon Simple Storage Service(Amazon S3) 콘솔 Amazon Simple Storage Service 콘솔 사용 설명서를 시작합니다.

Amazon S3는 인터넷에서 거의 무제한적인 스토리지를 제공합니다. 본 설명서에서는 AWS 서비스와 상호 작용하기 위해 브라우저 기반 그래픽 사용자 인터페이스인 AWS Management 콘솔을 사용하여 Amazon S3에서 버킷, 객체 및 폴더들을 관리할 방법을 설명합니다.

Amazon S3의 작동 방식에 관한 자세한 개념 정보는 Amazon Simple Storage Service 개발자 가이드의 Amazon S3란 무엇입니까? 단원을 참조하십시오. 또한 개발자 안내서는 기능과 그러한 기능을 지원하기 위한 코드 예제에 관한 자세한 정보를 수록하고 있습니다.

주제

AWS Management 콘솔의 언어를 어떻게 변경합니까?

AWS Management 콘솔의 표시 언어를 변경할 수 있습니다. 여러 언어가 지원됩니다.

콘솔 언어를 변경하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 창 하단의 표시줄까지 아래로 스크롤한 다음, 표시줄의 좌측에서 언어를 선택합니다.

3. 메뉴에서 원하는 언어를 선택합니다. 이렇게 하면 전체 AWS Management 콘솔의 언어가 변경됩니다.

S3 버킷 생성 및 구성

Amazon S3에 데이터(사진, 동영상, 문서 등)를 업로드하려면 우선 하나의 AWS 리전에 S3 버킷을 만들어야 합니다. 그런 다음 데이터 객체를 버킷에 업로드할 수 있습니다.

Amazon S3에 저장한 모든 객체는 버킷에 존재합니다. 디렉토리로 파일 시스템 내 파일을 그룹화하듯 버킷으로 관련 객체를 그룹화할 수 있습니다.

Amazon S3는 사용자가 지정한 AWS 리전에 버킷을 만듭니다. 지리적으로 가까운 AWS 리전을 선택하면 지연 시간을 최적화하고, 비용을 최소화하며, 규제 요건을 해결할 수 있습니다. 예를 들어 유럽에 거주할 경우 유럽(아일랜드) 또는 유럽(프랑크푸르트) 리전에서 버킷을 생성하는 것이 유리할 수 있습니다. Amazon S3 AWS 리전의 목록은 Amazon Web Services 일반 참조의 리전 및 엔드포인트 단원을 참조하십시오.

버킷을 만드는 데는 요금이 청구되지 않습니다. 객체를 버킷에 저장하거나 버킷에서 객체를 전송한 경우에만 요금이 부과됩니다. 요금에 대한 자세한 내용은 Amazon Simple Storage Service (S3) FAQ를 참조하십시오.

Amazon S3 버킷 이름은 버킷을 만든 AWS 리전과 상관없이 전역적으로 고유합니다. 버킷 이름은 버킷을 만들 때 지정합니다. 버킷 이름 지정 지침은 Amazon Simple Storage Service 개발자 가이드의 버킷 규제 및 제한 단원을 참조하십시오.

다음 주제에서는 Amazon S3 콘솔을 사용한 버킷 생성, 삭제, 관리 방법을 살펴봅니다.

주제

S3 버킷을 생성하려면 어떻게 해야 합니까?

Amazon S3에 데이터를 업로드하려면 먼저 AWS 리전 중 하나에 데이터를 저장할 버킷을 생성해야 합니다. 버킷을 생성하면, 해당 버킷에 데이터 객체를 무제한으로 업로드할 수 있습니다.

버킷을 생성하는 AWS 계정이 해당 버킷을 소유합니다. 기본적으로 AWS 계정 각각에 대해 최대 100개의 버킷을 만들 수 있습니다. 추가 버킷이 필요할 경우 서비스 할당량 증가를 제출하여 계정 버킷 할당량을 최대 1,000 버킷으로 늘릴 수 있습니다. 버킷 할당량을 늘리는 방법은 AWS 일반 참조의 AWS 서비스 할당량을 참조하십시오.

버킷에는 지리적 리전, 버킷의 객체에 대한 액세스 설정, 기타 메타데이터 등과 같은 구성 속성이 있습니다.

버킷을 만들려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.

2. 버킷 만들기를 선택합니다.

   버킷 만들기 마법사가 열립니다.
3. 버킷 이름에 버킷의 DNS 호환 이름을 입력합니다.

   버킷 이름은 다음과 같아야 합니다.

   - 모든 Amazon S3에서 고유해야 합니다.
   - 3~63자 이내여야 합니다.
   - 대문자가 없어야 합니다.
   - 소문자 또는 숫자로 시작해야 합니다.

   버킷을 생성한 후에는 해당 이름을 변경할 수 없습니다. 버킷 이름 지정에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 버킷 이름 지정 규칙을 참조하십시오.

   > **Important**
   >
   > 버킷 이름에 계정 번호와 같은 중요한 정보를 포함하지 마십시오. 버킷 이름은 버킷의 객체를 가리키는 URL에 표시됩니다.
4. 리전에서 버킷이 속할 AWS 리전을 선택합니다.

   가까운 리전을 선택하면 지연 시간과 요금을 최소화하고 규제 요건을 다룰 수 있습니다. 특정 리전에 저장된 객체는 사용자가 명시적으로 객체를 다른 리전으로 전송하지 않는 한 해당 리전을 벗어나지 않습니다. Amazon S3 AWS 리전 목록은 Amazon Web Services 일반 참조의 AWS 서비스 엔드포인트를 참조하십시오.
5. Bucket settings for Block Public Access(퍼블릭 액세스 차단을 위한 버킷 설정)에서 버킷에 적용할 퍼블릭 액세스 차단 설정을 선택합니다.

   퍼블릭 웹 사이트 호스팅과 같은 사용 사례에 대해 하나 이상의 설정을 해제해야 하는 경우가 아니면 모든 설정을 사용하도록 설정하는 것이 좋습니다. 버킷에 대해 활성화한 퍼블릭 액세스 차단 설정도 버킷에 생성한 모든 액세스 포인트에 대해 활성화됩니다. 퍼블릭 액세스 차단에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 퍼블릭 액세스 차단 사용을 참조하십시오.
6. (선택 사항) Amazon S3 객체 잠금을 활성화하려면 다음을 수행합니다.

   a. 고급 설정을 선택하고 나타나는 메시지를 읽습니다.

      > **Important**
      >
      > 버킷을 생성할 때만 객체 잠금을 활성화할 수 있습니다. 버킷에 대해 객체 잠금을 활성화하면 나중에 비활성화할 수 없습니다. 객체 잠금을 활성화하면 버킷의 버전 관리도 활성화됩니다. 버킷에 대해 객체 잠금을 활성화한 후 객체 잠금 설정을 구성해야 버킷의 객체가 보호됩니다. 객체의 보호 구성에 대한 자세한 내용은 Amazon S3 객체를 어떻게 잠급니까? (p. 51) 단원을 참조하십시오.

   b. 객체 잠금을 활성화하려면 텍스트 상자에 enable을 입력하고 확인을 선택합니다.

   Amazon S3 객체 잠금 기능에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 객체 잠금을 사용하여 객체 잠금을 참조하십시오.
7. 버킷 만들기를 선택합니다.

추가 정보

- S3 버킷을 삭제하려면 어떻게 해야 합니까? (p. 5)
- ACL 버킷 권한을 설정하려면 어떻게 해야 합니까? (p. 118)

S3 버킷을 삭제하려면 어떻게 해야 합니까?

빈 버킷은 삭제할 수 있습니다. AWS Management 콘솔을 사용하는 경우 객체가 포함된 버킷도 삭제할 수 있습니다. 객체가 포함된 버킷을 삭제하는 경우 버킷의 모든 객체가 영구히 삭제됩니다.

버전 관리를 활성화한 상태로 버킷을 삭제하면 버킷에 있는 모든 객체의 모든 버전이 영구히 삭제됩니다. 버전 관리에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 버전 관리를 사용하는 버킷의 객체 관리 단원을 참조하십시오.

버킷을 삭제하기 전에 다음 사항을 고려하십시오.

- 버킷 이름은 고유합니다. 버킷을 삭제하면 다른 AWS 사용자가 해당 이름을 사용할 수 있습니다.
- 객체가 포함된 버킷을 삭제하면 `S3 Glacier` 스토리지 클래스로 전환된 객체를 포함해 버킷의 모든 객체가 영구적으로 삭제됩니다.
- 버킷이 정적 웹 사이트를 호스팅하고 Amazon Route 53 호스팅 영역 생성 및 구성에서 설명한 대로 Amazon Route 53 호스팅 영역을 생성하여 구성한 경우 Route 53 호스팅 영역 삭제에서 설명한 대로 버킷과 관련된 Route 53 호스팅 영역 설정을 정리해야 합니다.
- 버킷이 Elastic Load Balancing(ELB)에서 로그 데이터를 수신하는 경우 버킷을 삭제하기 전에 버킷으로 ELB 로그 전달을 중지하는 것이 좋습니다. 그렇지 않으면 버킷을 삭제했는데 다른 사용자가 이름이 같은 버킷을 생성하면 여러분의 로그 데이터가 해당 버킷으로 전달될 수 있습니다. ELB 액세스 로그에 대한 자세한 내용은 Classic Load Balancer 사용 설명서의 액세스 로그 단원과 Application Load Balancer 사용 설명서의 액세스 로그 단원을 참조하십시오.

  Important

  같은 버킷 이름을 사용하려면 버킷을 삭제하지 마십시오. 버킷을 비우고 그대로 유지하는 것이 좋습니다. 버킷을 삭제하면 해당 이름을 다시 사용할 수 있지만, 다양한 이유로 인해 사용이 불가능할 수 있습니다. 예를 들어, 그 이름을 다시 사용할 수 있을 때까지는 시간이 걸리며, 다른 계정에서 먼저 그 이름으로 버킷을 생성할 수도 있습니다.

S3 버킷 삭제 방법

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 목록에서 삭제할 버킷 이름 옆에 있는 옵션을 선택한 다음 페이지 상단에서 삭제를 선택합니다.
3. 버킷 삭제 페이지의 텍스트 필드에 버킷 이름을 입력하여 버킷을 삭제할지 확인한 다음 버킷 삭제를 선택합니다.

   Note

   버킷에 객체가 포함된 경우 버킷을 삭제하기 전에 This bucket is not empty(이 버킷이 비어 있지 않음) 오류 알림의 empty bucket configuration(빈 버킷 구성) 링크를 선택하고 버킷 비우기 페이지의 지침에 따라 버킷을 비웁니다. 그런 다음 버킷 삭제 페이지로 돌아가서 버킷을 삭제합니다.

추가 정보

- S3 버킷을 어떻게 비웁니까? (p. 6)
- S3 버킷에서 객체를 삭제하려면? (p. 45)

S3 버킷을 어떻게 비웁니까?

버킷을 삭제하지 않고도 버킷을 비워서 버킷의 모든 객체를 삭제할 수 있습니다. 버전 관리를 활성화한 상태로 버킷을 비우면 버킷에 있는 모든 객체의 모든 버전이 삭제됩니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 버전 관리를 사용하는 버킷의 객체 관리 및 버킷 삭제/비우기 단원을 참조하십시오.

S3 버킷을 비우려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 비우려는 버킷의 이름 옆에 있는 옵션을 선택한 다음 Empty(비우기)를 선택합니다.
3. 버킷 비우기 페이지에서 텍스트 필드에 버킷 이름을 입력하여 버킷을 비울 것인지 확인한 다음 Empty(비우기)를 선택합니다.
4. (선택 사항) 버킷 비우기: 상태 페이지에서 버킷 비우기 프로세스의 진행 상황을 모니터링합니다.

S3 버킷에 대한 속성을 보려면?

이 주제에서는 S3 버킷에 대한 속성을 보는 방법을 설명합니다.

S3 버킷에 대한 속성 보기

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서, 속성을 보려는 버킷 이름을 선택하십시오.

3. [Properties]를 선택합니다.

4. 속성 페이지에서 다음과 같은 버킷 속성을 구성할 수 있습니다.

   a. 버전 관리 – 버전 관리를 통해 하나의 버킷에서 객체의 여러 버전을 유지할 수 있습니다. 새 버킷의 경우 버전 관리가 기본으로 비활성화됩니다. 버전 관리 사용에 대한 자세한 내용은 S3 버킷의 버전 관리 기능을 활성화하거나 해제하려면? (p. 7) 단원을 참조하십시오.

   b. Server access logging(서버 액세스 로깅) – 서버 액세스 로그는 버킷에 대해 이루어진 요청에 따른 상세 레코드를 제공합니다. Amazon S3은(는) 기본적으로 서버 액세스 로그를 수집하지 않습니다. 서버 액세스 로깅에 대한 자세한 내용은 S3 버킷에 대한 서버 액세스 로깅을 활성화하려면 어떻게 해야 합니까? (p. 11) 단원을 참조하십시오.

   c. 정적 웹 사이트 호스팅 – Amazon S3에 정적 웹 사이트를 호스팅할 수 있습니다. 정적 웹 사이트 호스팅을 활성화하려면 정적 웹 사이트 호스팅을 선택한 다음 사용하고자 하는 설정을 지정하십시오. 자세한 내용은 S3 버킷을 정적 웹 사이트 호스팅용으로 구성하려면? (p. 16) 단원을 참조하십시오.

   d. Object-level logging(객체 수준 로깅) – 객체 수준 로깅은 CloudTrail 데이터 이벤트를 사용해 객체 수준 API 활동을 기록합니다. 객체 수준 로깅을 활성화하는 자세한 방법은 AWS CloudTrail 데이터 이벤트로 S3 버킷에 대해 객체 수준 로깅을 활성화하려면 어떻게 합니까? (p. 13) 단원을 참조하십시오.

e. 태그 – AWS 비용 할당을 하면서 버킷 태그를 지정해 버킷 사용에 대한 요금 청구 주석을 달 수 있습니다. 태그는 버킷에 할당된 라벨을 나타내는 한 쌍의 키-값입니다. 태그를 추가하려면 태그를 선택한 후 태그 추가를 선택합니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 S3 버킷에서 비용 할당 태그 사용 단원을 참조하십시오.

f. 전송 속도 향상 – Amazon S3 Transfer Acceleration을 사용하면 클라이언트와 S3 버킷 간에 파일을 빠르고 쉽고 안전하게 장거리 전송할 수 있습니다. 전송 속도 향상 활성화에 대한 자세한 내용은 S3 버킷의 Transfer Acceleration을 활성화하려면 어떻게 해야 합니까? (p. 29) 단원을 참조하십시오.

g. 이벤트 – 특정 Amazon S3 버킷 이벤트를 활성화해 이벤트가 발생할 때마다 대상에 알림을 보낼 수 있습니다. 이벤트를 활성화하려면 이벤트를 선택한 다음 사용하고자 하는 설정을 지정하십시오. 자세한 내용은 S3 버킷에 대한 이벤트 알림을 활성화하고 구성하려면 어떻게 해야 합니까? (p. 24) 단원을 참조하십시오.

h. 요청자 지불 – 요청자 지불을 사용하여 버킷 소유자 대신 요청자가 요청 및 데이터 전송에 대한 비용을 지불하도록 할 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 요청자 지불 버킷 단원을 참조하십시오.

S3 버킷의 버전 관리 기능을 활성화하거나 해제하려면?

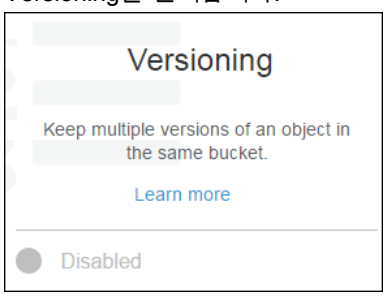
버전 관리를 통해 하나의 버킷에서 객체의 여러 버전을 유지할 수 있습니다. 이 단원에서는 버킷의 객체 버전 관리를 활성화하는 방법을 설명합니다. Amazon S3에서 버전 관리 지원에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 객체 버전 관리 및 버전 관리 사용 단원을 참조하십시오.

S3 버킷의 버전 관리 활성화 또는 비활성화 방법

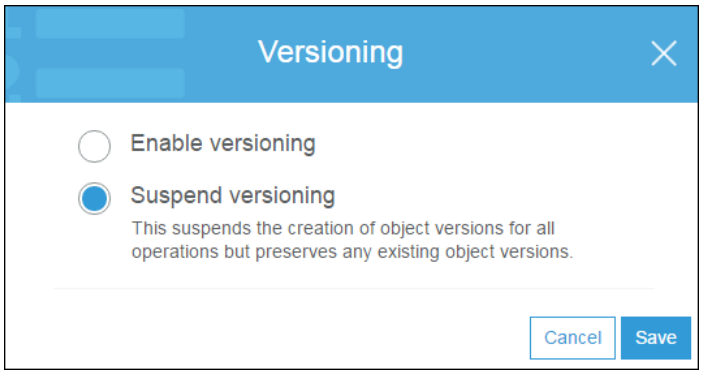
1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 버전 관리를 활성화하려는 버킷의 이름을 선택합니다.

3. [Properties]를 선택합니다.

4. Versioning을 선택합니다.



5. Enable versioning 또는 Suspend versioning을 선택한 후 Save를 선택합니다.



Note

버전 관리에 AWS Multi-Factor Authentication(MFA)을 사용할 수 있습니다. 버전 관리에 MFA를 사용하는 경우 객체 버전을 영구적으로 삭제하거나 버전 관리를 일시 중지 또는 다시 활성화하려면 계정의 MFA 디바이스에서 유효한 코드와 AWS 계정의 액세스 키를 제공해야 합니다. 버전 관리에 MFA를 사용하려면 `MFA Delete`를 활성화합니다. 그러나 AWS Management Console을 사용하여 `MFA Delete`를 활성화할 수는 없습니다. AWS CLI 또는 API를 사용해야 합니다. 자세한 내용은 MFA Delete 단원을 참조하십시오.

Amazon S3 버킷의 기본 암호화를 활성화하려면 어떻게 해야 합니까?

Amazon S3 기본 암호화를 사용하면 Amazon S3 버킷의 기본 암호화 동작을 설정할 수 있습니다. 버킷에 저장되는 모든 객체를 암호화하도록 버킷에 대한 기본 암호화를 설정할 수 있습니다. Amazon S3 관리형 키를 사용한 서버 측 암호화(SSE-S3) 또는 AWS Key Management Service(AWS KMS) 고객 마스터 키(CMK)를 사용한 서버 측 암호화로 객체를 암호화합니다.

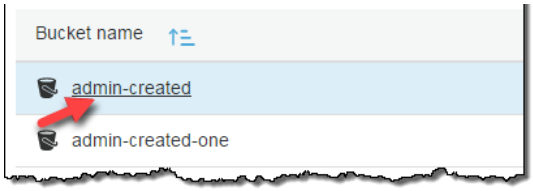
서버 측 암호화를 사용하는 경우 Amazon S3에서는 데이터 센터의 디스크에 저장하기 전에 객체를 암호화하고 객체를 다운로드할 때 이를 복호화합니다. 서버 측 암호화와 암호화 키 관리를 사용하여 데이터를 보호하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 서버 측 암호화를 사용하여 데이터 보호 단원을 참조하십시오.

기본 암호화는 모든 기존 및 새 Amazon S3 버킷에 작동합니다. 기본 암호화를 사용하지 않고 버킷에 저장된 모든 객체를 암호화하려면 모든 객체 스토리지 요청에 암호화 정보를 포함시켜야 합니다. 또한 암호화 정보를 포함하지 않는 스토리지 요청을 거부하도록 Amazon S3 버킷 정책을 설정해야 합니다.

S3 버킷의 기본 암호화를 사용하는 데 대한 추가 비용은 없습니다. 기본 암호화 기능을 구성하도록 요청할 경우 표준 Amazon S3 요청 요금이 발생합니다. 요금에 대한 자세한 내용은 Amazon S3 요금을 참조하십시오. SSE-KMS CMK 스토리지의 경우 AWS KMS 요금이 적용됩니다. 요금은 AWS KMS 요금에 나와 있습니다.

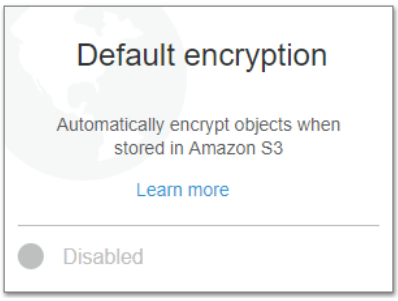
Amazon S3 버킷에 대한 기본 암호화를 활성화하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 원하는 버킷의 이름을 선택합니다.



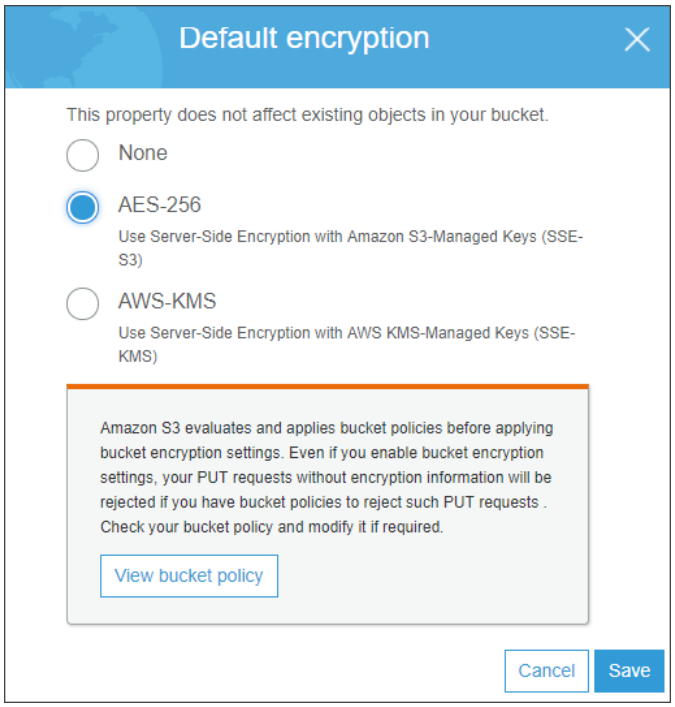
3. [Properties]를 선택합니다.

4. Default encryption(기본 암호화)을 선택합니다.



5. 기본 암호화에 대해 Amazon S3에서 관리되는 키를 사용하려면 AES-256을 선택하고 저장을 선택합니다.

   Amazon S3 서버 측 암호화를 사용하여 데이터를 암호화하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 관리형 암호화 키로 데이터 보호 단원을 참조하십시오.



Important

기본 암호화를 활성화할 때 버킷 정책을 업데이트해야 할 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 암호화 적용에 대해 버킷 정책 사용에서 기본 암호화로 전환 단원을 참조하십시오.

6. 기본 암호화에 대해 AWS KMS에 저장된 CMK를 사용하려면 다음 단계를 따르십시오.

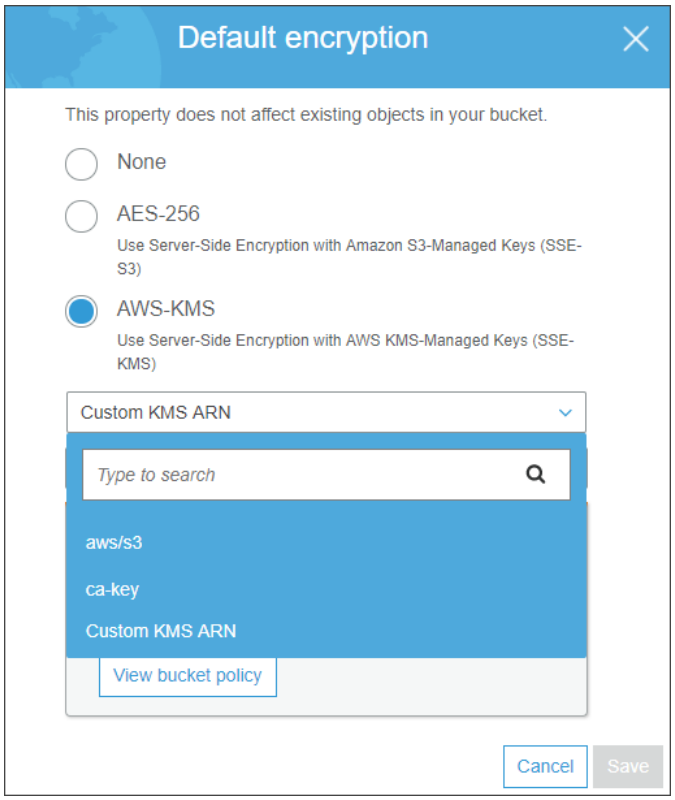
   a. AWS-KMS를 선택합니다.

   b. 사용자가 생성한 고객 관리형 AWS KMS CMK를 선택하려면 다음 방법 중 하나를 사용합니다.

   - 표시되는 목록에서 AWS KMS CMK를 선택합니다.
   - 표시되는 목록에서 사용자 지정 KMS ARN을 선택한 다음 AWS KMS CMK의 Amazon 리소스 이름을 입력합니다.

Important

Amazon S3에서 서버 측 암호화에 AWS KMS CMK를 사용하는 경우 대칭 CMK를 선택해야 합니다. Amazon S3는 대칭 CMK만 지원하고 비대칭 CMK는 지원하지 않습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 대칭 및 비대칭 키 사용을 참조하십시오.



Important

기본 암호화 구성에 대해 AWS KMS 옵션을 사용할 경우 AWS KMS에 대한 RPS(초당 요청 수) 제한이 적용됩니다. AWS KMS 제한과 한도 증가를 요청하는 방법에 대한 자세한 내용은 AWS KMS 제한 단원 참조하십시오.

AWS KMS CMK 생성에 대한 자세한 내용은 AWS Key Management Service Developer Guide의 키 생성을 참조하십시오. Amazon S3에서 AWS KMS를 사용하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 AWS KMS에 저장된 키로 데이터 보호를 참조하십시오.

7. Save를 선택합니다.

추가 정보

- Amazon Simple Storage Service 개발자 가이드의 S3 버킷에 대한 Amazon S3 기본 암호화
- S3 객체에 암호화를 추가하려면 어떻게 해야 합니까? (p. 59)

S3 버킷에 대한 서버 액세스 로깅을 활성화하려면 어떻게 해야 합니까?

이 주제에서는 AWS Management 콘솔을 사용하여 Amazon S3 버킷에 대한 서버 액세스 로깅을 활성화하는 방법을 설명합니다. 프로그래밍 방식으로 로깅을 활성화하는 방법과 로그가 전달되는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 서버 액세스 로깅 단원을 참조하십시오.

Amazon Simple Storage Service(Amazon S3)는 기본적으로 서버 액세스 로그를 수집하지 않습니다. 로깅을 활성화하면 Amazon S3는 사용자가 선택한 대상 버킷에 소스 버킷에 대한 액세스 로그를 전달합니다. 대상 버킷은 원본 버킷과 동일한 AWS 리전에 있어야 하며 기본 보존 기간 구성이어서는 안 됩니다.

서버 액세스 로깅은 S3 버킷에 대해 이루어진 요청에 따른 상세 레코드를 제공합니다. 서버 액세스 로그는 많은 애플리케이션에 있어 유용합니다. 예를 들어 액세스 로그 정보는 보안 및 액세스 감사에 유용할 수 있습니다. 또한 고객층을 파악하고 Amazon S3 결제 요금을 확인할 수 있습니다.

액세스 로그 레코드에는 버킷에 대한 요청 내역이 자세히 나와 있습니다. 이 정보에는 요청 유형, 요청에 지정된 리소스, 요청을 처리한 날짜 및 시간 등이 포함됩니다. 자세한 정보는 Amazon Simple Storage Service 개발자 가이드의 서버 액세스 로그 형식 단원을 참조하십시오.

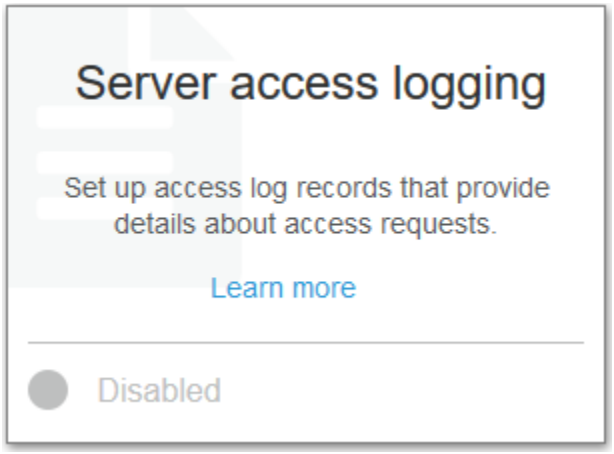
> **Important**
>
> Amazon S3 버킷에 서버 액세스 로그를 사용하는 데 따른 별도의 요금이 청구되지 않습니다. 단, 시스템이 사용자에게 전달하는 로그 파일에 대해서는 일반적인 스토리지 요금이 발생합니다. (로그 파일은 언제든지 삭제할 수 있습니다.) 로그 파일 전달에 따른 데이터 전송 요금은 발생하지 않지만 로그 파일 액세스에 따른 일반 데이터 전송 요금은 부과됩니다.

S3 버킷에 대한 서버 액세스 로깅을 활성화하려면

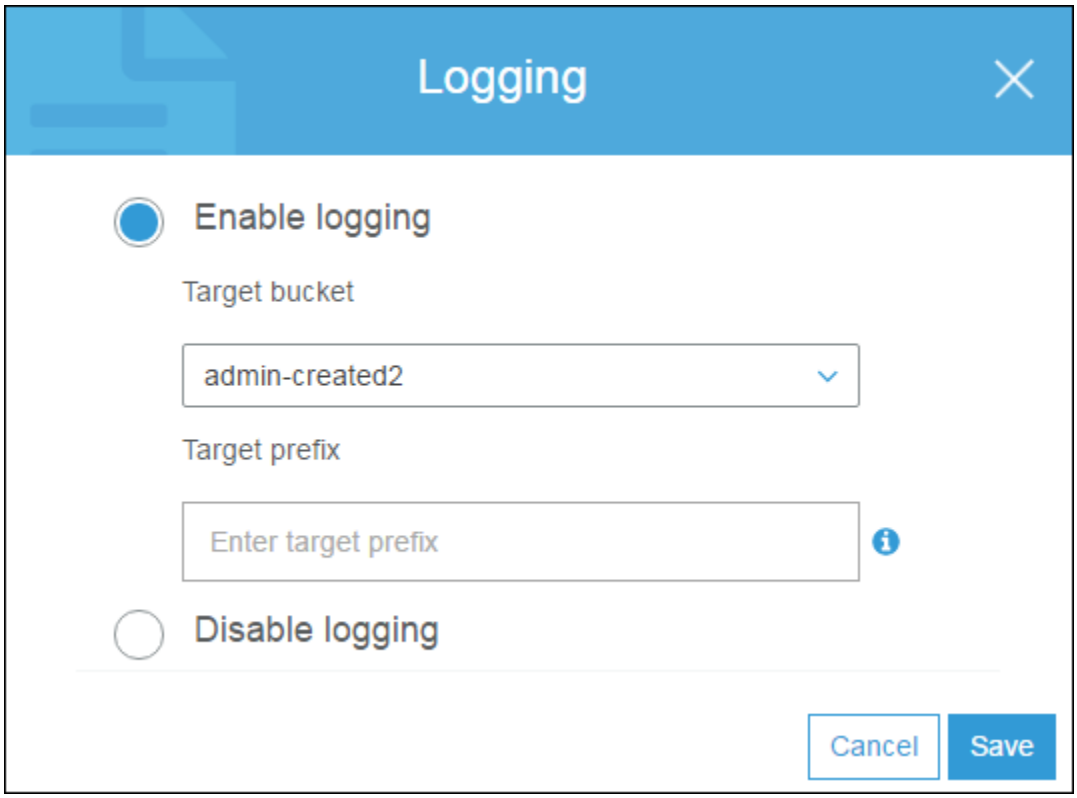
1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 서버 액세스 로깅을 활성화하려는 버킷의 이름을 선택합니다.

3. [Properties]를 선택합니다.

4. Server access logging(서버 액세스 로깅)을 선택합니다.



5. 로깅 활성화를 선택합니다. 대상으로는 로그 기록 객체를 받아 보고자 하는 버킷의 이름을 선택합니다. 대상 버킷은 원본 버킷과 동일한 리전에 있어야 하며 기본 보존 기간 구성이어서는 안 됩니다.



6. (선택 사항) 대상 접두사에 로그 객체의 키 이름 접두사를 입력하여 로그 객체 이름이 모두 동일한 문자열로 시작되도록 합니다.
7. Save를 선택합니다.

대상 버킷에서 로그를 볼 수 있습니다. 접두사를 지정한 경우 해당 접두사는 콘솔의 대상 버킷에 폴더로 표시됩니다. 서버 액세스 로깅을 활성화하면 로그가 대상 버킷에 전달되기까지 몇 시간이 소요될 수 있습니다. 로그가 전달되는 방법 및 시기에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 서버 액세스 로깅 단원을 참조하십시오.

추가 정보

S3 버킷에 대한 속성을 보려면? (p. 6)

AWS CloudTrail 데이터 이벤트로 S3 버킷에 대해 객체 수준 로깅을 활성화하려면 어떻게 합니까?

이 단원에서는 Amazon S3 콘솔을 사용하여 S3 버킷의 객체에 대한 데이터 이벤트를 기록하도록 AWS CloudTrail 추적을 활성화하는 방법에 대해 설명합니다. CloudTrail은 `GetObject`, `DeleteObject`, `PutObject` 같은 Amazon S3 객체 수준 API 작업 로깅을 지원합니다. 이러한 이벤트를 데이터 이벤트라고 합니다. 기본적으로 CloudTrail 추적은 데이터 이벤트를 로깅하지 않지만 지정한 S3 버킷에 대한 데이터 이벤트를 로깅하거나 AWS 계정의 모든 Amazon S3 버킷에 대한 데이터 이벤트를 로깅하도록 추적을 구성할 수 있습니다. 자세한 내용은 AWS CloudTrail을 사용하여 Amazon S3 API 호출 로깅을 참조하십시오. CloudTrail은 CloudTrail 이벤트 기록의 데이터 이벤트를 채우지 않습니다. 또한 모든 버킷 수준 작업이 CloudTrail 이벤트 기록에 채워지는 것은 아닙니다. 자세한 내용은 Amazon CloudWatch Logs 필터 패턴과 Amazon Athena를 사용하여 CloudTrail 로그 쿼리를 참조하십시오.

S3 버킷에 대한 데이터 이벤트를 기록하도록 추적을 구성하기 위해 AWS CloudTrail 콘솔 또는 Amazon S3 콘솔을 사용할 수 있습니다. AWS 계정의 모든 Amazon S3 버킷에 대해 데이터 이벤트를 기록하도록 추적을 구성하는 경우 CloudTrail 콘솔을 사용하는 편이 더 편리합니다. CloudTrail 콘솔을 사용하여 S3 데이터 이벤트를 기록하도록 추적을 구성하는 자세한 방법은 AWS CloudTrail User Guide의 데이터 이벤트 단원을 참조하십시오.

> **Important**
>
> 데이터 이벤트에는 추가 요금이 적용됩니다. 자세한 내용은 AWS CloudTrail 요금을 참조하십시오.

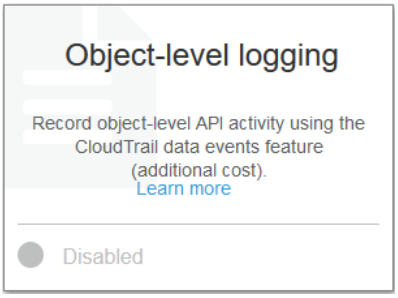
다음 절차는 Amazon S3 콘솔을 사용하여 CloudTrail 추적이 S3 버킷에 대한 데이터 이벤트를 기록할 수 있도록 하는 방법을 보여줍니다.

S3 버킷의 객체에 대해 CloudTrail 데이터 이벤트 로깅을 활성화하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 버킷의 이름을 선택합니다.

3. [Properties]를 선택합니다.

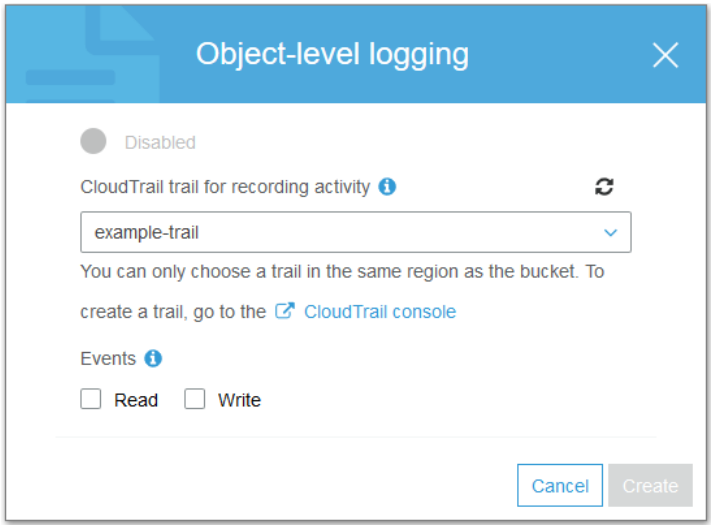
4. Object-level logging(객체 수준 로깅)을 선택합니다.



5. 드롭다운 메뉴에서 기존 CloudTrail 추적을 선택합니다.

   선택한 추적은 버킷과 동일한 AWS 리전에 있어야 하므로 드롭다운 목록에는 모든 리전에 대해 생성된 추적 또는 버킷과 동일한 리전에 있는 추적만 포함됩니다.

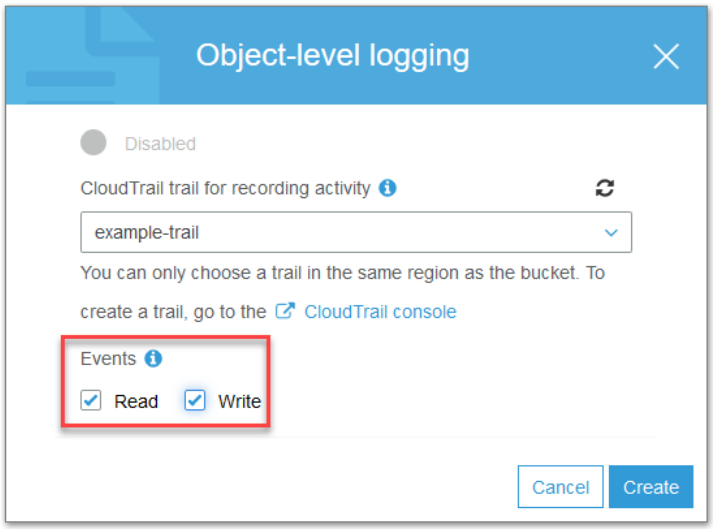
   추적을 생성해야 하는 경우 CloudTrail 콘솔 링크를 선택하여 CloudTrail 콘솔로 이동합니다. CloudTrail 콘솔에서 추적을 생성하는 자세한 방법은 AWS CloudTrail User Guide의 콘솔을 사용하여 추적 생성 단원을 참조하십시오.



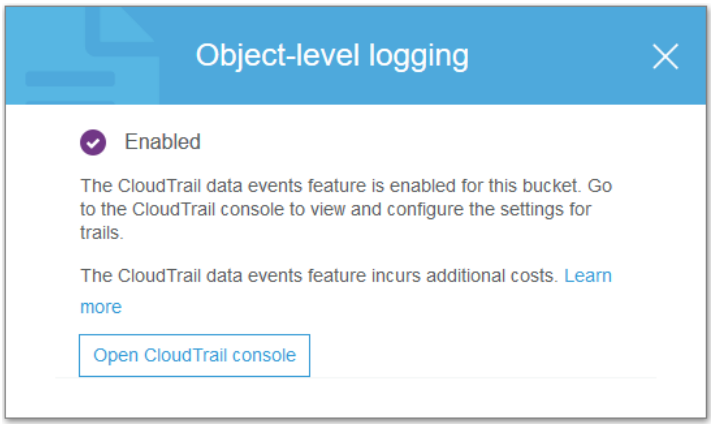
6. 이벤트에서 다음 중 하나를 선택합니다.

   - CloudTrail가 `GetObject` 같은 Amazon S3 읽기 API를 기록하도록 지정하려면 읽기를 선택합니다.
   - `PutObject` 같은 Amazon S3 쓰기 API를 기록하려면 쓰기를 선택합니다.
   - 읽기와 쓰기 객체 API를 모두 기록하려면 읽기와 쓰기를 선택합니다.

   Amazon S3 객체에 대해 CloudTrail이 기록하는 지원되는 데이터 이벤트 목록은 Amazon Simple Storage Service 개발자 가이드의 CloudTrail 로깅을 통해 추적되는 Amazon S3 객체 수준 작업 단원을 참조하십시오.



7. 버킷에 대해 객체 수준 로깅을 활성화하려면 생성을 선택합니다.



버킷에 대한 객체 수준 로깅을 비활성화하려면 CloudTrail 콘솔로 이동하여 추적의 Data events(데이터 이벤트)에서 버킷 이름을 제거해야 합니다.

Note

CloudTrail 콘솔이나 Amazon S3 콘솔을 사용하여 S3 버킷에 대해 데이터 이벤트를 기록하도록 추적을 구성하면 Amazon S3 콘솔에는 해당 버킷에 대해 객체 수준 로깅이 활성화된 것으로 표시됩니다.

S3 버킷을 생성할 때 객체 수준 로깅을 활성화하는 자세한 방법은 S3 버킷을 생성하려면 어떻게 해야 합니까? (p. 3) 단원을 참조하십시오.

추가 정보

- S3 버킷에 대한 속성을 보려면? (p. 6)
- Amazon Simple Storage Service 개발자 가이드의 AWS CloudTrail을 사용하여 Amazon S3 API 호출 로깅
- AWS CloudTrail User Guide의 CloudTrail 로그 파일 작업

S3 버킷을 정적 웹 사이트 호스팅용으로 구성하려면?

Amazon S3에 정적 웹 사이트를 호스팅할 수 있습니다. 정적 웹 사이트에서 개별 웹 페이지는 정적 콘텐츠를 포함합니다. 정적 웹 사이트에는 클라이언트 측 스크립트가 포함될 수도 있습니다. 이와는 대조적으로, 동적 웹 사이트는 PHP, JSP 또는 ASP.NET 등 서버 측 스크립트를 포함한 서버 측 처리에 의존합니다. Amazon S3에서는 서버 측 암호화가 지원되지 않습니다.

다음과 같은 빠른 절차를 사용하여 Amazon S3 콘솔에서 정적 웹 사이트 호스팅을 위한 S3 버킷을 구성할 수 있습니다. 자세한 내용과 자세한 연습은 Amazon Simple Storage Service 개발자 가이드에서 Amazon S3의 정적 웹 사이트 호스팅을 참조하십시오.

주제

1단계: 정적 웹 사이트 호스팅용 Amazon S3 버킷 구성

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 정적 웹 사이트 호스팅을 활성화하려는 버킷의 이름을 선택합니다.

3. [Properties]를 선택합니다.

4. [Static website hosting]을 선택합니다.

5. 이 버킷을 사용하여 웹 사이트를 호스팅합니다.를 선택합니다.

6. 인덱스 문서에 인덱스 문서 이름을 입력합니다(일반적으로 `index.html`).

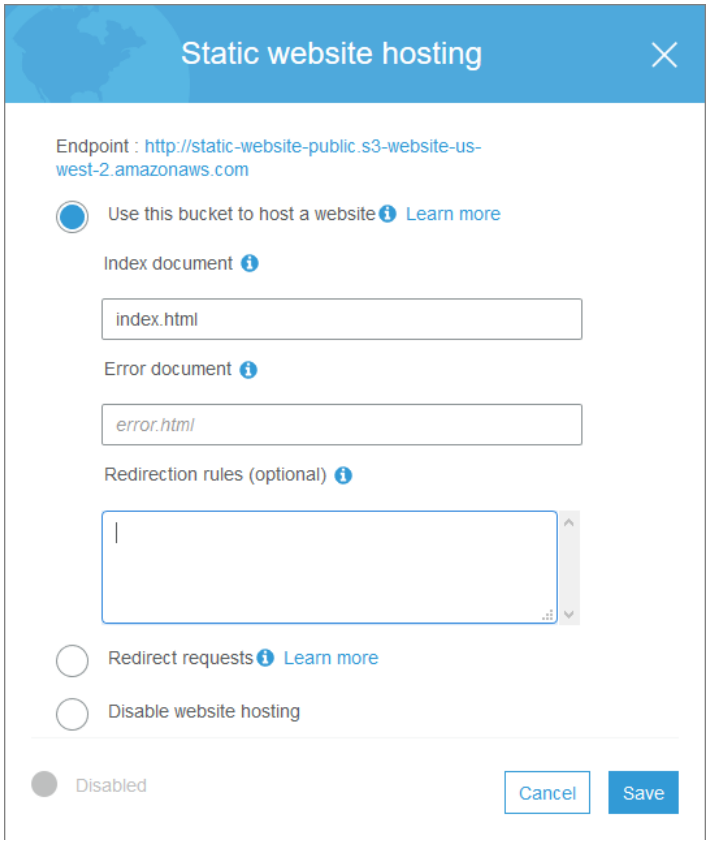
   웹 사이트 호스팅용 버킷을 구성하는 경우 인덱스 문서를 지정해야 합니다. 루트 도메인이나 임의의 하위 폴더로 요청이 전송되면 Amazon S3가 이 인덱스 문서를 반환합니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 인덱스 문서 지원 구성을 참조하십시오.

7. (선택 사항) 4XX 클래스 오류에 대한 사용자 지정 오류 문서를 제공하려면 오류 문서에서 사용자 지정 오류 문서 파일 이름을 입력합니다.

   사용자 지정 오류 문서를 지정하지 않았는데 오류가 발생하면 Amazon S3에서 기본 HTML 오류 문서를 반환합니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 사용자 지정 오류 문서 지원 단원을 참조하십시오.

8. (선택 사항) 고급 리디렉션 규칙을 지정하려면 Edit redirection rules(리디렉션 규칙 편집) 상자에서 규칙을 설명하는 XML을 입력하십시오.

   예를 들어, 요청의 특정 객체 키 이름 또는 접두사에 따라 조건부로 요청을 라우팅할 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 고급 조건부 리디렉션을 참조하십시오.



9. 저장을 선택합니다.

10. 버킷에 인덱스 문서를 업로드합니다.

    S3 버킷에 객체를 업로드하는 방법에 대한 단계별 지침은 선택하여 클릭하기로 파일 업로드 (p. 40) 단원을 참조하십시오.
11. 선택적 사용자 지정 오류 문서를 포함하여 웹 사이트에 대한 다른 파일을 업로드합니다.

다음 단원에서는 정적 웹 사이트로 버킷에 액세스하는 데 필요한 권한을 설정합니다.

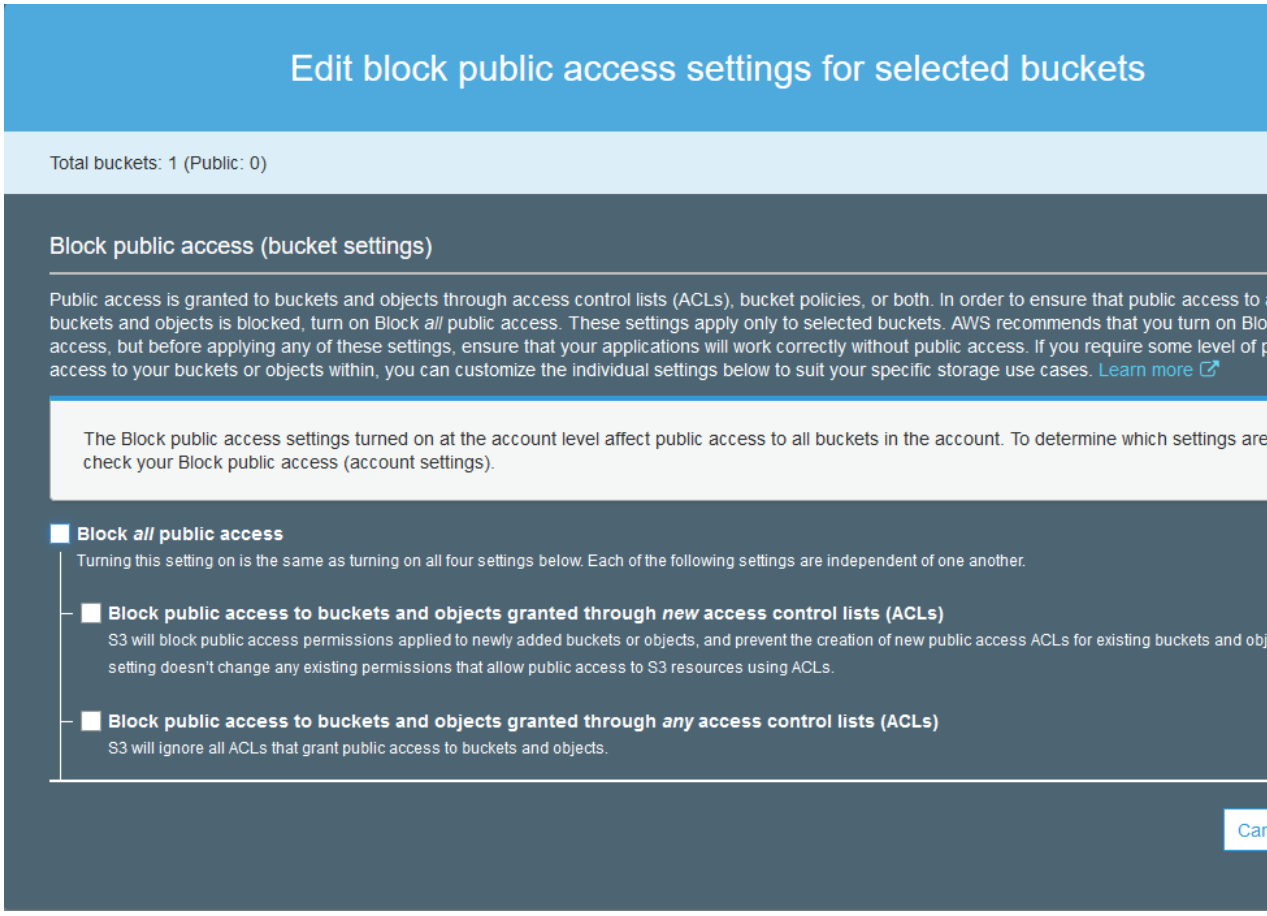
2단계: 퍼블릭 액세스 차단 설정 편집

기본적으로 Amazon S3은 계정 및 버킷에 대한 퍼블릭 액세스를 차단합니다. 버킷을 사용하여 정적 웹 사이트를 호스팅하려는 경우 이러한 단계를 사용하여 퍼블릭 액세스 차단 설정을 편집할 수 있습니다.

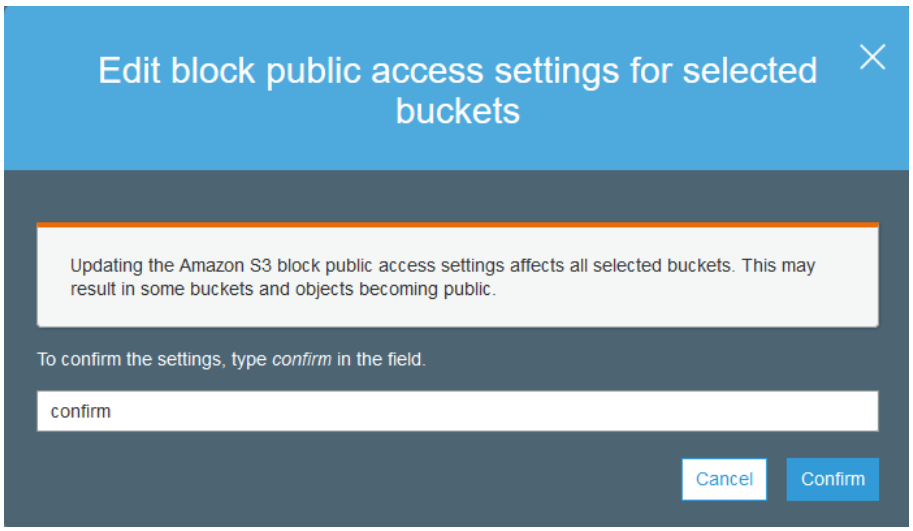
> Warning
>
> 이 단계를 완료하기 전에 Amazon S3 퍼블릭 액세스 차단 사용을 검토하여 퍼블릭 액세스 허용과 관련된 위험을 이해하고 이에 동의하는지 확인하십시오. 퍼블릭 액세스 차단 설정을 해제하여 버킷을 퍼블릭으로 만들면 인터넷상의 모든 사용자가 버킷에 액세스할 수 있습니다. 버킷에 대한 모든 퍼블릭 액세스를 차단하는 것이 좋습니다.

1. https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 정적 웹 사이트로 구성한 버킷의 이름을 선택합니다.
3. Permissions를 선택합니다.
4. [Edit]를 선택합니다.
5. Block all public access(모든 퍼블릭 액세스 차단)를 선택 취소하고 저장을 선택합니다.

   > Warning
   >
   > 이 단계를 완료하기 전에 Amazon S3 퍼블릭 액세스 차단 사용을 검토하여 퍼블릭 액세스 허용과 관련된 위험을 이해하고 이에 동의하는지 확인하십시오. 퍼블릭 액세스 차단 설정을 해제하여 버킷을 퍼블릭으로 만들면 인터넷상의 모든 사용자가 버킷에 액세스할 수 있습니다. 버킷에 대한 모든 퍼블릭 액세스를 차단하는 것이 좋습니다.



6. 확인 상자에 **`confirm`**을 입력한 다음 확인을 선택합니다.



S3 버킷에서 버킷에 대한 액세스가 Objects can be public(객체가 퍼블릭이 될 수 있음)으로 업데이트됩니다. 이제 버킷의 객체를 공개적으로 읽기 가능하게 만들 버킷 정책을 추가할 수 있습니다. 액세스가 계속 Bucket and objects not public(버킷 및 객체가 퍼블릭이 아님)으로 표시되는 경우, 버킷 정책을 추가하기 전에 계정에 대해 퍼블릭 액세스 차단 설정을 편집해야 할 수도 있습니다.

3단계: 버킷 정책 추가

S3 퍼블릭 액세스 차단 설정을 편집한 후에는 버킷 정책을 추가하여 버킷에 퍼블릭 읽기 액세스 권한을 부여할 수 있습니다. 퍼블릭 읽기 액세스 권한을 부여하면 인터넷의 모든 사용자가 버킷에 액세스할 수 있습니다.

> Important
>
> 다음 정책은 하나의 예일 뿐이며 버킷의 콘텐츠에 대한 전체 액세스를 허용합니다. 이 단계를 진행하기 전에 Amazon S3 버킷의 파일을 보호하려면 어떻게 해야 합니까?를 검토하여 S3 버킷의 파일 보안을 위한 모범 사례 및 퍼블릭 액세스 권한 부여와 관련된 위험을 파악할 수 있습니다.

1. 버킷에서 버킷의 이름을 선택합니다.
2. Permissions를 선택합니다.
3. [Bucket Policy]를 선택합니다.
4. 웹 사이트에 대한 퍼블릭 읽기 액세스 권한을 부여하려면 다음 버킷 정책을 복사한 후 버킷 정책 편집기에 붙여 넣습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::example.com/*"
            ]
        }
    ]
}
```

5. `Resource`를 업데이트하여 버킷 이름을 포함합니다.

   앞의 예제 버킷 정책에서 *example.com*은 버킷 이름입니다. 자체 버킷에 이 버킷 정책을 사용하려면 자체 버킷 이름과 일치하도록 이 이름을 업데이트해야 합니다.
6. 저장을 선택합니다.

   버킷에 퍼블릭 액세스 권한이 있음을 나타내는 경고가 나타납니다. 버킷 정책에 퍼블릭 레이블이 나타납니다.

   `Policy has invalid resource`라는 오류가 표시되면 버킷 정책의 버킷 이름이 사용자의 버킷 이름과 일치하는지 확인합니다. 버킷 정책 추가에 대한 자세한 내용은 S3 버킷 정책을 추가하려면 어떻게 해야 합니까?를 참조하십시오.

   오류 - 액세스 거부됨 경고가 표시되고 버킷 정책 편집기에서 버킷 정책을 저장할 수 없는 경우 계정 수준 및 버킷 수준 퍼블릭 액세스 차단 설정을 확인하여 버킷에 대한 퍼블릭 액세스를 허용하는지 확인하십시오. 웹 사이트 권한에 대한 자세한 내용은 웹 사이트 액세스에 필요한 권한을 참조하십시오.

3단계: 웹 사이트 엔드포인트 테스트

버킷을 정적 웹 사이트로 구성하고 권한을 설정하면 Amazon S3 웹 사이트 엔드포인트를 통해 웹 사이트에 액세스할 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 웹 사이트 엔드포인트를 참조하십시오. Amazon S3 웹 사이트 엔드포인트의 전체 목록은 Amazon Web Services 일반 참조의 Amazon S3 웹 사이트 엔드포인트를 참조하십시오.

S3 버킷이 호스트한 웹 사이트에 대한 모든 요청을 다른 호스트로 리디렉션하려면 어떻게 해야 합니까?

S3 버킷이 호스트한 정적 웹 사이트에 대한 모든 요청을 다른 호스트로 리디렉션할 수 있습니다.

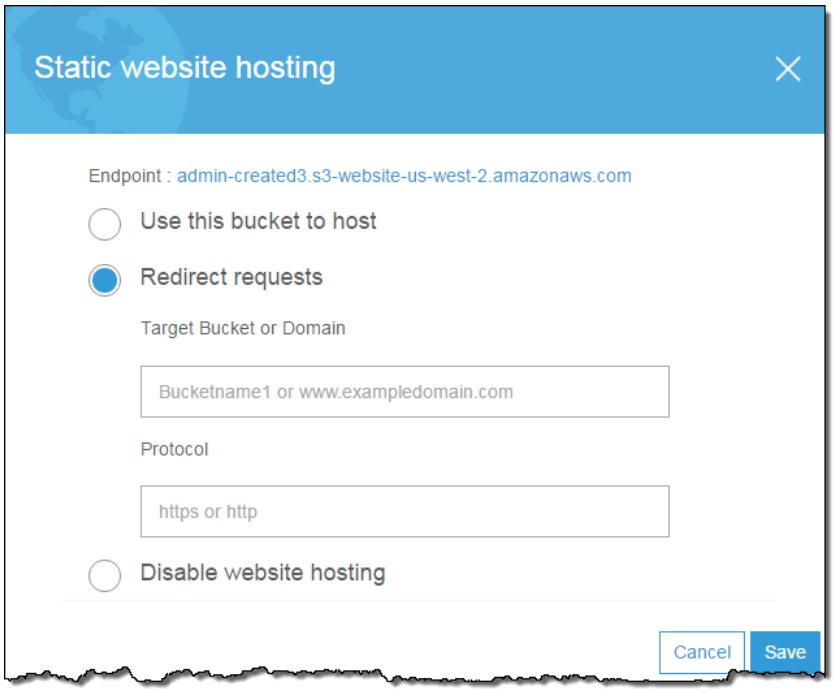
S3 버킷의 웹 사이트 엔드포인트에 대한 모든 요청을 다른 호스트로 리디렉션하는 방법

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 모든 요청을 리디렉션할 버킷 이름을 선택합니다.

3. [Properties]를 선택합니다.

4. [Static website hosting]을 선택합니다.

5. [Redirect requests]를 선택합니다.



a. 대상 버킷 또는 도메인에 요청을 리디렉션할 버킷이나 도메인 이름을 입력합니다. 요청을 다른 버킷으로 리디렉션하려면 대상 버킷의 이름을 입력하십시오. 예를 들어, 루트 도메인 어드레스로 리디렉션하려면 www.example.com을 입력해야 합니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드에서 웹사이트 호스팅용 버킷 구성을 참조하십시오.

b. 프로토콜에 리디렉션 요청의 프로토콜(http, https)을 입력합니다. 프로토콜을 지정하지 않으면, 기존 요청의 프로토콜을 사용합니다. 모든 요청을 리디렉션하면 버킷의 웹 사이트 엔드포인트로 전송된 요청이 지정된 호스트 이름으로 리디렉션됩니다.

6. Save를 선택합니다.

S3 버킷 속성에 대한 고급 설정

이 단원에서는 객체 복제, 이벤트 알림 및 전송 속도 향상에 대한 고급 S3 버킷 속성 설정을 구성하는 방법에 대해 설명합니다.

주제

이벤트 알림 수신 대상을 설정하려면 어떻게 해야 합니까?

버킷에 대한 이벤트 알림을 활성화하려면 먼저 다음 대상 유형 중 하나를 설정합니다.

Amazon SNS 주제

Amazon Simple Notification Service(Amazon SNS)는 구독 중인 endpoint 또는 클라이언트에 메시지 전달 또는 전송을 조정 및 관리하는 웹 서비스입니다. Amazon SNS 콘솔로 알림을 수신할 Amazon

SNS 주제를 만들 수 있습니다. Amazon SNS 주제는 Amazon S3 버킷과 같은 리전에 있어야 합니다. Amazon SNS 주제 생성에 대한 정보는 Amazon Simple Notification Service 개발자 안내서의 시작하기를 참조하십시오.

이벤트 알림 대상으로 만든 Amazon SNS 주제를 사용하려면 다음과 같이 수행합니다.

- Amazon SNS 주제에 대한 Amazon 리소스 이름(ARN)
- 유효한 Amazon SNS 주제 구독(Amazon SNS 주제에 메시지가 게시되면 해당 주제 구독자에게 알림이 전송됨)
- 사용자가 Amazon SNS 콘솔에 설정한 권한 정책(아래 예제 참고)

```
{
  "Version":"2012-10-17",
  "Id": "__example_policy_ID",
  "Statement":[
    {
      "Sid": "example-statement-ID",
      "Effect":"Allow",
      "Principal": "*",
      "Action": "SNS:Publish",
      "Resource":"arn:aws:sns:region:account-number:topic-name",
      "Condition": {
        "ArnEquals": {
        "aws:SourceArn": "arn:aws:s3:::bucket-name"
         }
       }
     }
   ]
}
```

Amazon SQS 대기열

Amazon SQS 콘솔을 이용해 알림을 수신할 Amazon SQS 대기열을 만들 수 있습니다. Amazon SQS 대기열은 Amazon S3 버킷과 같은 리전에 있어야 합니다. Amazon SQS 대기열 생성에 대한 자세한 내용은 Amazon Simple Queue Service 개발자 안내서의 Amazon SQS 시작하기 단원을 참조하십시오.

이벤트 알림 대상으로 만든 Amazon SQS 대기열 사용하려면 다음과 같이 수행합니다.

- Amazon SQS 주제에 대한 Amazon 리소스 이름(ARN)
- 사용자가 Amazon SQS 콘솔에 설정한 권한 정책(아래 예제 참고)

```
{
  "Version":"2012-10-17",
  "Id": "__example_policy_ID",
  "Statement":[
    {
      "Sid": "example-statement-ID",
      "Effect":"Allow",
      "Principal": "*",
      "Action": "SQS:*",
      "Resource":"arn:aws:sqs:region:account-number:queue-name",
      "Condition": {
        "ArnEquals": {
        "aws:SourceArn": "arn:aws:s3:::bucket-name"
         }
       }
     }
   ]
}
```

Lambda 기능

AWS Lambda 콘솔을 사용하여 Lambda 함수를 생성할 수 있습니다. Lambda 함수는 S3 버킷과 같은 리전에 있어야 합니다. Lambda 함수 생성에 대한 자세한 내용은 AWS Lambda Developer Guide을 참조하십시오.

Lambda 함수를 이벤트 알림 대상으로 사용하려면 먼저 Lambda 함수를 이벤트 알림 대상으로 설정할 Lambda 함수의 이름 또는 ARN이 있어야 합니다.

Warning

알림이 알림을 트리거하는 버킷에 기록되면 실행 루프가 발생할 수 있습니다. 예를 들어, 객체가 업로드될 때마다 버킷이 Lambda 함수를 트리거하고 그 함수가 객체를 버킷에 업로드하는 경우 함수는 간접적으로 자신을 트리거합니다 이렇게 되지 않도록 하려면 두 개의 버킷을 사용하거나, 수신 객체에 사용되는 접두사에만 적용되도록 트리거를 구성합니다.
AWS Lambda를 이용한 Amazon S3 알림에 대한 자세한 내용과 사용 예는 AWS Lambda Developer Guide의 Amazon S3와 함께 AWS Lambda 사용을 참조하십시오.

S3 버킷에 대한 이벤트 알림을 활성화하고 구성하려면 어떻게 해야 합니까?

특정 Amazon S3 버킷 이벤트를 활성화해 이벤트가 발생할 때마다 대상에 알림을 보낼 수 있습니다. 이 단원에서는 Amazon S3 콘솔로 이벤트 알림을 활성화하는 방법을 살펴봅니다. AWS SDK 및 Amazon S3 REST API의 이벤트 알림 사용에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 이벤트 알림 구성을 참조하십시오.

주제

이벤트 알림 유형

버킷에 대한 이벤트 알림을 구성할 때 알림을 받을 이벤트 유형을 지정해야 합니다. 이벤트 유형의 전체 목록은 Amazon Simple Storage Service 개발자 가이드의 지원되는 이벤트 유형 섹션을 참조하십시오.

Amazon S3 콘솔에는 다음과 같은 이벤트 알림 구성 옵션이 있습니다. 단일 옵션 또는 여러 옵션을 선택할 수 있습니다.

- 객체 생성
  - 객체 생성(모두) – 버킷에 객체가 생성될 때마다 알림
  - Put, Post, Copy 및 멀티파트 업로드 완료 – 특정 객체 생성 작업에 대한 알림
- 객체 삭제
  - 객체 삭제(모두) – 버킷의 객체가 삭제될 때마다 알림
  - 삭제 마커 생성 – 버전이 지정된 객체에 대해 삭제 마커가 생성되면 알림

    버전이 지정된 객체 삭제에 대한 자세한 내용은 객체 버전 삭제를 참조하십시오. 객체 버전 관리에 대한 자세한 내용은 객체 버전 관리 및 버전 관리 사용을 참조하십시오.
- S3 Glacier 스토리지 클래스에서 객체 복원
  - 복원 시작 – 개체 복원 시작 알림
  - 복원 완료 – 개체 복원 완료 알림

- RRS(Reduced Redundancy Storage) 객체 손실 이벤트
  - RSS 객체 손실 – RRS 스토리지 클래스의 객체가 손실되었다는 알림
- Amazon S3 복제 시간 제어를 사용하는 복제에 적합한 객체
  - 복제 시간 임계값 누락 – 객체가 복제되지 않았다는 알림
  - 임계값 이후 복제 시간 완료 – 객체가 복제에 대한 15분 임계값을 초과했다는 알림
  - 복제 시간 추적되지 않음 – 15분 임계값 이후에 객체가 복제되었다는 알림
  - 복제 시간 실패 – 복제에 적합한 객체가 복제 지표로 더 이상 추적되지 않는다는 알림

Note

폴더에서 마지막 객체를 삭제하면 Amazon S3가 객체 생성 이벤트를 생성할 수 있습니다. 같은 접두사를 사용하며 이름에 후행 슬래시(/)가 있는 객체가 여러 개 있다면, 이러한 객체는 Amazon S3 콘솔에 폴더의 일부로 표시됩니다. 폴더 이름은 후행 슬래시(/) 앞에 있는 문자로 형성됩니다.
해당 폴더에 있는 객체를 모두 삭제하면, 빈 폴더를 나타내는 실제 객체는 존재하지 않습니다. 이러한 상황에서는, Amazon S3 콘솔이 해당 폴더를 나타내는 0바이트 객체를 생성합니다. 객체 생성 시 이벤트 알림을 활성화하면, 콘솔이 수행한 0바이트 객체 생성 작업이 객체 생성 이벤트를 트리거합니다.
Amazon S3 콘솔에는 다음과 같은 상황에서 폴더가 표시됩니다.

- 0 바이트 객체의 이름에 후행 슬래시(/)가 있는 경우. 이 경우 폴더를 나타내는 0 바이트의 실제 Amazon S3 객체가 있습니다.
- 객체의 이름에 슬래시(/)가 있는 경우. 이 경우 폴더를 나타내는 실제 객체가 없습니다.

이벤트 알림 대상

버킷에 대한 이벤트 알림을 구성할 때 알림 대상도 선택합니다. 이벤트 알림 메시지는 다음과 같은 대상에 보낼 수 있습니다.

- Amazon Simple Notification Service(Amazon SNS) 주제 – 구독 엔드포인트나 클라이언트로의 메시지 배달 또는 전송을 조정하고 관리합니다. Amazon SNS 주제 형식에 대한 자세한 내용은 SNS FAQ를 참조하십시오.
- Amazon Simple Queue Service(Amazon SQS) 대기열 – 컴퓨터 간에 주고받는 메시지를 저장하기 위한 안정적이고 확장성이 뛰어난 호스팅 대기열을 제공합니다. Amazon SQS에 대한 자세한 내용은 Amazon Simple Queue Service 개발자 안내서의 Amazon Simple Queue Service 소개 단원을 참조하십시오.
- AWS Lambda – Lambda 함수를 호출하고 이벤트 메시지를 인수로 제공합니다. Lambda 함수를 만들 때 사용자 지정 코드를 패키징하고 AWS Lambda에 업로드합니다. AWS Lambda은 AWS 인프라를 사용하여 사용자 대신 코드를 실행합니다. Amazon S3와 함께 Lambda을 사용하는 방법에 대한 자세한 내용은 AWS Lambda Developer Guide의 Amazon S3와 AWS Lambda 사용하기 단원을 참조하십시오.

Amazon S3 서비스 보안 주체에 이벤트 알림을 대상에 게시하는 데 필요한 권한을 부여하는 방법에 대한 자세한 내용은 Amazon S3 개발자 안내서의 대상에 이벤트 알림 메시지를 게시할 권한 부여를 참조하십시오.

Warning

알림이 알림을 트리거하는 버킷에 기록되면 실행 루프가 발생할 수 있습니다. 예를 들어, 객체가 업로드될 때마다 버킷이 Lambda 함수를 트리거하고 그 함수가 객체를 버킷에 업로드하는 경우 함수는 간접적으로 자신을 트리거합니다 이렇게 되지 않도록 하려면 두 개의 버킷을 사용하거나, 수신 객체에 사용되는 접두사에만 적용되도록 트리거를 구성합니다.
AWS Lambda를 이용한 Amazon S3 알림에 대한 자세한 내용과 사용 예는 AWS Lambda Developer Guide의 Amazon S3와 함께 AWS Lambda 사용을 참조하십시오.

이벤트 알림 활성화 및 구성

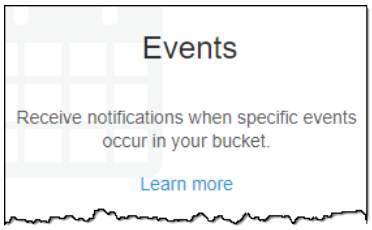
버킷에 대한 이벤트 알림을 활성화하려면 먼저 다음 대상 유형 중 하나를 설정해야 합니다. 자세한 내용은 이벤트 알림 수신 대상을 설정하려면 어떻게 해야 합니까? (p. 22) 단원을 참조하십시오.

S3 버킷에 대한 이벤트 알림 활성화 및 구성 방법

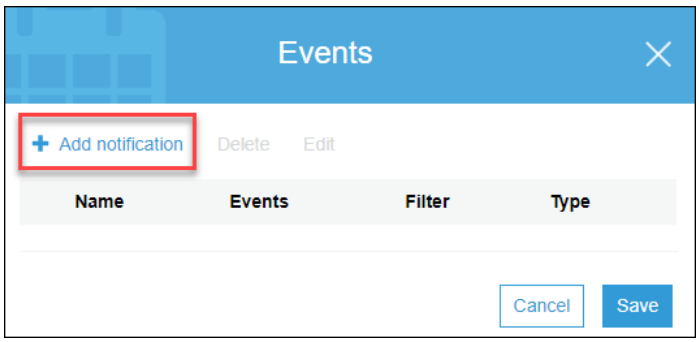
1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 이벤트를 활성화하려는 버킷의 이름을 선택합니다.

3. [Properties]를 선택합니다.

4. Advanced settings에서 이벤트를 선택합니다.

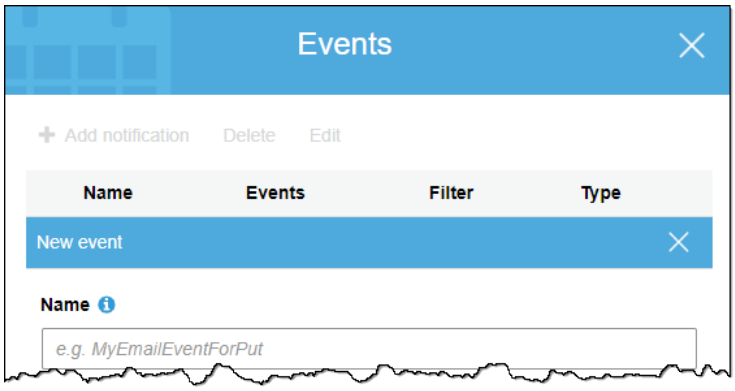


5. 알림 추가를 선택합니다.



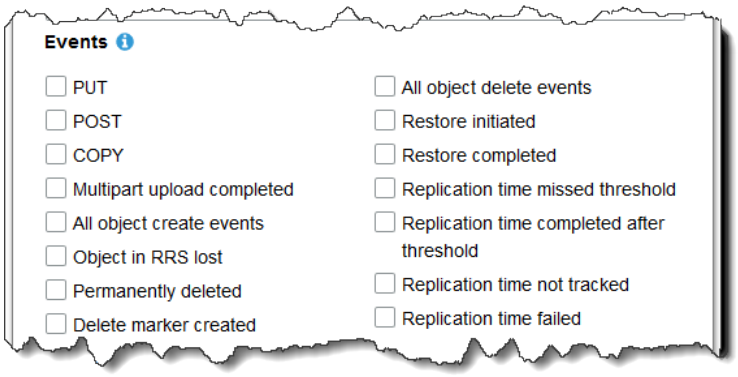
6. 이름에 이벤트 알림을 나타내는 이름을 입력합니다.

   이름을 입력하지 않으면 GUID가 생성되어 이름에 사용됩니다.



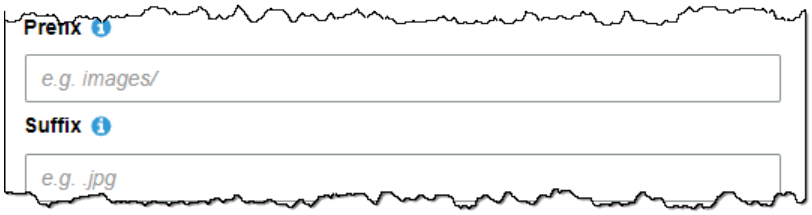
7. 이벤트 아래에서 이벤트를 하나 이상 선택합니다.

   이벤트 유형 목록은 이벤트 알림 유형 (p. 24) 단원을 참조하십시오.



8. 접두사 또는 접미사별로 이벤트 알림을 필터링하려면 접두사 또는 접미사를 입력합니다.

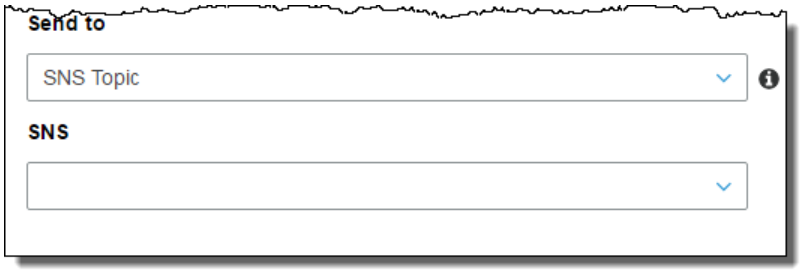
   예를 들어 특정 폴더에 파일이 추가될 때만 알림을 받도록 접두사 필터를 설정할 수 있습니다(예: `images/`). 자세한 내용은 객체 키 이름 필터링으로 알림 구성을 참조하십시오.



9. 이벤트 알림 대상(SNS 주제, SQS 대기열 또는 Lambda 함수)을 선택합니다.

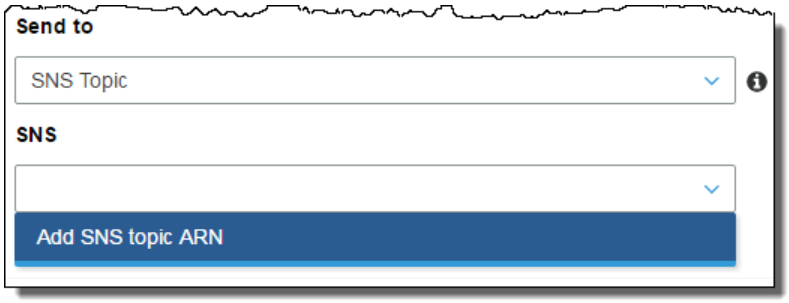
   대상에 대한 설명은 이벤트 알림 대상 (p. 25) 단원을 참조하십시오.

전송 대상 대상을 선택하면 특정 SNS, SQS 또는 Lambda 함수 대상을 입력할 수 있는 상자가 나타납니다. 아래 예제 이미지에서 전송 대상 위치는 SNS 주제이며 SNS 주제 이름에 대한 SNS 상자를 볼 수 있습니다.

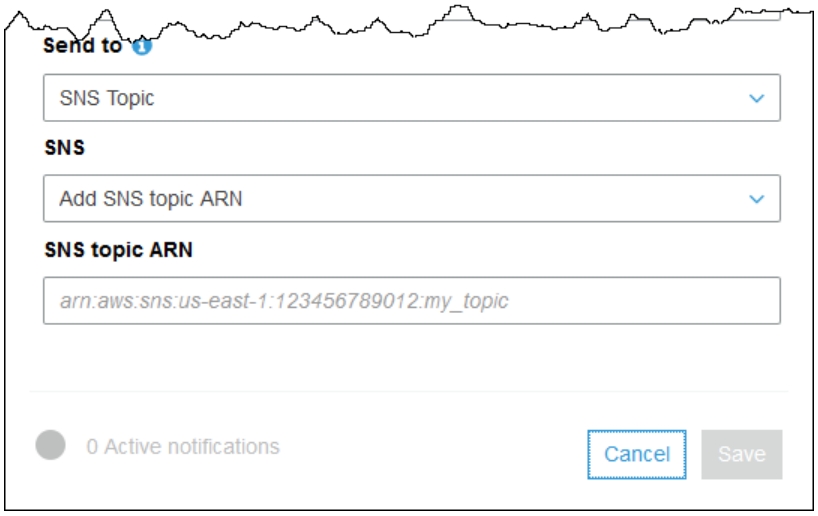


10. 표시되는 상자에서 대상 SNS, SQS 또는 Lambda 함수를 선택하거나 입력합니다.

    SNS, SQS 또는 Lambda 함수 이름을 선택 또는 입력하거나 대상 Amazon 리소스 이름(ARN) 을 선택할 수 있습니다. 아래 예제 스크린샷은 SNS 주제 ARN 추가 옵션을 보여줍니다.



11. ARN 추가를 선택한 경우 SNS 주제, SQS 대기열 또는 Lambda 함수 ARN을 입력합니다.



12. 저장을 선택합니다.

    Amazon S3에서 이벤트 알림 대상에 테스트 메시지를 보냅니다.

추가 정보

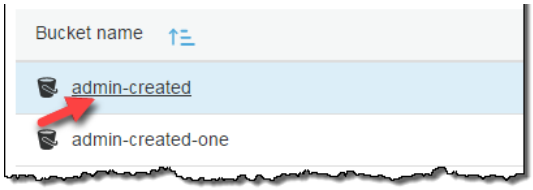
- 아카이브된 S3 객체를 복원하려면 어떻게 해야 합니까? (p. 46)

S3 버킷의 Transfer Acceleration을 활성화하려면 어떻게 해야 합니까?

Amazon Simple Storage Service(Amazon S3) Transfer Acceleration을 사용하면 클라이언트와 S3 버킷 사이에서 파일을 빠르고 쉽고 안전하게 장거리 전송할 수 있습니다. 이 주제에서는 버킷에 대해 Amazon S3 Transfer Acceleration을 활성화하는 방법을 설명합니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 Transfer Acceleration 단원을 참조하십시오.

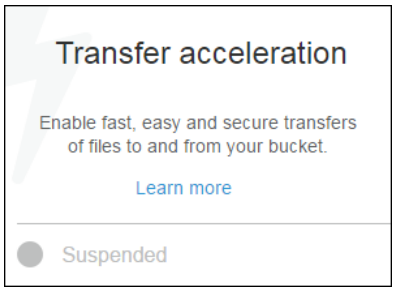
S3 버킷의 Transfer Acceleration을 활성화하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 Transfer Acceleration을 활성화하려는 버킷의 이름을 선택합니다.



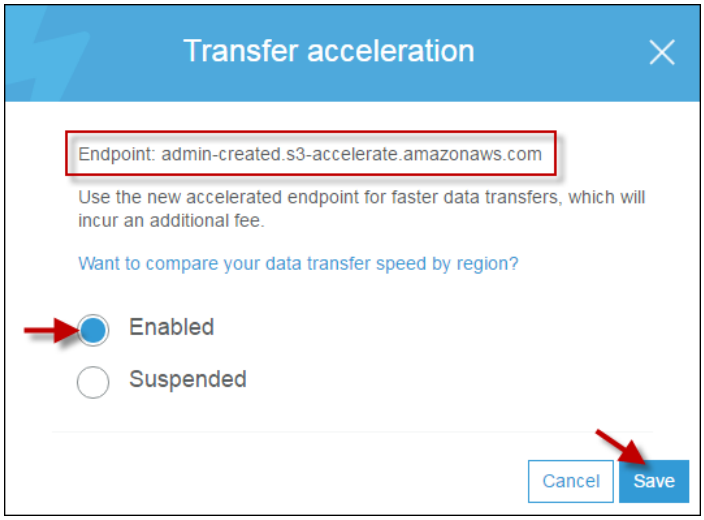
3. [Properties]를 선택합니다.

4. 전송 속도 향상을 선택합니다.



5. Enabled(활성)를 선택한 다음 Save(저장)를 선택합니다.

   엔드포인트에는 Transfer Acceleration이 설정된 버킷과 더 빠르게 데이터를 주고받는 데 사용할 엔드포인트 도메인 이름이 표시됩니다. Transfer Acceleration을 중지하면 가속 엔드포인트는 더 이상 작동하지 않습니다.



6. (선택 사항) Transfer Acceleration 버킷이 활성화된 리전부터 시작하여 가속 업로드 속도와 비가속 업로드 속도를 비교해 주는 Amazon S3 Transfer Acceleration 속도 비교 도구를 실행하려는 경우, 리전별로 데이터 전송 속도를 비교하고 싶으십니까? 옵션을 선택합니다. 이 속도 비교 도구는 멀티파트 업로드를 통해 Amazon S3 Transfer Acceleration을 사용하거나 사용하지 않으면서 브라우저에서 여러 AWS 리전으로 파일을 전송합니다.

추가 정보

S3 버킷에 대한 속성을 보려면? (p. 6)

Amazon S3 액세스 포인트 소개

Amazon S3 액세스 포인트를 사용하여 S3 객체에 대한 액세스를 관리할 수 있습니다. Amazon S3 액세스 포인트는 객체 업로드 및 검색과 같은 S3 객체 작업을 수행하는 데 사용할 수 있는 버킷에 연결된 네트워크 엔드포인트입니다. 버킷에는 최대 1,000개의 액세스 포인트가 연결될 수 있으며, 각 액세스 포인트는 고유한 권한과 네트워크 제어를 적용하여 S3 객체에 대한 액세스를 세부적으로 제어할 수 있습니다.

Amazon S3 액세스 포인트에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 액세스 포인트를 사용한 데이터 액세스 관리를 참조하십시오.

다음 주제에서는 S3 관리 콘솔을 사용하여 Amazon S3 액세스 포인트를 생성, 관리 및 사용하는 방법에 대해 설명합니다.

주제

Amazon S3 액세스 포인트 생성

이 단원에서는 AWS Management 콘솔을 사용하여 Amazon S3 액세스 포인트를 생성하는 방법에 대해 설명합니다 AWS CLI, AWS SDK 및 Amazon S3 REST API를 사용하여 액세스 포인트를 생성하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 액세스 포인트를 사용한 데이터 액세스 관리를 참조하십시오.

액세스 포인트는 정확히 하나의 Amazon S3 버킷과 연결됩니다. 시작하기 전에 이 액세스 포인트에 사용할 버킷을 생성해야 합니다. 버킷 생성에 대한 자세한 내용은 S3 버킷 생성 및 구성 (p. 3) 단원을 참조하십시오.

액세스 포인트를 생성하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. S3 버킷 섹션에서 이 액세스 포인트를 연결할 버킷을 선택합니다.
3. 버킷 세부 정보 페이지에서 액세스 포인트 탭을 선택합니다.
4. 액세스 포인트 생성을 선택합니다.
5. 액세스 포인트 이름 필드에 원하는 액세스 포인트 이름을 입력합니다.
6. 네트워크 액세스 유형을 선택합니다. Virtual Private Cloud(VPC)를 선택한 경우 액세스 포인트에 사용할 VPC ID를 입력합니다.

   액세스 포인트의 네트워크 액세스 유형에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Virtual Private Cloud(VPC)로 제한된 액세스 포인트 생성을 참조하십시오.
7. 액세스 포인트에 적용할 퍼블릭 액세스 차단 설정을 선택합니다. 모든 퍼블릭 액세스 차단 설정은 기본적으로 새 액세스 포인트에 대해 활성화되어 있으며, 특정 설정을 비활성화해야 하는 경우가 아니면 모든 설정을 활성화된 상태로 유지하는 것이 좋습니다. Amazon S3에서는 현재 액세스 포인트가 생성된 후 액세스 포인트의 퍼블릭 액세스 차단 설정을 변경하도록 지원하지 않습니다.

   액세스 포인트에서 Amazon S3 퍼블릭 액세스 차단을 사용하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 액세스 포인트에 대한 퍼블릭 액세스 관리를 참조하십시오.
8. (선택 사항) 액세스 포인트 정책을 지정합니다. 콘솔에는 정책에서 사용할 수 있는 액세스 포인트의 Amazon 리소스 이름(ARN)이 자동으로 표시됩니다.
9. 액세스 포인트 생성을 선택합니다.

Amazon S3 액세스 포인트 관리 및 사용

이 단원에서는 AWS Management 콘솔을 사용하여 Amazon S3 액세스 포인트를 관리하고 사용하는 방법에 대해 설명합니다. 각 액세스 포인트는 단일 Amazon S3 버킷과 연결됩니다. 시작하기 전에 다음 절차에 설명된 대로 버킷에 대한 액세스 포인트 목록으로 이동합니다.

버킷에 대한 액세스 포인트 목록을 찾으려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. S3 버킷 섹션에서 액세스 포인트를 관리할 버킷을 선택합니다.
3. 버킷 세부 정보 페이지에서 액세스 포인트 탭을 선택합니다.

액세스 포인트 탭에서 액세스 포인트의 구성 세부 정보를 보거나, 액세스 포인트의 정책을 편집하거나, 액세스 포인트를 사용하여 버킷에 액세스하거나, 액세스 포인트를 삭제할 수 있습니다. 다음 절차에서는 이러한 각 작업을 수행하는 방법에 대해 설명합니다.

액세스 포인트 구성 세부 정보를 보려면

1. 버킷의 액세스 포인트 탭으로 이동합니다.
2. 구성을 보려는 액세스 포인트를 찾습니다. 액세스 포인트 목록에서 액세스 포인트를 찾아보거나 이름으로 검색 필드를 사용하여 특정 액세스 포인트를 검색할 수 있습니다.
3. 구성을 보려는 액세스 포인트의 이름을 선택합니다.

   Note

   액세스 포인트의 구성을 보려면 액세스 포인트 이름 옆에 있는 옵션 버튼이 아니라 액세스 포인트 이름을 선택(클릭)합니다.

액세스 포인트 정책을 편집하려면

1. 버킷의 액세스 포인트 탭으로 이동합니다.
2. 정책을 편집할 액세스 포인트 이름 옆에 있는 옵션 버튼을 선택합니다.
3. 액세스 포인트 정책 편집을 선택합니다.
4. 텍스트 필드에 정책을 입력합니다. 콘솔에는 정책에서 사용할 수 있는 액세스 포인트의 Amazon 리소스 이름(ARN)이 자동으로 표시됩니다. 정책 생성기를 선택하여 AWS 정책 생성기를 사용해 정책을 구성할 수도 있습니다.
5. Save를 선택합니다.

액세스 포인트를 사용하여 버킷에 액세스하려면

1. 버킷의 액세스 포인트 탭으로 이동합니다.
2. 사용할 액세스 포인트 이름 옆에 있는 옵션 버튼을 선택합니다.
3. 이 액세스 포인트 사용을 선택합니다.
4. 콘솔의 버킷 이름 위에 현재 사용 중인 액세스 포인트를 나타내는 레이블이 표시됩니다. 액세스 포인트를 사용하는 동안에는 액세스 포인트 권한에서 허용하는 객체 작업만 수행할 수 있습니다.

   Note

   콘솔 보기에는 항상 버킷의 모든 객체가 표시됩니다. 이 절차에 설명된 대로 액세스 포인트를 사용하면 해당 객체에 대해 수행할 수 있는 작업은 제한되지만 버킷에 해당 객체가 존재하는지 여부는 제한되지 않습니다.
5. 버킷의 액세스 포인트 보기를 종료하려면 액세스 포인트 종료를 선택합니다.

Note

S3 관리 콘솔은 Virtual Private Cloud(VPC) 액세스 포인트를 사용하여 버킷 리소스에 액세스하는 것을 지원하지 않습니다. VPC 액세스 포인트에서 버킷 리소스에 액세스하려면 AWS CLI, AWS SDK 또는 Amazon S3 REST API를 사용합니다.

액세스 포인트를 삭제하려면

1. 버킷의 액세스 포인트 탭으로 이동합니다.
2. 삭제할 액세스 포인트 이름 옆에 있는 옵션 버튼을 선택합니다.
3. 삭제를 선택합니다.
4. 표시되는 텍스트 필드에 액세스 포인트 이름을 입력하여 액세스 포인트를 삭제할 것인지 확인하고 확인을 선택합니다.

객체 업로드, 다운로드 및 관리

Amazon S3에 데이터(사진, 동영상, 문서 등)를 업로드하려면 우선 하나의 AWS 리전에 S3 버킷을 만들어야 합니다. 그런 다음 버킷에 객체를 무제한으로 업로드할 수 있습니다.

Amazon S3에 저장하는 데이터는 객체로 이루어져 있습니다. 모든 객체는 특정 AWS 리전에서 생성되는 버킷 내에 상주합니다. Amazon S3에 저장하는 모든 객체는 버킷에 상주합니다.

특정 리전에 저장된 객체는 사용자가 명시적으로 객체를 다른 리전으로 전송하지 않는 한 해당 리전을 벗어나지 않습니다. 예를 들어 유럽(아일랜드) 리전에 저장된 객체는 해당 리전을 벗어나지 않습니다. AWS 리전에 저장된 객체는 물리적으로 해당 리전에 유지됩니다. Amazon S3가 복사본을 유지하거나 객체를 다른 리전으로 이동하지 않습니다. 그러나 그렇게 할 권한이 있는 경우 어디서든 객체에 액세스할 수 있습니다.

객체를 Amazon S3로 업로드하려면 먼저 버킷에 대한 쓰기 권한을 부여 받아야 합니다.

객체는 이미지, 백업, 데이터, 동영상 등 임의의 파일 형식일 수 있습니다. 또한 버킷에 저장할 수 있는 객체 수에는 제한이 없습니다. Amazon S3 콘솔을 사용하여 업로드할 수 있는 파일의 최대 크기는 160GB입니다. 160GB가 넘는 파일을 업로드하려면 AWS CLI, AWS SDK 또는 Amazon S3 REST API를 사용하십시오. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드에서 객체 업로드 항목을 참조하십시오.

다음 주제에서는 Amazon S3 콘솔을 사용하여 객체를 업로드, 삭제 및 관리하는 방법을 살펴봅니다.

주제

S3 버킷에 파일 및 폴더를 업로드하려면 어떻게 해야 합니까?

이 주제에서는 AWS Management 콘솔을 사용하여 하나 이상의 파일이나 전체 폴더를 Amazon S3 버킷에 업로드하는 방법을 설명합니다. Amazon S3 버킷에 파일과 폴더를 업로드하려면 해당 버킷에 대한 쓰기 권한이 있어야 합니다. 액세스 권한에 대한 자세한 내용은 버킷 및 객체 액세스 권한 설정 (p. 110)을 참조하십시오. 프로그래밍 방식으로 파일을 업로드하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 객체 업로드 단원을 참조하십시오.

Amazon S3에 업로드한 파일은 S3 객체로 저장됩니다. 객체는 파일 데이터 및 그 객체를 설명하는 메타데이터로 구성됩니다. 또한 버킷에 저장할 수 있는 객체 수에는 제한이 없습니다.

이미지, 백업, 데이터, 동영상 등 모든 유형의 파일을 S3 버킷에 업로드할 수 있습니다. Amazon S3 콘솔을 사용하여 업로드할 수 있는 파일의 최대 크기는160GB입니다. 160GB가 넘는 파일을 업로드하려면 AWS CLI, AWS SDK 또는 Amazon S3 REST API를 사용하십시오. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드에서 객체 업로드 항목을 참조하십시오.

파일을 끌어서 놓거나 선택하여 클릭하는 방법으로 업로드할 수 있습니다. 폴더를 업로드할 때는 반드시 끌어서 놓아야 합니다. 끌어서 놓기 기능은 Chrome 및 Firefox 브라우저에서만 지원됩니다. 지원되는 Chrome 및 Firefox 브라우저 버전은 AWS Management Console을 사용할 수 있는 브라우저는 무엇입니까?를 참조하십시오.

폴더를 업로드하면 Amazon S3는 지정된 폴더의 모든 파일과 하위 폴더를 버킷으로 업로드합니다. 그러면 업로드된 파일 이름과 폴더 이름을 조합하여 객체 키 이름이 지정됩니다. 예를 들어, `sample1.jpg` 및 `sample2.jpg`라는 두 개의 파일을 포함하는 폴더 `/images`를 업로드하는 경우 Amazon S3가 파일을 업로드한 다음 해당 키 이름인 `images/sample1.jpg` 및 `images/sample2.jpg`를 할당합니다. 키 이름에는 폴더 이름이 접두사로 포함됩니다. Amazon S3 콘솔에는 마지막 "/" 이후의 키 이름 부분만 표시됩니다. 예를 들어, 이미지 폴더의 `images/sample1.jpg`와 `images/sample2.jpg` 객체는 `sample1.jpg` 및 `sample2.jpg`로 표시됩니다.

개별 파일을 업로드하고 Amazon S3 콘솔에서 폴더를 열어 두면, Amazon S3는 해당 파일을 업로드할 때 열려 있는 폴더 이름을 키 이름의 접두사로 사용합니다. 예를 들어, Amazon S3 콘솔에서 `backup`이라는 폴더를 열고 `sample1.jpg`라는 파일을 업로드하면 키 이름은 `backup/sample1.jpg`가 됩니다. 그러나 콘솔에는 해당 객체가 `sample1.jpg` 폴더의 `backup`로 표시됩니다.

개별 파일을 업로드하고 Amazon S3 콘솔에서 폴더를 열지 않으면, Amazon S3는 해당 파일을 업로드할 때 파일 이름만 키 이름으로 할당합니다. 예를 들어, `sample1.jpg`라는 파일을 업로드하면 키 이름은 `sample1.jpg`가 됩니다. 키 이름에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 객체 키와 메타데이터 단원을 참조하십시오.

버전 관리를 사용하는 버킷에 이미 키 이름이 있는 객체를 업로드하면 Amazon S3는 기존 객체를 대체하는 대신 객체의 다른 버전을 만듭니다. 버전 관리에 대한 자세한 내용은 S3 버킷의 버전 관리 기능을 활성화하거나 해제하려면? (p. 7) 단원을 참조하십시오.

주제

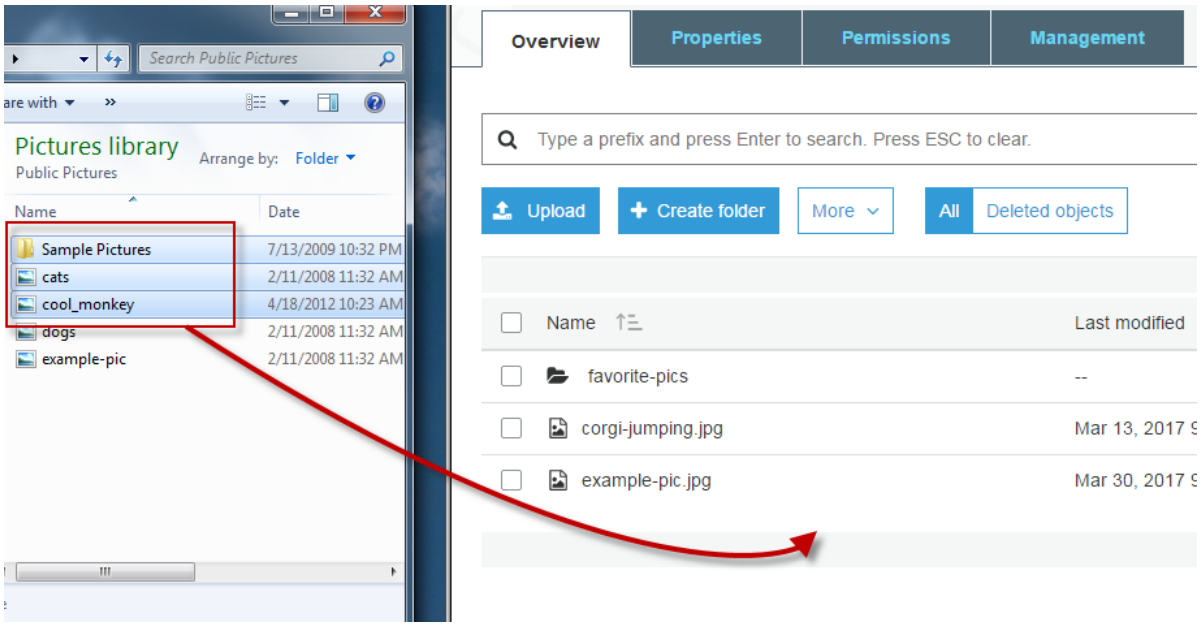
끌어서 놓기를 사용하여 파일 및 폴더 업로드

Chrome이나 Firefox 브라우저를 사용하는 경우, 업로드할 폴더와 파일을 선택한 후 대상 버킷으로 끌어 놓을 수 있습니다. 폴더를 업로드하는 방법은 끌어서 놓기뿐입니다.

끌어서 놓기를 사용하여 폴더 및 파일을 S3 버킷으로 업로드하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 폴더 또는 파일을 업로드할 버킷 이름을 선택합니다.

3. 콘솔 창 이외의 창에서 업로드할 파일과 폴더를 선택합니다. 그런 다음 선택한 항목을 대상 버킷의 객체가 나열되어 있는 콘솔 창으로 끌어서 놓습니다.



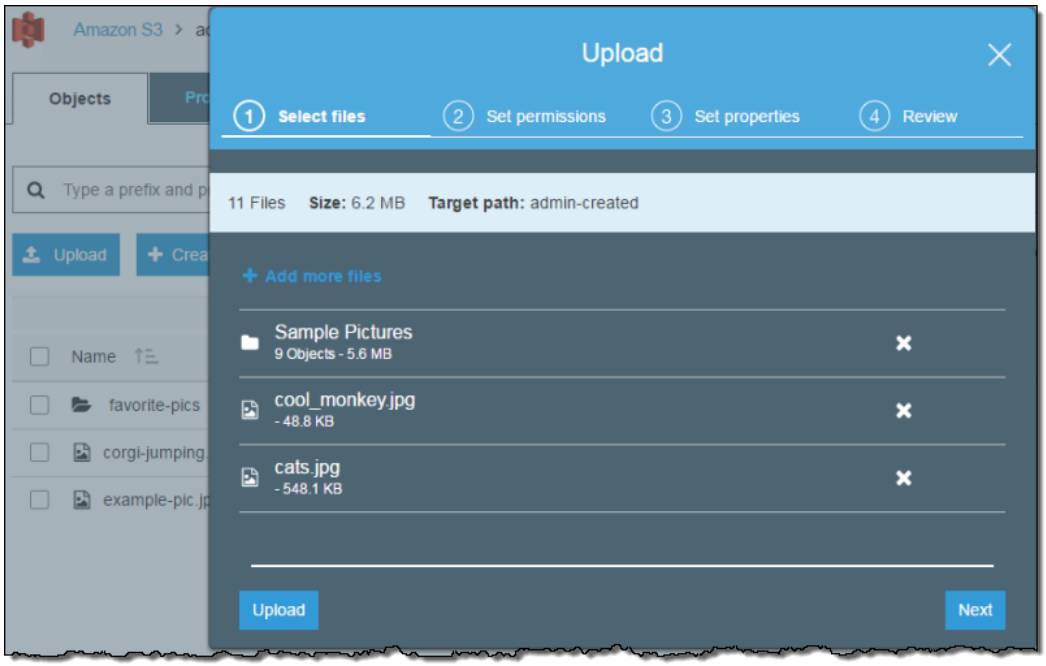
선택한 파일들이 업로드 대화 상자에 나열됩니다.

4. 업로드 대화 상자에서 다음 중 하나를 수행합니다.

   a. 업로드 대화 상자가 표시된 콘솔 창에 파일과 폴더를 더 많이 끌어다 놓습니다. 파일을 더 추가를 선택하여 파일을 더 추가할 수도 있습니다. 이 옵션은 폴더가 아닌 파일에 한해 사용할 수 있습니다.

   b. 특정 사용자의 권한을 부여 또는 제거하거나 업로드할 모든 파일에 대해 퍼블릭 권한을 설정하지 않고 나열된 파일과 폴더를 즉시 업로드하려면 업로드를 선택합니다. 객체 액세스 권한에 대한 자세한 내용은 객체에 대한 권한은 어떻게 설정하나요? (p. 115)를 참조하십시오.

   c. 업로드할 파일에 대한 권한 또는 속성을 설정하려면 다음을 선택합니다.

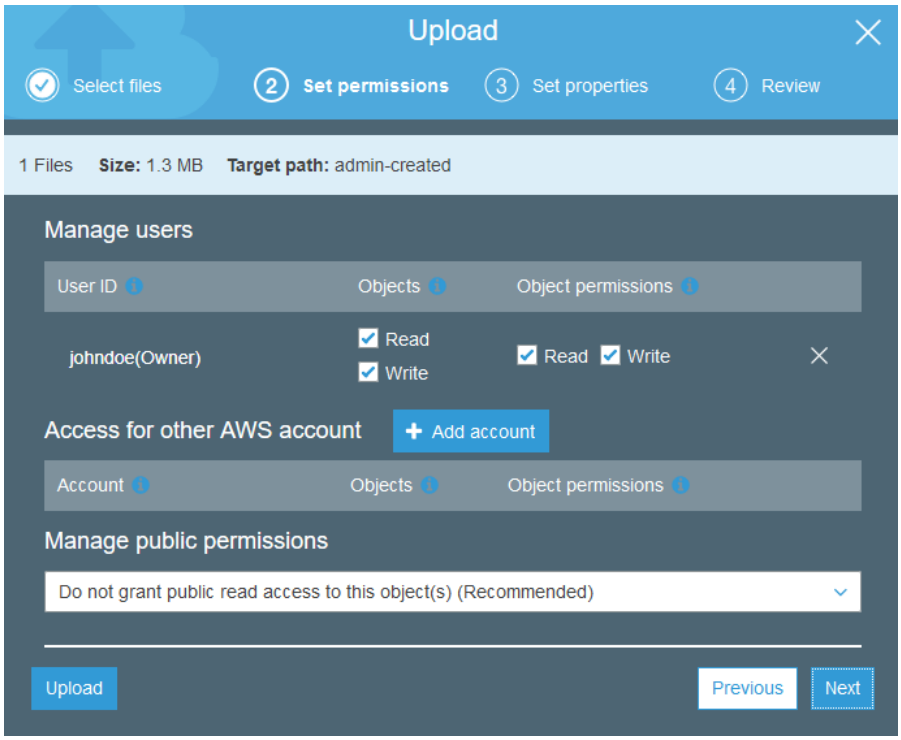


5. 권한 설정 페이지의 사용자 관리에서 AWS 계정 소유자에 대한 권한을 변경할 수 있습니다. 소유자란 AWS Identity and Access Management(IAM) 사용자가 아닌 AWS 계정 루트 사용자를 지칭합니다. 루트 사용자에 대한 자세한 내용은 AWS 계정 루트 사용자 단원을 참조하십시오.

   다른 AWS 계정에 액세스를 허용하려면 Add account를 선택합니다. 다른 AWS 계정에 권한을 부여하는 것에 대한 자세한 정보는 ACL 버킷 권한을 설정하려면 어떻게 해야 합니까? (p. 118) 단원을 참조하십시오.

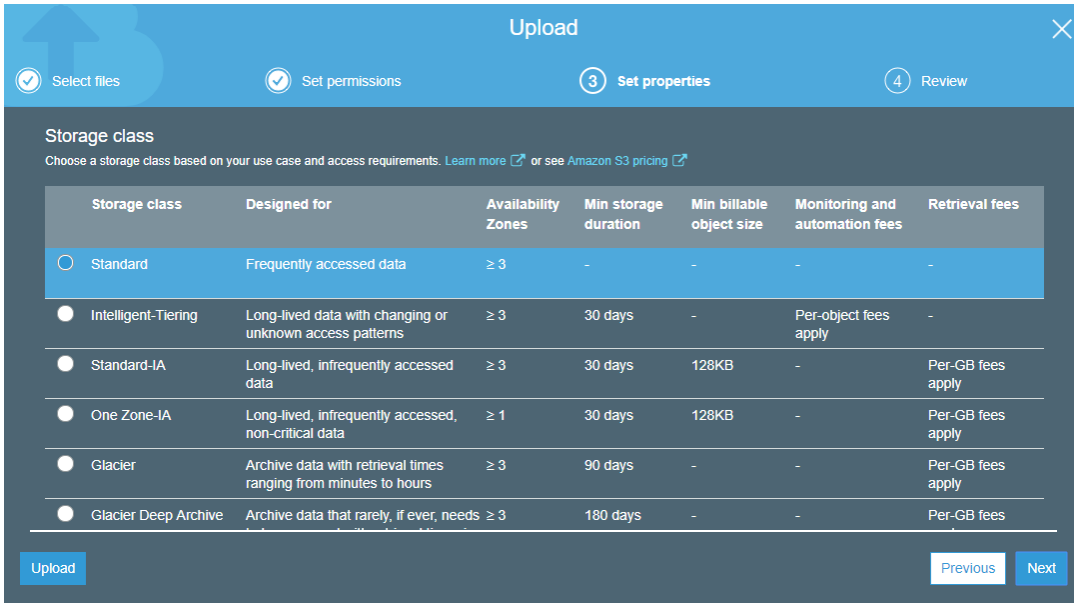
   퍼블릭 권한 관리에서 업로드 중인 모든 파일에 대해 일반 대중(전 세계 모든 사람)에게 객체에 대한 읽기 액세스 권한을 부여할 수 있습니다. 퍼블릭 읽기 액세스 권한 부여는 웹 사이트에 버킷을 사용하는 경우와 같은 사용 사례의 작은 하위 집합에 적용할 수 있습니다. Do not grant public read access to this object(s)(이 버킷에 퍼블릭 읽기 액세스를 부여하지 말 것)의 기본 설정은 변경하지 않는 것이 좋습니다. 객체를 업로드한 후에도 언제든 객체 권한을 변경할 수 있습니다. 객체 액세스 권한에 대한 자세한 내용은 객체에 대한 권한은 어떻게 설정하나요? (p. 115)를 참조하십시오.

   권한 구성이 끝나면 다음을 선택합니다.



6. 속성 설정 페이지에서 업로드하는 파일에 사용할 스토리지 클래스와 암호화 방법을 선택할 수 있습니다. 메타데이터를 추가하거나 수정할 수도 있습니다.

   a. 업로드할 파일의 스토리지 클래스를 선택합니다. 스토리지 클래스에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 스토리지 클래스 단원을 참조하십시오.



b. 업로드할 파일의 암호화 유형을 선택합니다. 암호화하지 않으려면 없음을 선택합니다.

   i. Amazon S3에서 관리하는 키를 사용하여 업로드된 파일을 암호화하려면 Amazon S3 마스터 키를 선택합니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3가 관리하는 암호화 키 클래스를 사용하는 데이터 보호 단원을 참조하십시오.

   ii. AWS Key Management Service(AWS KMS)를 사용하여 업로드된 파일을 암호화하려면 AWS KMS 마스터 키를 선택합니다. 그런 다음 AWS KMS CMK 목록에서 고객 마스터 키(CMK)를 선택합니다.

   > Note
   >
   > 버킷의 객체를 암호화할 때는 해당 버킷과 동일한 AWS 리전에 있는 CMK만 사용할 수 있습니다.

   AWS KMS CMK로 보호되는 객체를 사용할 수 있는 능력을 외부 계정에 부여할 수 있습니다. 이렇게 하려면 목록에서 사용자 지정 KMS ARN을 선택한 후 외부 계정의 Amazon 리소스 이름(ARN)을 입력합니다. AWS KMS CMK로 보호되는 객체에 대한 사용 권한이 있는 외부 계정의 관리자는 리소스 레벨의 IAM 정책을 생성하여 액세스를 더 제한할 수 있습니다.

   AWS KMS CMK 생성에 대한 자세한 내용은 AWS Key Management Service Developer Guide의 키 생성을 참조하십시오. AWS KMS로 데이터를 보호하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 AWS KMS에 저장된 키(SSE-KMS)로 데이터 보호를 참조하십시오.

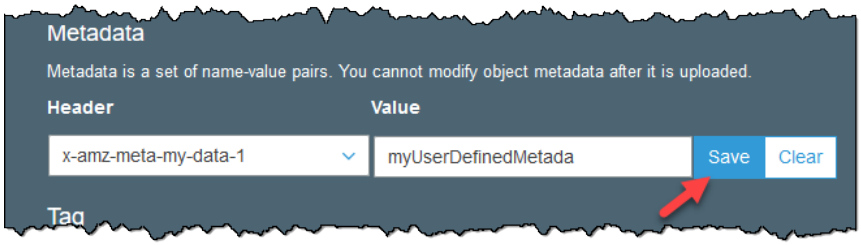
c. Amazon S3 객체 메타데이터는 이름-값(키-값) 페어로 표현됩니다. 시스템 정의 메타데이터 및 사용자 정의 메타데이터라는 두 종류의 메타데이터가 있습니다.

   업로드하는 모든 객체에 Amazon S3 시스템 정의 메타데이터를 추가하려면 헤더에서 헤더를 선택합니다. Content-Type과 Content-Disposition 같은 공통 HTTP 헤더를 선택할 수 있습니다. 헤더의 값을 입력한 후 저장을 선택합니다. 시스템 정의 메타데이터 목록과 값 추가 가능 여부를 확인하려면 Amazon Simple Storage Service 개발자 가이드의 시스템 정의 메타데이터 단원을 참조하십시오.

d. 접두사 `x-amz-meta-`로 시작하는 모든 메타데이터는 사용자 정의 메타데이터로 처리됩니다. 사용자 정의 메타데이터는 객체와 함께 저장되었다가 해당 객체를 다운로드할 때 반환됩니다.

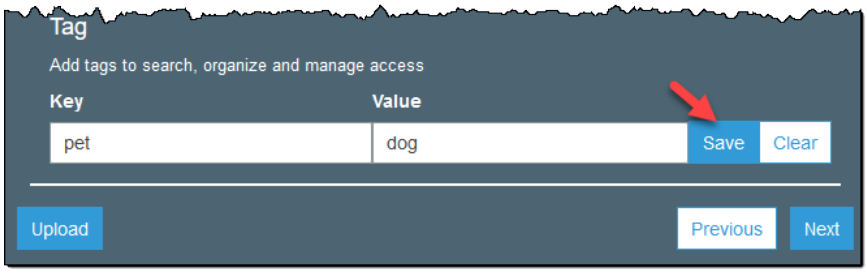
   업로드하는 모든 객체에 사용자 정의 메타데이터를 추가하려면 헤더 필드에 `x-amz-meta-`와 함께 사용자 정의 메타데이터 이름을 입력합니다. 헤더의 값을 입력한 후 저장을 선택합니다. 키와 값 모두 US-ASCII 표준에 부합해야 합니다. 사용자 정의 메타데이터의 최대 크기는 2KB입니다. 사용자

정의 메타데이터에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 사용자 정의 메타데이터 단원을 참조하십시오.

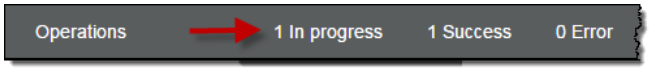


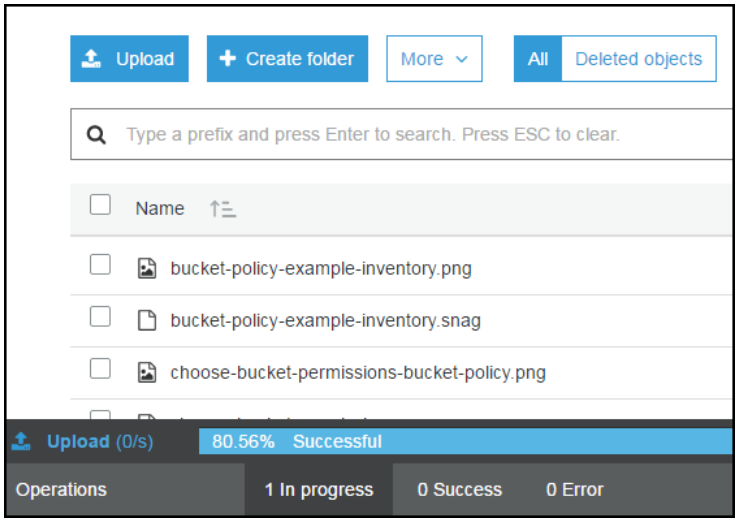
e. 객체 태그 지정을 통해 스토리지를 분류할 수 있습니다. 각 태그는 키-값 페어입니다. 키와 태그 값은 대/소문자를 구분합니다. 객체마다 태그를 10개까지 포함할 수 있습니다.

   업로드하는 모든 객체에 태그를 추가하려면 키 필드에 태그 이름을 입력합니다. 태그의 값을 입력한 후 저장을 선택합니다. 태그 키는 최대 128개 유니코드 문자이며, 태그 값은 최대 255개 유니코드 문자입니다. 객체 태그에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 객체 태그 지정 단원을 참조하십시오.

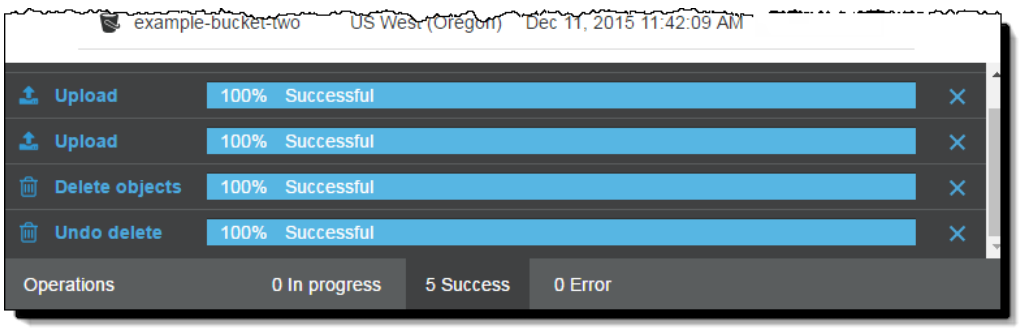


7. [Next]를 선택합니다.
8. 업로드 검토 페이지에서 설정이 올바른지 확인한 후 업로드를 선택합니다. 변경하려면 이전을 선택합니다.
9. 업로드 진행 상황을 보려면 브라우저 창 하단에서 진행 중을 선택합니다.





업로드 및 기타 작업의 기록을 보려면 성공을 선택합니다.

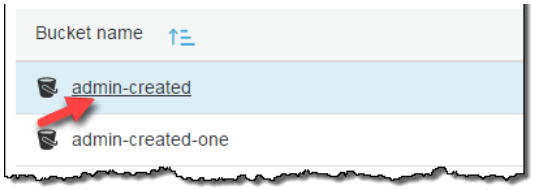


선택하여 클릭하기로 파일 업로드

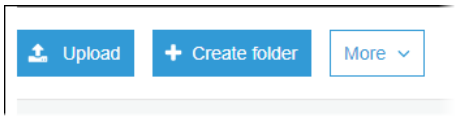
이 절차에서는 업로드를 선택하여 S3 버킷에 파일을 업로드하는 방법을 설명합니다.

선택하여 클릭하기로 S3 버킷에 파일을 업로드하려면

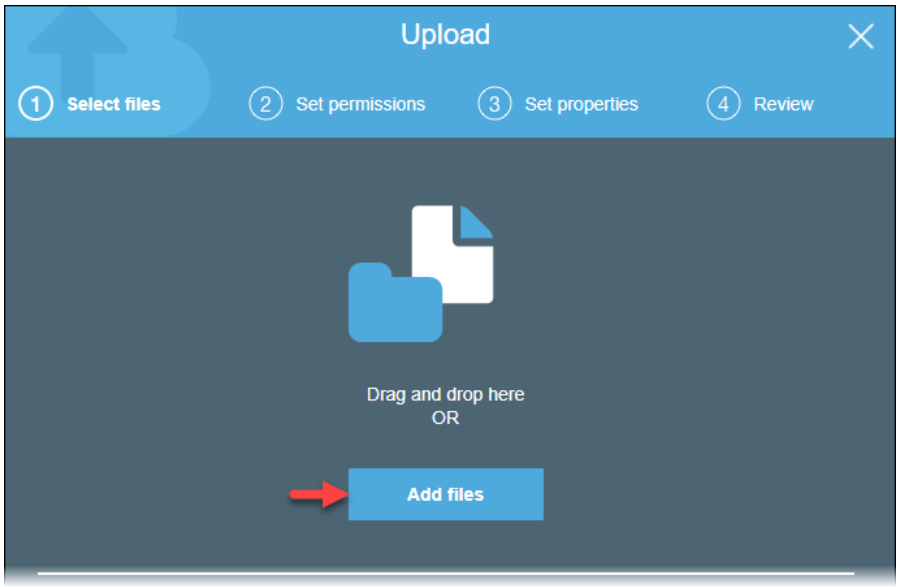
1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 파일을 업로드하려는 버킷 이름을 선택합니다.



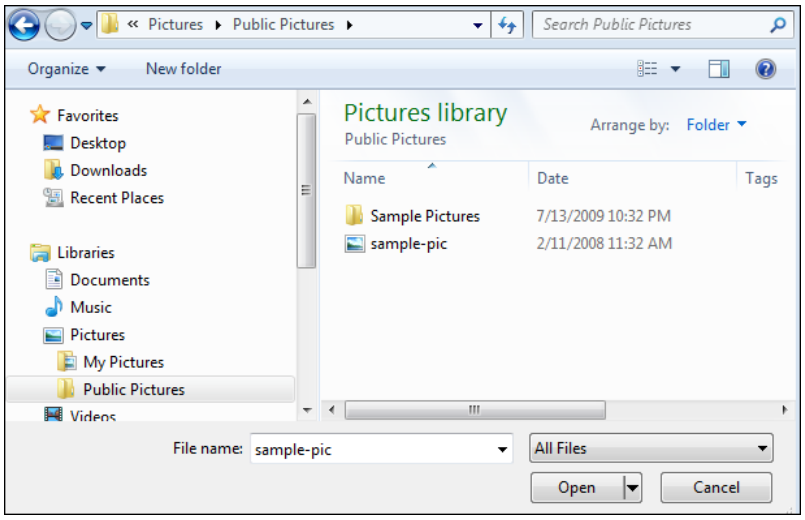
3. Upload를 선택합니다.



4. 업로드 대화 상자에서 파일 추가를 선택합니다.

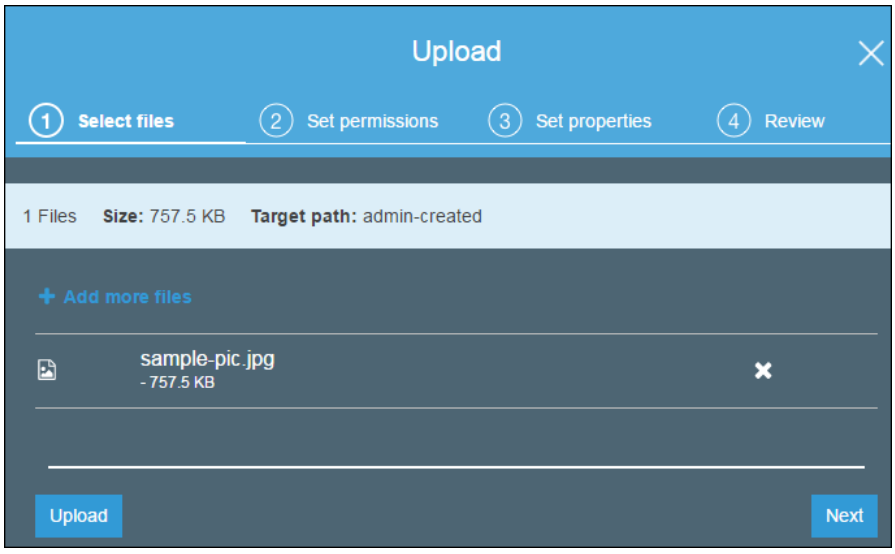


5. 업로드할 파일을 하나 이상 선택한 후 열기를 선택합니다.



6. 선택한 파일이 업로드 대화 상자에 표시되면 다음 중 하나를 수행합니다.

   a. 파일을 더 추가하려면 파일을 더 추가를 선택합니다.
   b. 나열된 파일을 즉시 업로드하려면 업로드를 선택합니다.
   c. 업로드할 파일에 대한 권한 또는 속성을 설정하려면 다음을 선택합니다.



7. 권한과 속성을 설정하려면 끌어서 놓기를 사용하여 파일 및 폴더 업로드 (p. 35)의 5단계부터 시작하십시오.

추가 정보

- 객체에 대한 권한은 어떻게 설정하나요? (p. 115)를 선택하십시오.
- S3 버킷에서 객체를 다운로드하려면? (p. 42)

S3 버킷에서 객체를 다운로드하려면?

이 단원에서는 Amazon S3 콘솔을 사용하여 S3 버킷에서 객체를 다운로드하는 방법을 설명합니다.

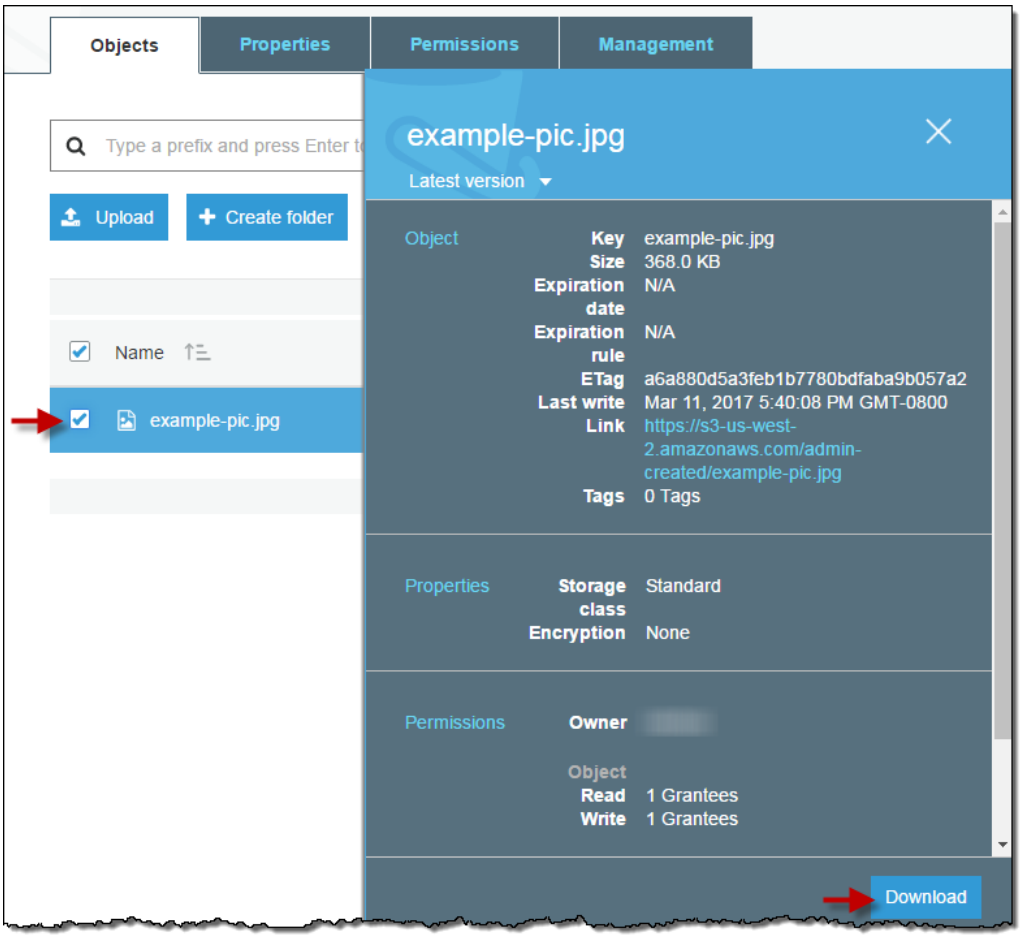
객체를 다운로드할 때는 데이터 전송 요금이 부과됩니다. Amazon S3 기능 및 요금에 대한 자세한 내용은 Amazon S3를 참조하십시오.

> **Important**
>
> 객체 키 이름이 마침표(.) 또는 2개의 마침표(..)로 구성된 경우 Amazon S3 콘솔을 사용하여 객체를 다운로드할 수 없습니다. 키 이름이 "." 또는 ".."인 객체를 다운로드하려면 AWS CLI, AWS SDK 또는 REST API를 사용해야 합니다. 객체 명명에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 객체 키 명명 지침을 참조하십시오.

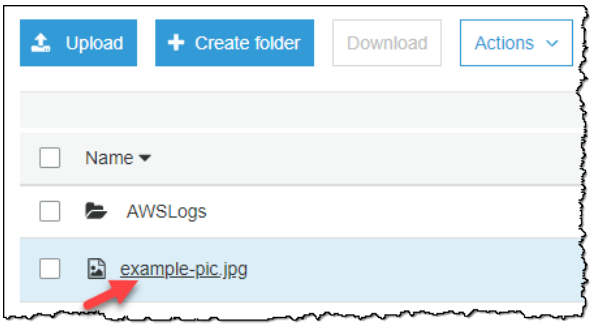
S3 버킷에서 객체를 다운로드하는 방법

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 객체를 다운로드하려는 버킷 이름을 선택합니다.

3. 다음 방법 중 하나를 사용하여 S3 버킷에서 객체를 다운로드할 수 있습니다.
   - 이름 목록에서 다운로드하려는 객체 옆에 있는 확인란을 선택한 다음 나타나는 객체 설명 페이지에서 다운로드를 선택합니다.

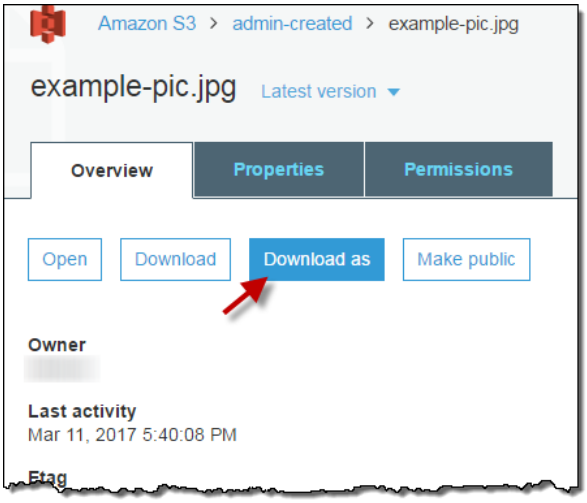


- 다운로드하려는 객체의 이름을 선택합니다.

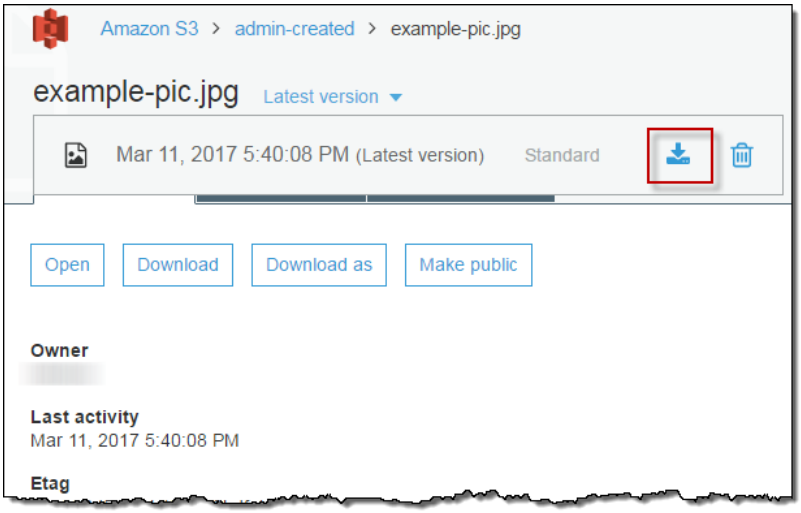


개요 페이지에서 다운로드를 선택합니다.

- 다운로드하려는 객체 이름을 선택한 다음 개요 페이지에서 다운로드를 선택합니다.



- 다운로드하려는 객체의 이름을 선택합니다. 최신 버전을 선택한 다음 다운로드 아이콘을 선택합니다.



관련 주제

- S3 버킷에 파일 및 폴더를 업로드하려면 어떻게 해야 합니까? (p. 34)

S3 버킷에서 객체를 삭제하려면?

이 단원에서는 Amazon S3 콘솔을 사용하여 객체를 삭제하는 방법을 설명합니다. S3 버킷에 있는 모든 객체에 스토리지 비용이 발생하기 때문에 더 이상 필요하지 않은 객체는 삭제해야 합니다. 예를 들어, 로그 파일을 수집하는 경우, 더 이상 필요가 없는 로그 파일은 삭제하는 것이 좋습니다. 로그 파일과 같은 객체를 자동으로 삭제하도록 수명 주기 규칙을 설정할 수 있습니다.

Amazon S3 기능 및 요금에 대한 자세한 내용은 Amazon S3를 참조하십시오.

S3 버킷에서 객체 삭제 방법

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 객체를 삭제하려는 버킷 이름을 선택합니다.
3. 다음 방법 중 하나를 사용하여 S3 버킷에서 객체를 삭제할 수 있습니다.
   - 이름 목록에서 삭제하려는 객체와 폴더 옆에 있는 확인란을 선택하고, 작업을 선택한 후 드롭다운 메뉴에서 삭제를 선택합니다.

     Delete object(객체 삭제) 대화 상자에서 삭제를 선택한 객체 및/또는 폴더의 이름이 열거되어 있는지 확인한 후 삭제를 선택합니다.
   - 또는 삭제하려는 객체 이름을 선택하고, 최신 버전을 선택한 다음 휴지통 아이콘을 선택합니다.

추가 정보

- S3 객체를 삭제 취소하려면? (p. 45)
- S3 버킷에 대한 수명 주기 정책을 생성하려면 어떻게 해야 합니까? (p. 76)

S3 객체를 삭제 취소하려면?

이 단원에서는 Amazon S3 콘솔을 사용하여 객체를 삭제 취소하는 방법에 대해 설명합니다.

삭제된 객체를 복원하려면 객체를 삭제하기 전에 해당 객체를 포함하는 버킷에 버전 관리가 활성화되어 있어야 합니다. 버전 관리 사용에 대한 자세한 내용은 S3 버킷의 버전 관리 기능을 활성화하거나 해제하려면? (p. 7) 단원을 참조하십시오.

버전 관리를 사용하는 버킷에서 한 객체를 삭제하면 모든 버전이 버킷에 그대로 유지되며 Amazon S3는 해당 객체에 대한 삭제 마커를 생성합니다. 객체 삭제를 취소하려면 이 삭제 마커를 삭제해야 합니다. 버전 관리 및 삭제 마커에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 객체 버전 관리 단원을 참조하십시오.

S3 버킷에서 삭제된 객체를 복원하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 원하는 버킷의 이름을 선택합니다.
3. 버킷의 객체 버전 목록을 확인하려면 표시를 선택합니다. 삭제된 객체들에 대한 삭제 마커를 볼 수 있습니다.

4. 어떤 객체의 삭제를 취소하려면 삭제 마커를 삭제해야 합니다. 복원할 객체의 삭제 마커 옆에 있는 확인란을 선택한 후, 작업 메뉴에서 삭제를 선택합니다.
5. 그런 다음 숨기기를 선택하면 삭제가 취소된 객체가 목록에 나타납니다.

추가 정보

- S3 객체의 버전을 보려면? (p. 56)
- S3 버킷의 버전 관리 기능을 활성화하거나 해제하려면? (p. 7)
- Amazon Simple Storage Service 개발자 가이드의 버전 관리 사용

아카이브된 S3 객체를 복원하려면 어떻게 해야 합니까?

이 섹션에서는 Amazon S3 콘솔을 사용하여 GLACIER 또는 DEEP_ARCHIVE 스토리지 클래스에 아카이브된 객체 복원 방법에 대해 설명합니다. GLACIER or DEEP_ARCHIVE에 저장된 객체는 즉시 액세스할 수 없습니다. 이 클래스의 객체에 액세스하려면 지정된 기간(일수) 동안 S3 버킷에 임시 복사본을 복원해야 합니다. GLACIER 또는 DEEP_ARCHIVE 스토리지 클래스에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드에서 스토리지 클래스 항목을 참조하십시오.

아카이브를 복원하면 아카이브 및 복원한 사본 모두에 대해 요금이 청구됩니다. 사본에 대한 스토리지 비용이 부과되기 때문에 필요한 기간 동안만 객체를 복원해야 합니다. 객체의 영구 복사본이 필요한 경우, S3 버킷에 객체의 복사본을 만드십시오. Amazon S3 기능 및 요금에 대한 자세한 내용은 Amazon S3를 참조하십시오.

객체를 복원한 뒤 개요 페이지에서 다운로드할 수 있습니다. 자세한 내용은 객체의 개요를 보려면? (p. 53) 단원을 참조하십시오.

주제

- 아카이브 검색 옵션 (p. 46)
- 아카이브된 S3 객체 복원 (p. 47)
- 진행 중인 복원 업그레이드 (p. 49)
- 아카이브 복원 상태 및 만료 날짜 확인 (p. 50)

아카이브 검색 옵션

다음은 아카이브된 객체를 복원할 때 사용 가능한 검색 옵션입니다.

- **`Expedited`** - 신속 검색을 사용하면 가끔 발생하는 아카이브의 하위 집합에 대한 긴급 요청이 필요할 때 GLACIER 스토리지 클래스에 저장된 데이터에 신속하게 액세스할 수 있습니다. 아카이브된 가장 큰 객체(250MB+)를 제외한 모든 경우, 신속 검색을 사용하여 액세스된 데이터는 일반적으로 1~5분 안에 사용할 수 있게 됩니다. 프로비저닝된 용량을 통해 필요할 때 신속 검색에 대한 검색 용량이 보장됩니다. 자세한 정보는 프로비저닝된 용량 단원을 참조하십시오. DEEP_ARCHIVE 스토리지 클래스에 저장된 객체에는 신속 검색 및 프로비저닝된 용량을 사용할 수 없습니다.
- **`Standard`** - 표준 검색을 사용하면 몇 시간 내에 아카이브된 모든 객체에 액세스할 수 있습니다. 이는 검색 옵션을 지정하지 않은 GLACIER 및 DEEP_ARCHIVE 검색 요청에 대한 기본 옵션입니다. 스탠다드 검색은 일반적으로 GLACIER 스토리지 클래스에 저장된 객체의 경우 3~5시간 이내에 완료됩니다. 일반적으로 DEEP_ARCHIVE 스토리지 클래스에 저장된 객체의 경우 12시간 이내에 완료됩니다.
- **`Bulk`** - 대량 검색은 Amazon S3 Glacier에서 가장 저렴한 검색 옵션으로 페타바이트 단위의 대용량 데이터도 저렴하게 검색할 수 있습니다. 대량 검색은 일반적으로 GLACIER 스토리지 클래스에 저장된 객체의

경우 5~12시간 이내에 완료됩니다. 일반적으로 DEEP_ARCHIVE 스토리지 클래스에 저장된 객체의 경우 48시간 이내에 완료됩니다.

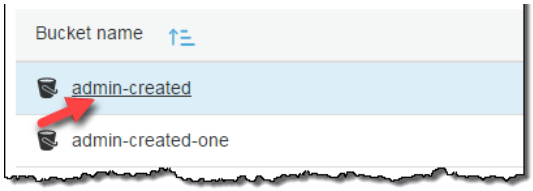
검색 옵션에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 아카이브된 객체 복원 단원을 참조하십시오.

아카이브된 S3 객체 복원

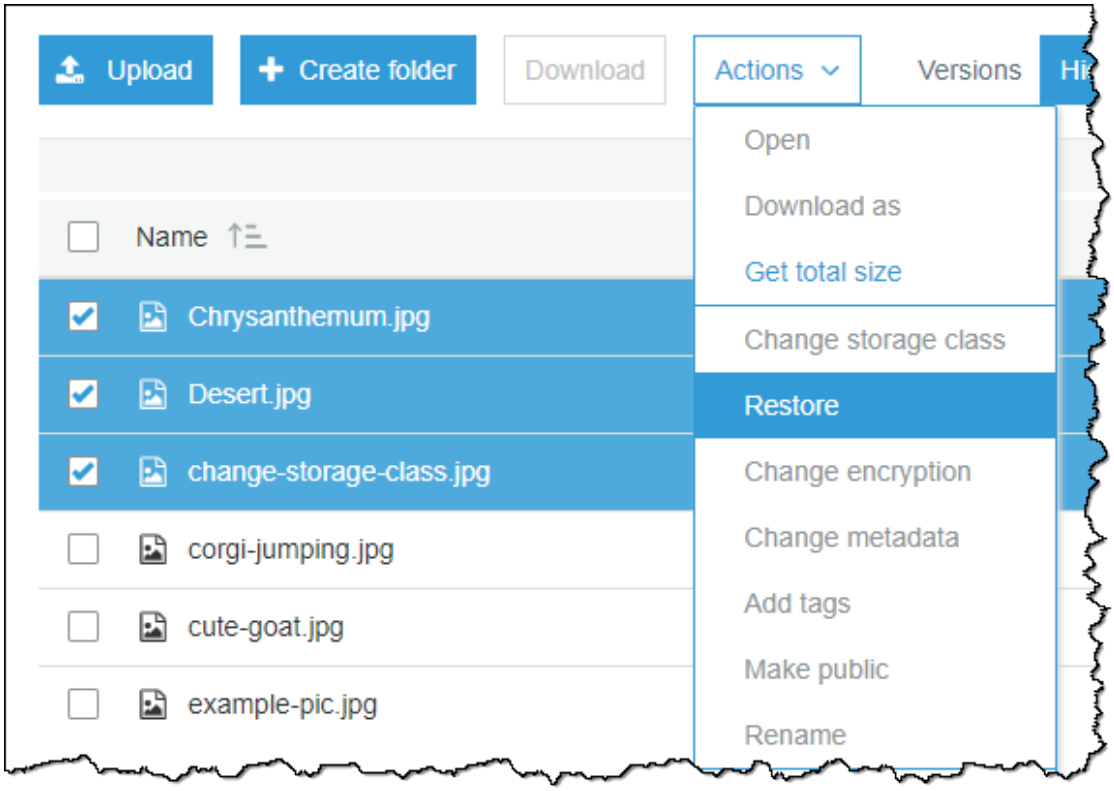
이 주제에서는 Amazon S3 콘솔을 사용하여 GLACIER 또는 DEEP_ARCHIVE 스토리지 클래스로 아카이브된 객체 복원 방법에 대해 설명합니다. (이 콘솔에는 이러한 스토리지 클래스에 Glacier 및 Glacier Deep Archive라는 이름을 사용합니다.)

아카이브된 S3 객체를 복원하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 복원할 객체가 들어 있는 버킷 이름을 선택합니다.

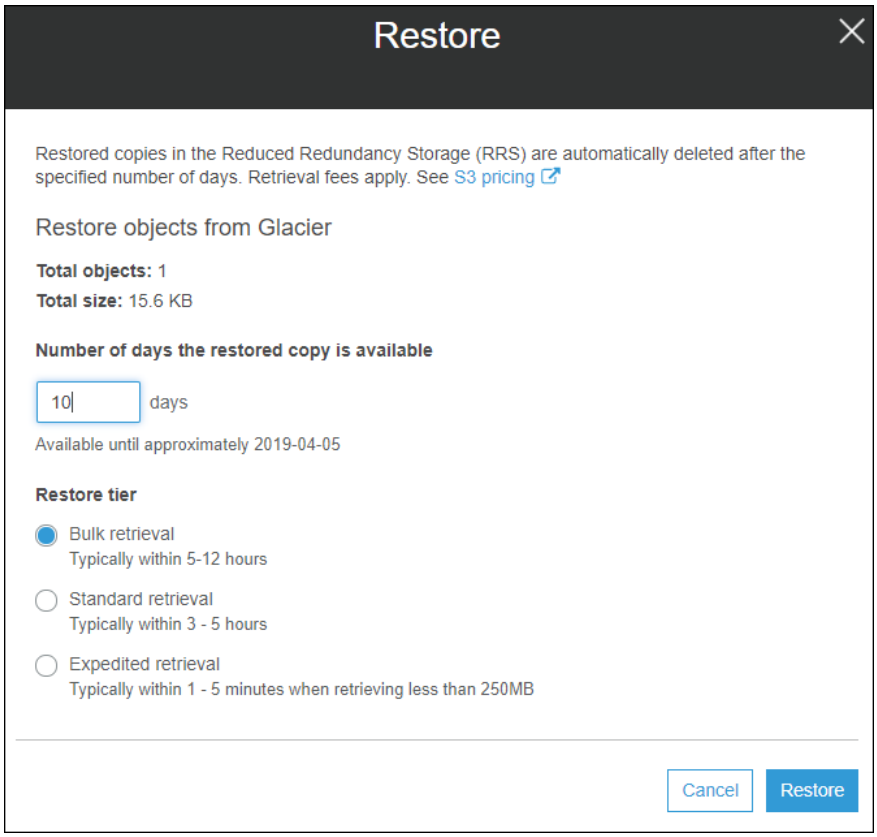


3. 이름 목록에서 객체 또는 복원할 객체를 선택하고 작업을 선택한 다음 복원을 선택합니다.



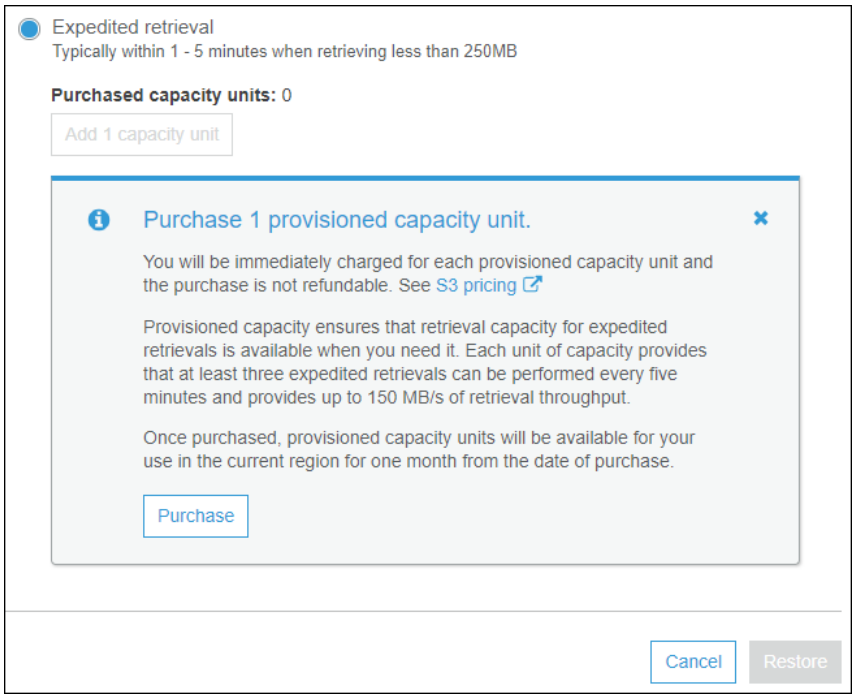
4. 복원 시작 대화 상자에 아카이브된 데이터에 액세스하고자 하는 일수를 입력합니다.
5. 검색 옵션 메뉴에서 다음 검색 옵션 중 하나를 선택합니다.

- Bulk retrieval(벌크 검색) 또는 Standard retrieval(표준 검색)을 선택하고 복원을 선택합니다.
- Expedited retrieval(신속 검색)(Glacier 스토리지 클래스에서만 사용 가능)을 선택합니다.



6. 프로비저닝된 용량은 Glacier 스토리지 클래스에서만 사용할 수 있습니다. 프로비저닝된 용량이 있는 경우, 복원을 선택하여 프로비저닝된 검색을 시작합니다. 프로비저닝된 용량이 있으면 모든 신속 검색을 프로비저닝된 용량으로 처리합니다. 프로비저닝된 용량에 대한 자세한 내용은 프로비저닝된 용량 단원을 참조하십시오.

   - 프로비저닝된 용량이 없고 구매할 계획도 없는 경우, 복원을 선택합니다.
   - 프로비저닝된 용량이 없지만 구매할 계획인 경우, 용량 단위 추가를 선택한 다음 구매하기를 선택합니다. 구매 성공 메시지가 나타나면 복원을 선택하여 프로비저닝된 검색을 시작합니다.

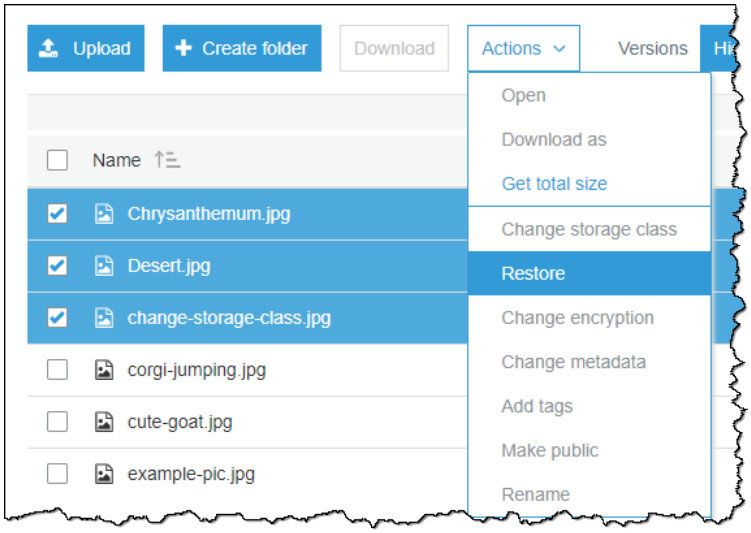


진행 중인 복원 업그레이드

복원 진행 중에 복원 속도를 업그레이드할 수 있습니다.

진행 중인 복원을 더 빠른 티어로 업그레이드하는 방법

1. 이름 목록에서 복원할 객체를 하나 이상 선택하고, 작업을 선택한 후 Restore from Glacier(Glacier에서 복원)를 선택합니다. 객체의 복원 상태 점검에 관한 내용은 아카이브 복원 상태 및 만료 날짜 확인 (p. 50) 단원을 참조하십시오.



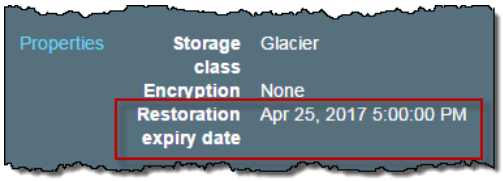
2. 업그레이드할 티어를 선택한 후 복원을 선택합니다. 더 빠른 복원 티어로 업그레이드하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 아카이브된 객체 복원을 참조하십시오.

아카이브 복원 상태 및 만료 날짜 확인

복원 진행 상황을 점검하려면 객체 개요 패널을 참조하십시오. 개요 패널에 대한 자세한 내용은 객체의 개요를 보려면? (p. 53) 단원을 참조하십시오.

개요 섹션에 복원이 진행 중이라고 표시됩니다.

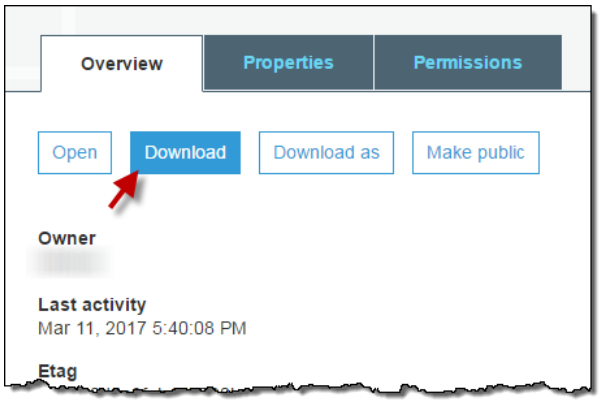
객체의 임시 복사본을 사용할 수 있는 경우, 해당 객체의 개요 섹션에 복원 만료 날짜가 표시됩니다. 이때 Amazon S3는 아카이브 항목의 복원된 복사본을 제거합니다.



복원된 객체는 지정된 일수 동안만 저장됩니다. 객체의 영구 복사본이 필요한 경우, Amazon S3 버킷에 객체의 복사본을 만드십시오.

Amazon S3에서는 사용자가 지정한 일수를 사용자가 요청한 객체 복원 시간에 더한 다음 익일 자정(UTC)으로 반올림하여 만료 날짜를 계산합니다. 이 계산법은 객체를 처음 복원할 때는 물론 사용자 요청에 따라 가용성을 확장할 때도 적용됩니다. 예를 들어, 객체가 2012년 10월 15일 오전 10시 30분(UTC)에 복원되었고 사용자가 일수를 3으로 지정한 경우, 2012년 10월 19일 00:00(UTC)까지 해당 객체를 사용할 수 있습니다. 한편 2012년 10월 16일 오전 11시(UTC)에 객체에 대한 액세스 가능 일수를 1로 변경하는 경우, Amazon S3는 복원된 객체를 2012년 10월 18일 00:00(UTC)까지 사용할 수 있도록 합니다.

객체를 복원한 뒤 개요 페이지에서 다운로드할 수 있습니다. 자세한 내용은 객체의 개요를 보려면? (p. 53) 단원을 참조하십시오.



추가 정보

- S3 버킷에 대한 수명 주기 정책을 생성하려면 어떻게 해야 합니까? (p. 76)
- S3 객체를 삭제 취소하려면? (p. 45)

Amazon S3 객체를 어떻게 잠급니까?

Amazon S3 객체 잠금을 사용하면 Amazon S3에서 write-once-read-many(WORM) 모델을 사용하여 객체를 저장할 수 있습니다. Amazon S3 객체 잠금을 사용하면 고정된 시간 동안 또는 무기한으로 객체를 삭제하거나 덮어쓰지 않도록 할 수 있습니다. AWS CLI, AWS SDK, Amazon S3 REST API를 이용한 객체 잠금에 대한 정보는 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 객체 잠금을 사용하는 객체 잠금을 참조하십시오.

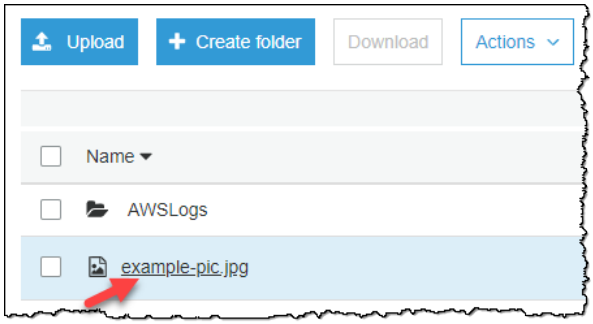
객체를 잠그기 전에 버킷이 Amazon S3 객체 잠금을 사용하도록 활성화해야 합니다. 버킷을 생성할 때 객체 잠금을 활성화합니다. 버킷에서 Amazon S3 객체 잠금을 활성화하면 해당 버킷의 객체를 잠글 수 있습니다. 객체 잠금이 활성화된 버킷을 생성하면 객체 잠금을 비활성화하거나 버킷의 버전 관리를 일시 중지할 수 없습니다.

Amazon S3 객체 잠금을 활성화하여 버킷을 생성하는 방법에 대한 정보는 S3 버킷을 생성하려면 어떻게 해야 합니까? (p. 3) 단원을 참조하십시오.

Amazon S3 객체를 잠그려면

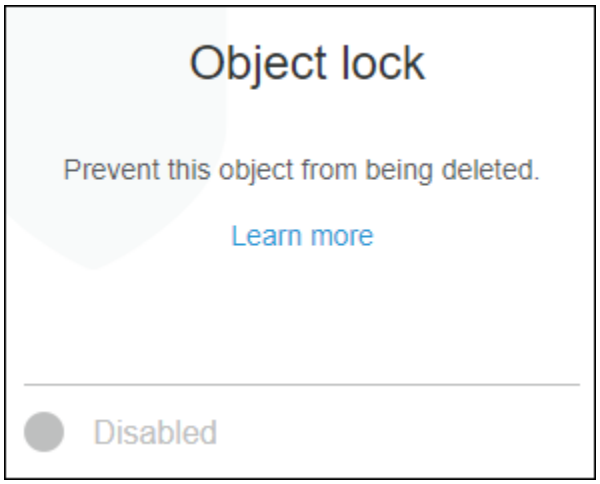
1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 원하는 버킷의 이름을 선택합니다.

3. 이름 목록에서 잠그려는 객체의 이름을 선택합니다.

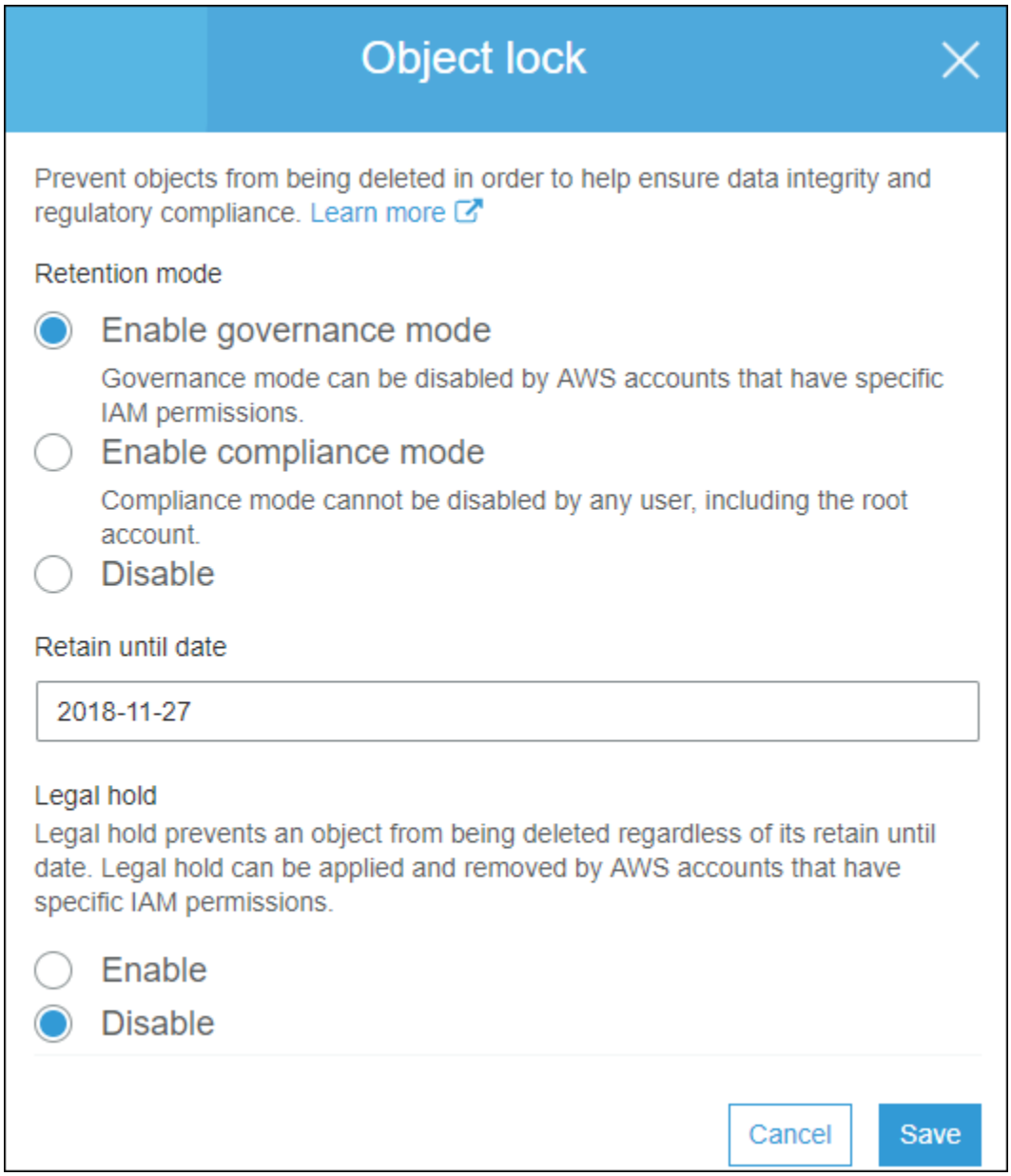


4. [Properties]를 선택합니다.

5. Object Lock(객체 잠금)을 선택합니다.



6. 보존 모드를 선택하십시오. Retain until date(보관 종료일)를 변경할 수 있습니다. 또한 법적 보존을 활성화하도록 선택할 수도 있습니다. 자세한 정보는 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 객체 잠금 개요를 참조하십시오.



7. Save를 선택합니다.

추가 정보

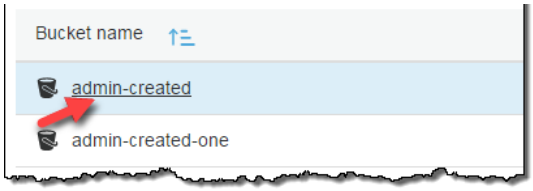
- 버킷 및 객체 액세스 권한 설정 (p. 110)

객체의 개요를 보려면?

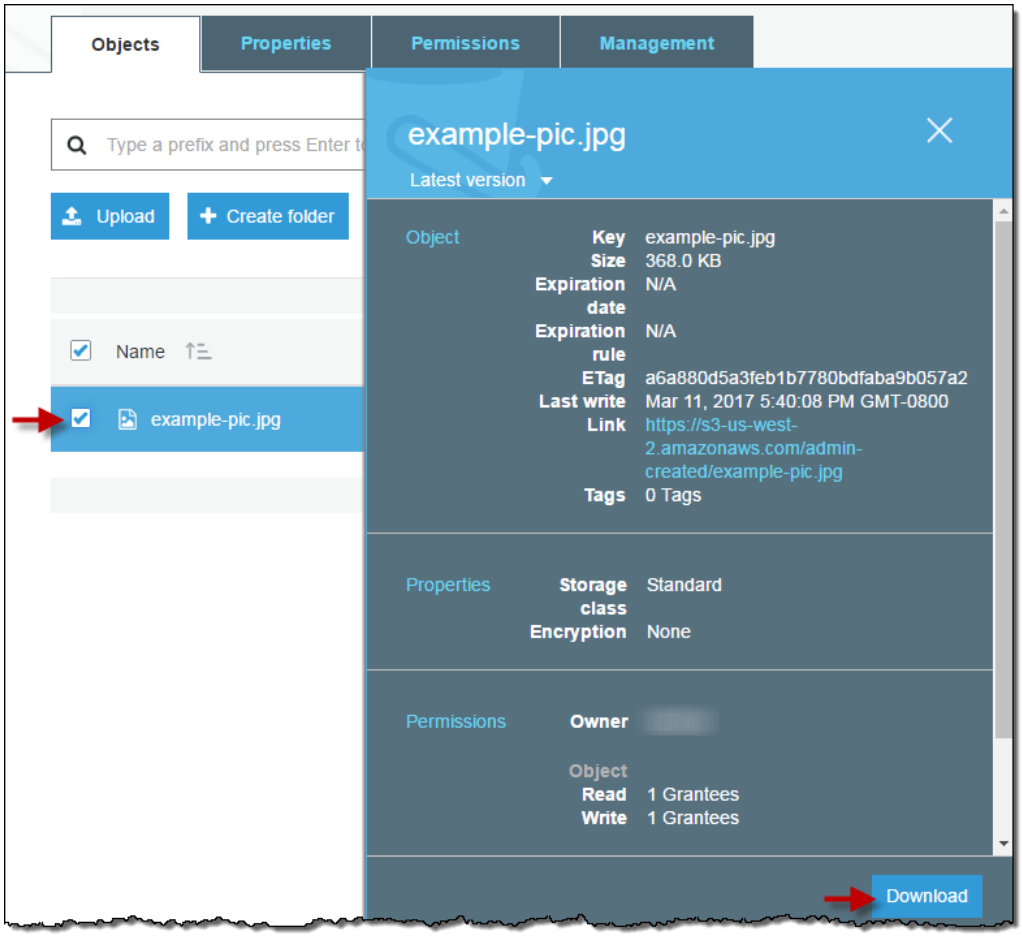
이 단원에서는 Amazon S3 콘솔을 사용하여 객체 개요 패널을 보는 방법을 설명합니다. 이 패널에는 객체에 대한 모든 기본 정보가 개괄적으로 한 곳에 표시됩니다.

객체의 개요 패널을 보는 방법

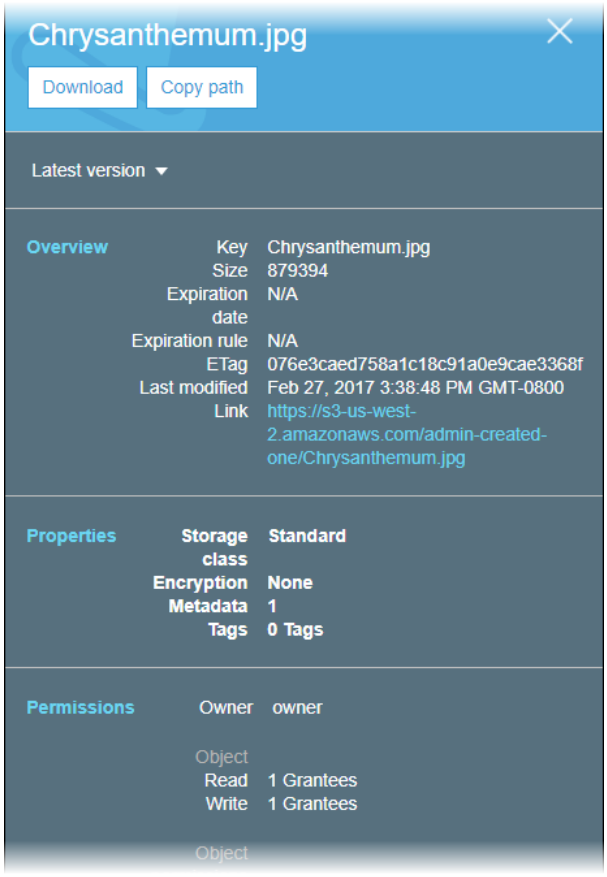
1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 객체가 포함된 버킷의 이름을 선택합니다.



3. 이름 목록에서 개요를 보려는 객체의 이름 옆에 있는 확인란을 선택합니다.



4. 객체를 다운로드하려면 객체 개요 패널에서 다운로드를 선택합니다. 객체의 경로를 클립보드에 복사하려면 경로 복사를 선택합니다.



5. 버킷에 버전 관리 기능이 활성화되어 있을 경우, Latest versions(최신 버전)를 선택하면 객체의 버전이 목록으로 나열됩니다. 그런 다음 다운로드 아이콘을 선택하여 객체 버전을 다운로드하거나, 휴지통 아이콘을 선택하여 객체 버전을 삭제할 수 있습니다.

Important

객체는 최신 버전으로 삭제한 경우에만 삭제를 취소할 수 있습니다. 삭제했던 객체의 이전 버전은 삭제를 취소할 수 없습니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 객체 버전 관리 및 버전 관리 사용 단원을 참조하십시오.

추가 정보

- S3 객체의 버전을 보려면? (p. 56)

S3 객체의 버전을 보려면?

이 단원에서는 Amazon S3 콘솔을 사용하여 객체의 다른 버전을 보는 방법을 설명합니다.

버전 관리를 사용하는 버킷에는 동일 객체에 대한 여러 버전, 1개의 최신 버전 및 버전 0 이상의 최신 버전이 아닌 이전 버전이 존재할 수 있습니다. Amazon S3는 각 객체에 고유한 버전 ID를 할당합니다. 버전 관리 사용에 대한 자세한 내용은 S3 버킷의 버전 관리 기능을 활성화하거나 해제하려면? (p. 7) 단원을 참조하십시오.

버킷에 버전 관리 기능이 활성화된 경우 Amazon S3는 다음과 같은 조건으로 객체에 대해 다른 버전을 생성합니다.

- 버킷에 이미 있는 객체와 이름이 동일한 객체를 업로드하면 Amazon S3는 기존 객체를 대체하는 대신 객체의 다른 버전을 만듭니다.
- 객체를 버킷에 업로드한 후에 스토리지 세부 정보나 기타 메타데이터를 변경하는 등 객체 속성을 업데이트하면 Amazon S3는 버킷에 새로운 객체 버전을 만듭니다.

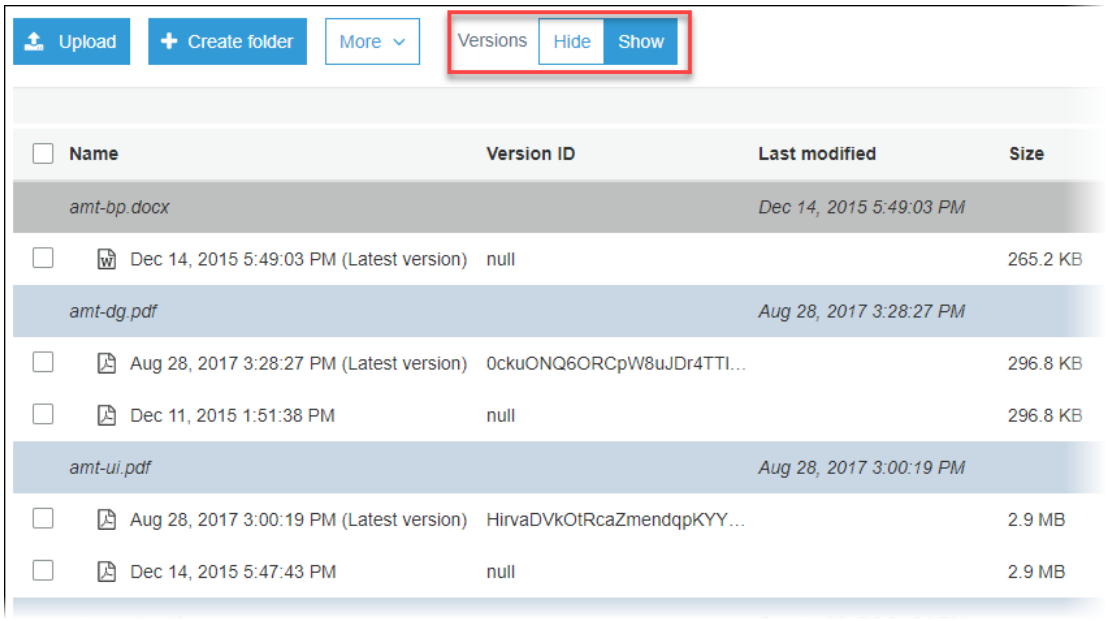
Amazon S3에서 버전 관리 지원에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 객체 버전 관리 및 버전 관리 사용 단원을 참조하십시오.

객체의 여러 버전을 보려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 객체가 포함된 버킷의 이름을 선택합니다.

3. 버킷의 객체 버전 목록을 확인하려면 표시를 선택합니다. 각 객체 버전에 대해 콘솔에 고유한 버전 ID, 객체 버전이 생성된 날짜/시간 및 기타 속성이 표시됩니다. (버전 관리 상태로 설정하기 전에 버킷에 저장된 객체의 버전 ID는 null이 됩니다.)

   해당 버전이 없는 객체 목록을 보려면 숨기기를 선택합니다.



또한 객체 개요 패널에서 객체 버전의 보기, 다운로드 및 삭제도 가능합니다. 자세한 내용은 객체의 개요를 보려면? (p. 53) 단원을 참조하십시오.

Important

객체는 최신 버전으로 삭제한 경우에만 삭제를 취소할 수 있습니다. 삭제했던 객체의 이전 버전은 삭제를 취소할 수 없습니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 객체 버전 관리 및 버전 관리 사용 단원을 참조하십시오.

추가 정보

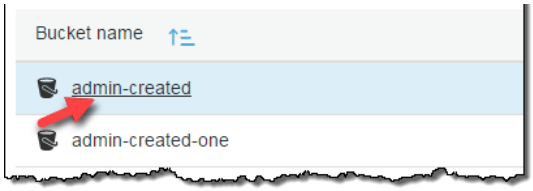
- S3 버킷의 버전 관리 기능을 활성화하거나 해제하려면? (p. 7)
- S3 버킷에 대한 수명 주기 정책을 생성하려면 어떻게 해야 합니까? (p. 76)

객체의 속성을 보려면?

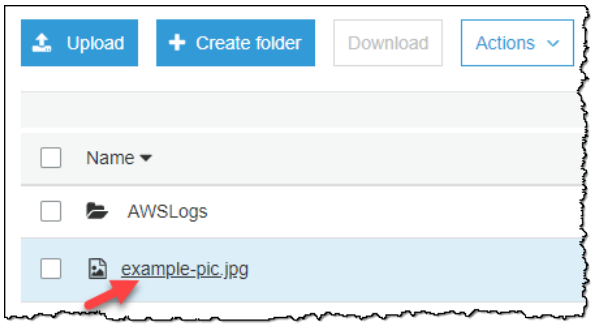
이 단원에서는 콘솔을 사용하여 객체의 속성을 보는 방법을 설명합니다.

객체의 속성을 보려면

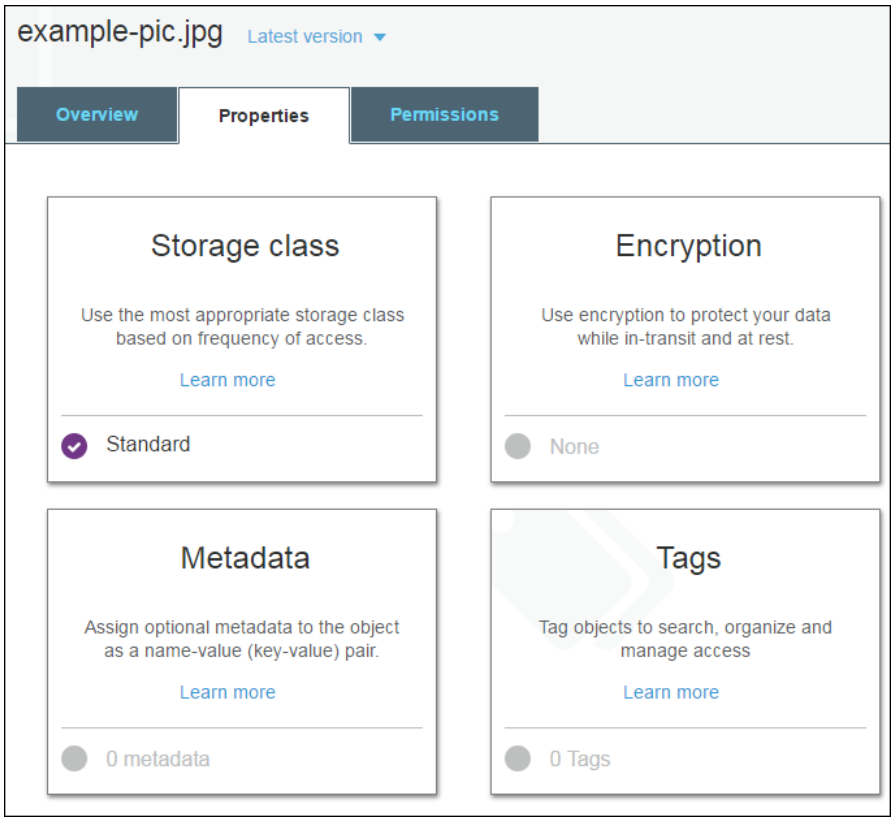
1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 객체가 포함된 버킷의 이름을 선택합니다.



3. 이름 목록에서 속성을 보려는 객체의 이름을 선택합니다.



4. [Properties]를 선택합니다.



5. 속성 페이지에서 다음과 같은 객체 속성을 구성할 수 있습니다.

   a. 스토리지 클래스 – Amazon S3의 각 객체에는 연결된 스토리지 클래스가 있습니다. 해당 객체에 액세스하는 빈도에 따라 사용할 스토리지 클래스를 선택합니다. S3 객체의 기본 스토리지 클래스는 표준입니다. 객체를 업로드할 때 사용할 스토리지 클래스를 선택하면 됩니다. 스토리지 클래스에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 스토리지 클래스 단원을 참조하십시오.

      객체를 업로드한 뒤에 스토리지 클래스를 변경하려면 스토리지 클래스를 선택합니다. 원하는 스토리지 클래스를 선택한 다음 저장을 선택합니다.

   b. 암호화 – S3 객체를 암호화할 수 있습니다. 자세한 내용은 S3 객체에 암호화를 추가하려면 어떻게 해야 합니까? (p. 59) 단원을 참조하십시오.

   c. 메타데이터 – Amazon S3의 각 객체에는 해당 메타데이터를 나타내는 이름-값 페어 세트가 있습니다. S3 객체에 메타데이터를 추가하는 방법에 대한 자세한 내용은 S3 객체에 메타데이터를 추가하려면 어떻게 해야 합니까? (p. 61) 단원을 참조하십시오.

d. 태그 - S3 객체에 태그를 추가할 수 있습니다. 자세한 내용은 S3 객체에 태그를 추가하려면 어떻게 해야 합니까? (p. 66) 단원을 참조하십시오.

S3 객체에 암호화를 추가하려면 어떻게 해야 합니까?

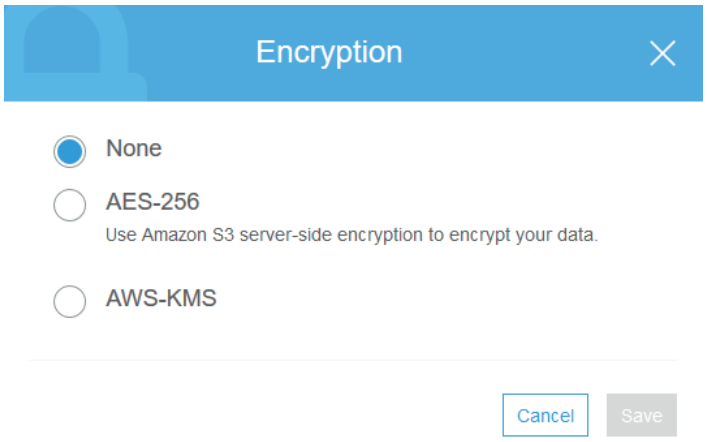
이 주제에서는 객체에서 사용 중인 암호화의 유형을 설정하거나 변경하는 방법을 설명합니다.

객체에 대한 암호화를 추가하거나 변경하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 객체가 포함된 버킷의 이름을 선택합니다.
3. 이름 목록에서 암호화를 추가하거나 변경할 객체의 이름을 선택합니다.
4. 속성를 선택한 다음, Encryption을 선택합니다.

   객체 암호화에 대한 세 가지 선택 사항을 제공하는 암호화 대화 상자가 열립니다.

   - 없음 - 객체 암호화가 없습니다.
   - AES-256 - Amazon S3 관리형 키를 사용한 서버 측 암호화(SSE-S3)입니다.
   - AWS-KMS - AWS Key Management Service(AWS KMS) 고객 마스터 키를 사용한 서버 측 암호화(SSE-KMS)입니다.
5. 이미 암호화 설정이 있는 객체에서 암호화를 제거하려면 없음과 저장을 선택합니다.

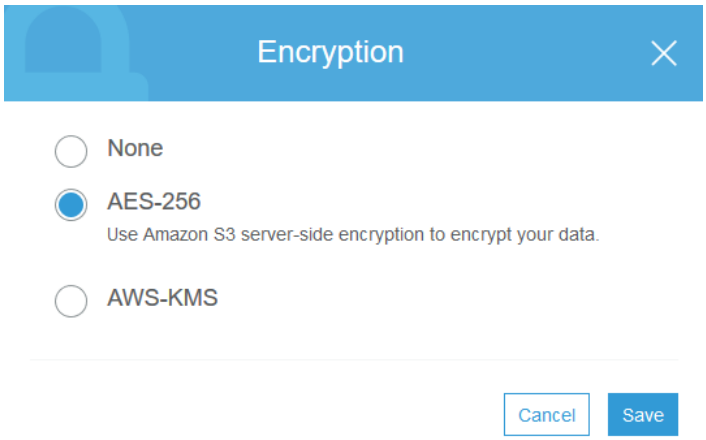


6. Amazon S3에서 관리하는 키를 사용하여 객체를 암호화하려면 다음 단계를 따르십시오.

   a. AES-256을 선택합니다.

      Amazon S3 서버 측 암호화를 사용하여 데이터를 암호화하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 관리형 암호화 키 클래스로 데이터 보호 단원을 참조하십시오.

   b. 저장을 선택합니다.



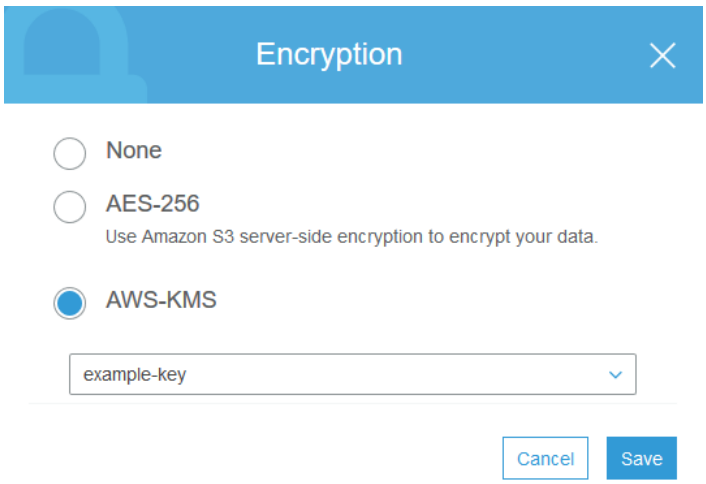
7. AWS KMS를 사용하여 객체를 암호화하려면 다음 단계를 따르십시오.

   a. AWS-KMS를 선택합니다.

   b. AWS KMS CMK를 선택합니다.

      이 목록에는 사용자가 생성한 고객 관리형 CMK와 Amazon S3에 대한 AWS 관리형 CMK가 표시됩니다. 고객 관리형 AWS KMS CMK 생성에 대한 자세한 내용은 AWS Key Management Service Developer Guide의 키 생성을 참조하십시오.

   c. 저장을 선택합니다.



   Important

   버킷의 객체를 암호화하려면 버킷과 동일한 AWS 리전에서 활성화된 CMK만 사용할 수 있습니다. Amazon S3는 대칭 CMK만 지원합니다. Amazon S3는 비대칭 CMK를 지원하지 않습니다. 자세한 내용은 대칭 및 비대칭 키 사용을 참조하십시오.

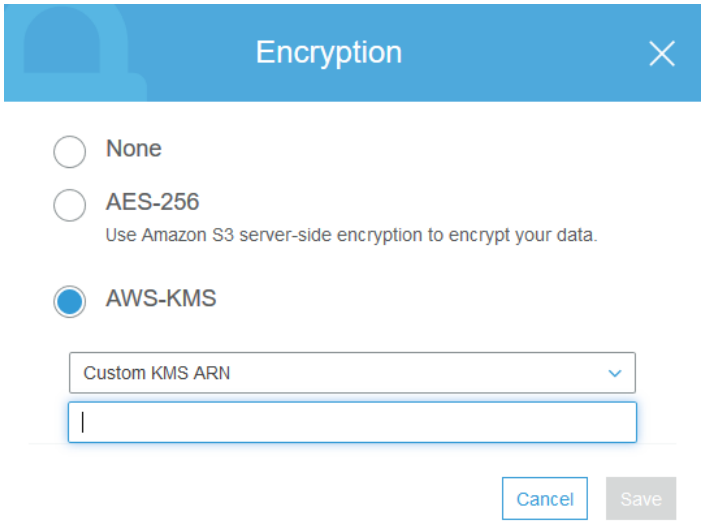
8. AWS KMS CMK로 보호되는 객체를 사용할 수 있는 기능을 외부 계정에 부여하려면 다음 단계를 따르십시오.

   a. AWS-KMS를 선택합니다.

   b. 외부 계정의 Amazon 리소스 이름(ARN)을 입력합니다.

   c. 저장을 선택합니다.

AWS KMS CMK로 보호되는 객체에 대한 사용 권한이 있는 외부 계정의 관리자는 리소스 레벨의 AWS Identity and Access Management(IAM) 정책을 생성하여 액세스를 더 제한할 수 있습니다.



추가 정보

- Amazon S3 버킷의 기본 암호화를 활성화하려면 어떻게 해야 합니까? (p. 8)
- Amazon Simple Storage Service 개발자 가이드의 S3 버킷에 대한 Amazon S3 기본 암호화
- 객체의 속성을 보려면? (p. 57)
- 객체 업로드, 다운로드 및 관리 (p. 34)

S3 객체에 메타데이터를 추가하려면 어떻게 해야 합니까?

Amazon Simple Storage Service(Amazon S3)의 각 객체에는 해당 객체에 대한 메타데이터를 담은 이름-값 페어 세트가 있습니다. 메타데이터란 해당 객체에 대한 추가 정보입니다. `Date`, `Content-Length` 등 사용자가 객체를 업로드할 때 Amazon S3에서 설정하는 메타데이터도 있습니다. 객체를 업로드할 때 메타데이터를 설정할 수도 있고, 나중에 추가할 수도 있습니다. 이 단원에서는 Amazon S3 콘솔을 사용하여 S3 객체에 메타데이터를 추가하는 방법을 설명합니다.

객체 메타데이터는 이름-값(키-값) 페어의 집합입니다. 예를 들어, 콘텐츠 길이에 대한 메타데이터인 `Content-Length`는 이름(키)과 바이트 단위의 객체 크기(값)로 구성됩니다. 객체 메타데이터에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 객체 메타데이터 단원을 참조하십시오.

S3 객체에는 Amazon S3 시스템 메타데이터 및 사용자 정의 메타데이터라는 두 종류의 메타데이터가 있습니다.

- 시스템 메타데이터–시스템 메타데이터는 두 범주로 나뉩니다. `Last-Modified` 날짜와 같은 메타데이터는 시스템에서 제어하며, Amazon S3만 값을 수정할 수 있습니다. 한편 해당 객체에 대해 구성된 스토리지 클래스 등 사용자가 제어하는 시스템 메타데이터도 있습니다.
- 사용자 정의 메타데이터–사용자가 직접 자신의 메타데이터를 정의한 것을 사용자 정의 메타데이터라고 합니다. 객체를 업로드할 때 또는 객체를 업로드한 이후에 객체에 사용자 정의 메타데이터를 할당할 수

있습니다. 사용자 정의 메타데이터는 객체와 함께 저장되었다가 해당 객체를 다운로드할 때 반환됩니다. Amazon S3는 사용자 정의 메타데이터를 처리하지 않습니다.

다음 주제에서는 객체에 메타데이터를 추가하는 방법에 대해 설명합니다.

주제

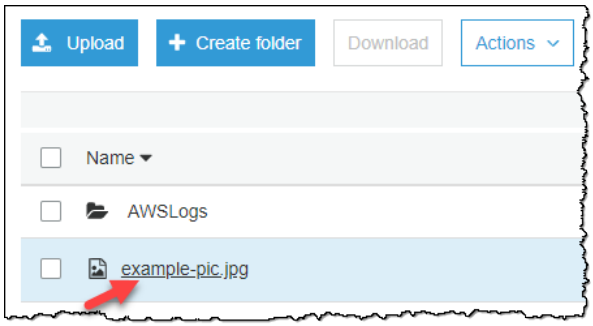
S3 객체에 시스템 정의 메타데이터 추가

S3 객체에 대해 몇 가지 시스템 메타데이터를 구성할 수 있습니다. 시스템 정의 메타데이터 목록과 값 수정 가능 여부를 확인하려면 Amazon Simple Storage Service 개발자 가이드의 시스템 정의 메타데이터 단원을 참조하십시오.

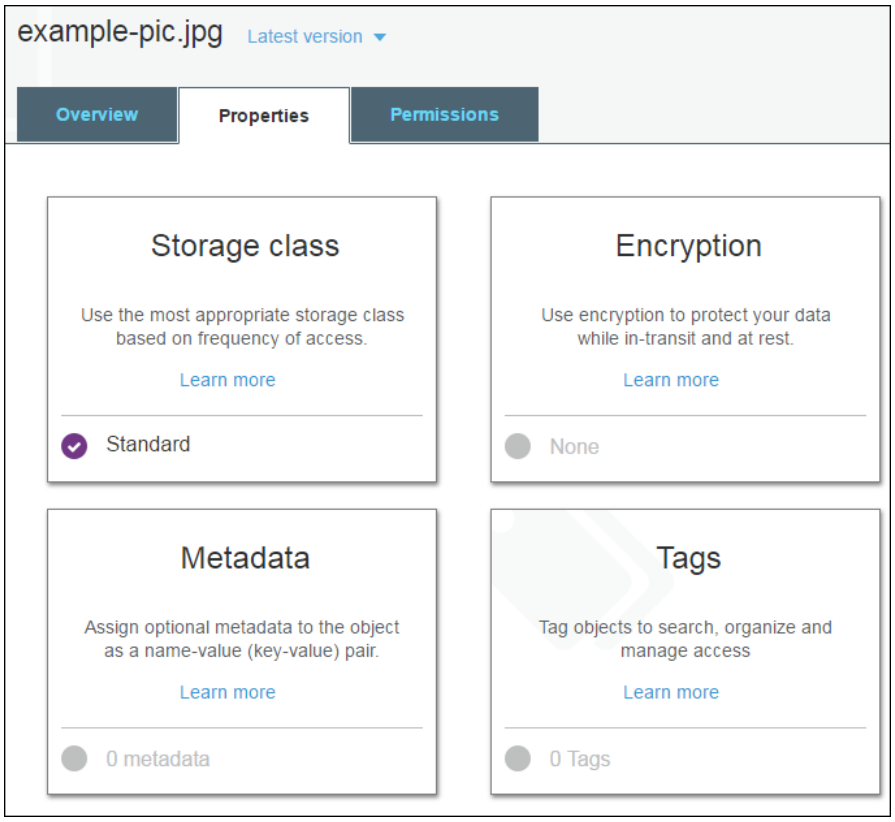
객체에 시스템 메타데이터를 추가하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 객체가 포함된 버킷의 이름을 선택합니다.

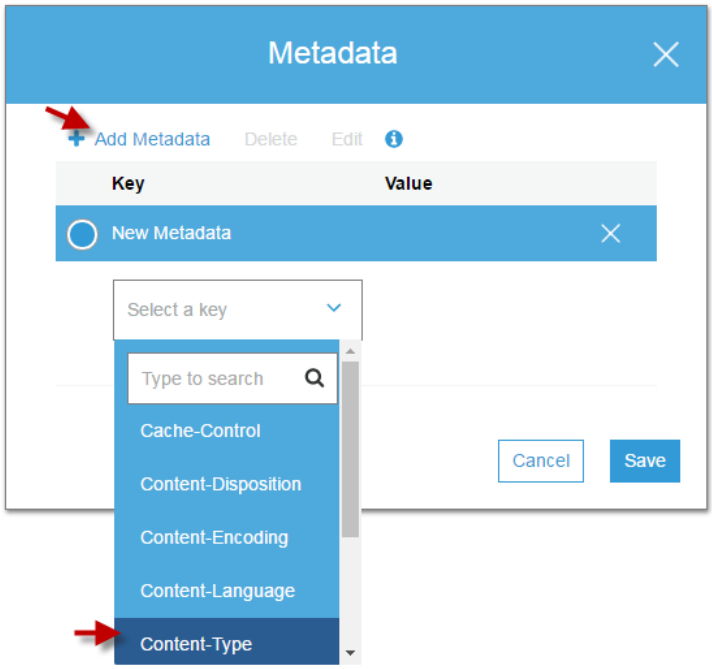
3. 이름 목록에서 메타데이터를 추가하려는 객체의 이름을 선택합니다.



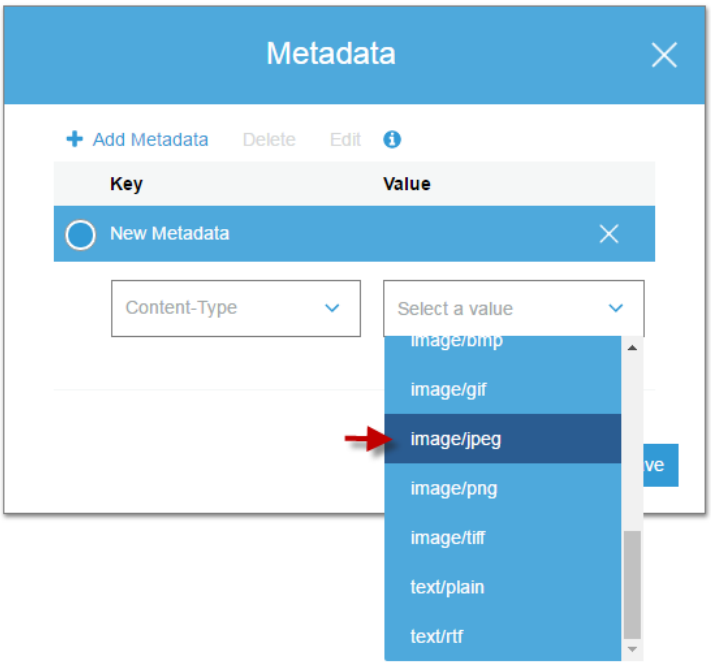
4. 속성를 선택한 다음, 메타데이터를 선택합니다.



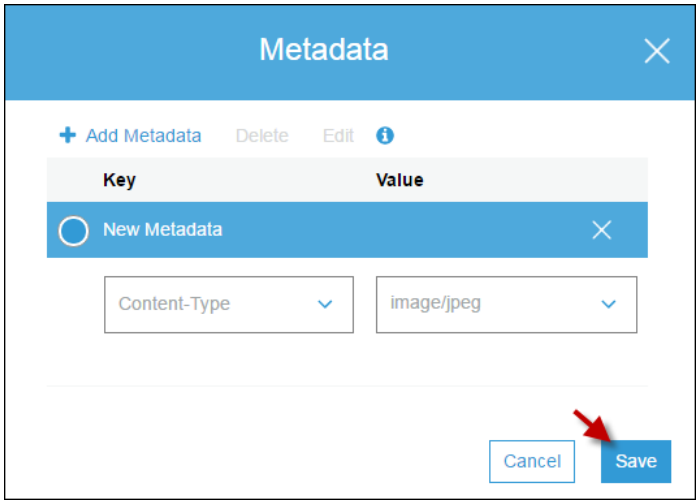
5. 메타데이터 추가를 선택한 다음 키 선택 메뉴에서 키를 선택합니다.



6. 선택한 키에 따라 값 선택 메뉴에서 값을 선택하거나 값을 직접 입력합니다.



7. Save를 선택합니다.



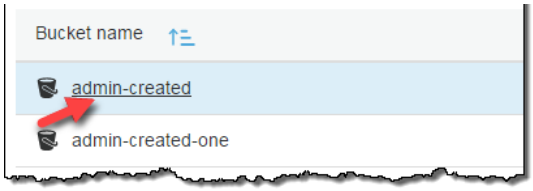
S3 객체에 사용자 정의 메타데이터 추가

객체에 사용자 정의 메타데이터를 추가할 수 있습니다. 사용자 정의 메타데이터는 접두사 "`x-amz-meta-`"로 시작해야 하며, 그렇지 않으면 Amazon S3에서 키 값 페어를 사용자가 정의한 대로 설정하지 않습니다. 사용자는 선택한 이름을 `x-amz-meta-` 키에 추가하여 메타데이터를 사용자 정의할 수 있습니다. 이렇게 해서 사용자 정의 키가 생성됩니다. 예를 들어, `alt-name`을 사용자 이름으로 추가하면 메타데이터 키는 `x-amz-meta-alt-name`이 됩니다.

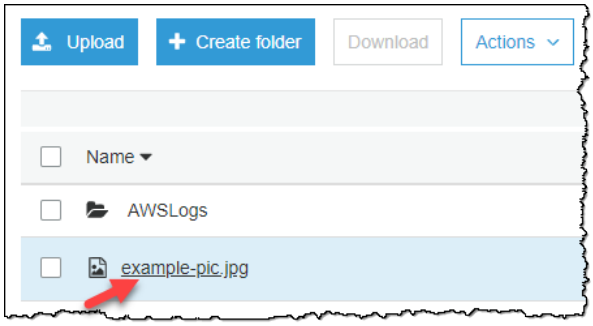
사용자 정의 메타데이터의 최대 크기는 2KB입니다. 키와 값 모두 US-ASCII 표준에 부합해야 합니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 사용자 정의 메타데이터 단원을 참조하십시오.

객체에 사용자 정의 메타데이터를 추가하려면

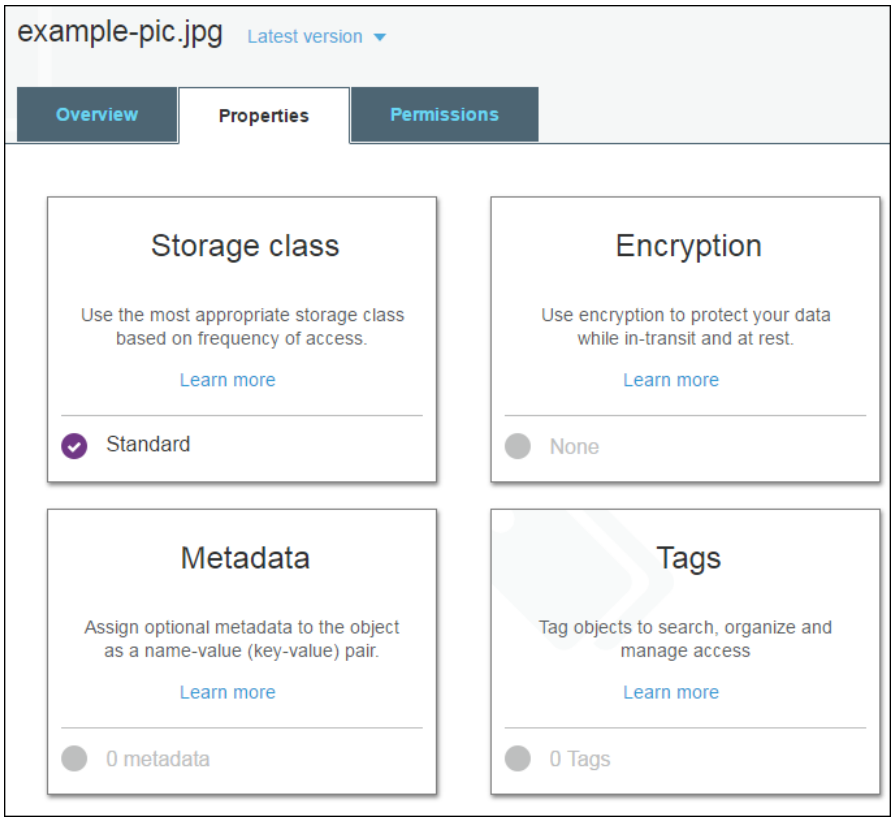
1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 객체가 포함된 버킷의 이름을 선택합니다.



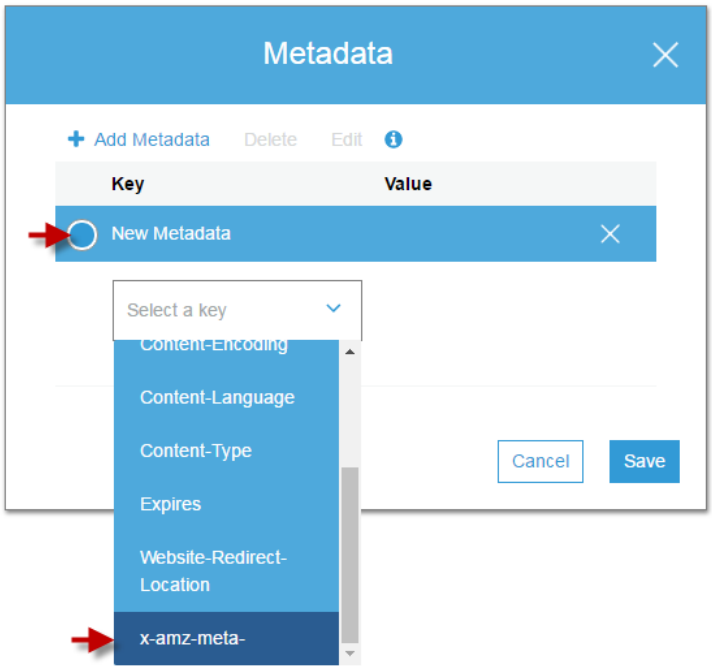
3. 이름 목록에서 메타데이터를 추가하려는 객체의 이름을 선택합니다.



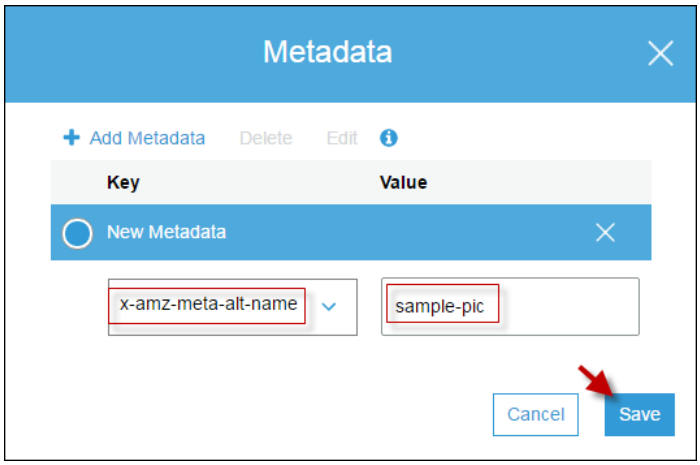
4. 속성를 선택한 다음, 메타데이터를 선택합니다.



5. 메타데이터 추가를 선택한 다음 Select a key(키 선택) 메뉴에서 `x-amz-meta-` 키를 선택합니다. 접두사 `x-amz-meta-`로 시작하는 모든 메타데이터는 사용자 정의 메타데이터입니다.



6. `x-amz-meta-` 키 뒤에 사용자 정의 이름을 입력합니다. 예를 들어, 사용자 이름이 `alt-name`이면 메타데이터 키는 `x-amz-meta-alt-name`이 됩니다. 사용자 정의 키의 값을 입력한 다음 저장을 선택합니다.



- 객체의 속성을 보려면? (p. 57)
- 객체 업로드, 다운로드 및 관리 (p. 34)

S3 객체에 태그를 추가하려면 어떻게 해야 합니까?

객체 태그 지정을 통해 스토리지를 분류할 수 있습니다. 이 주제에서는 S3 객체를 업로드한 후에 콘솔을 사용하여 그 객체에 태그를 추가하는 방법을 설명합니다. 객체가 업로드될 때 객체에 태그를 추가하는 것에 대한 내용은 S3 버킷에 파일 및 폴더를 업로드하려면 어떻게 해야 합니까? (p. 34) 단원을 참조하십시오.

모든 태그는 다음 규칙이 적용되는 키-값 페어입니다.

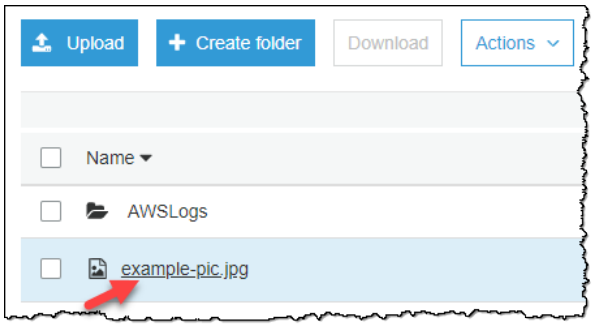
- 한 개체에 태그를 최대 10개까지 연결할 수 있습니다. 각 객체에 연결된 태그에는 고유한 태그 키가 있어야 합니다.
- 태그 키는 최대 128개 유니코드 문자이며, 태그 값은 최대 255개 유니코드 문자입니다.
- 키와 태그 값은 대/소문자를 구분합니다.

객체 태그에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 객체 태그 지정 단원을 참조하십시오.

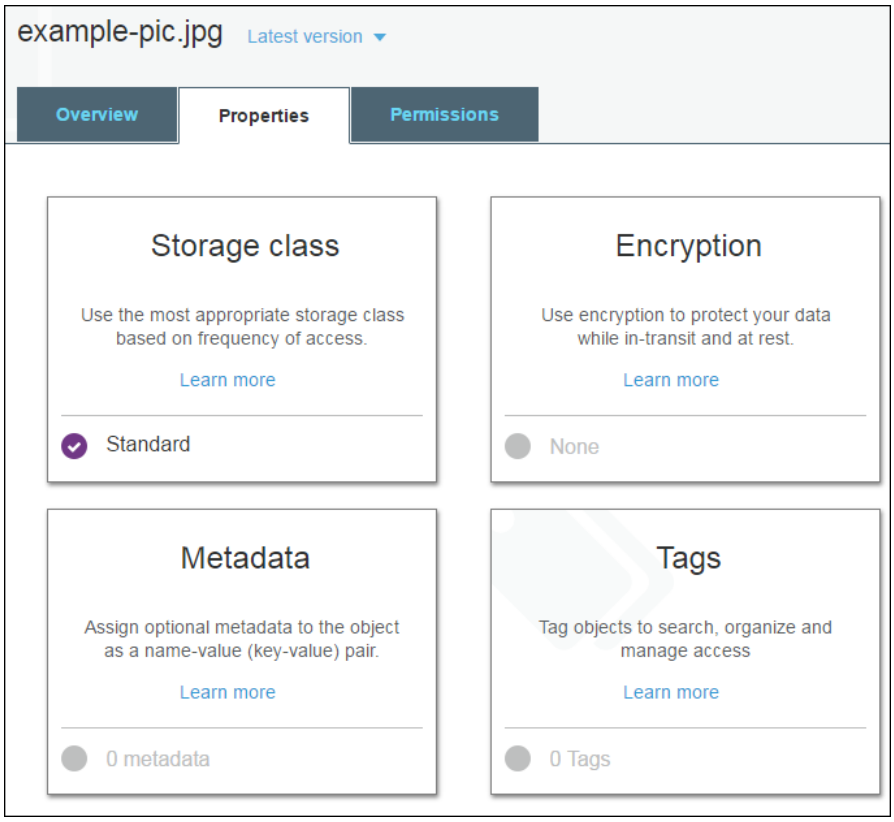
객체에 태그 추가

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 객체가 포함된 버킷의 이름을 선택합니다.

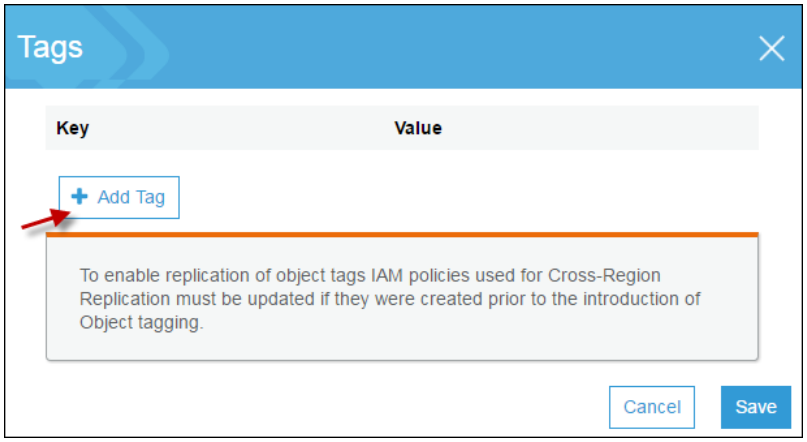
3. 이름 목록에서 태그를 추가하려는 객체의 이름을 선택합니다.



4. [Properties]를 선택합니다.

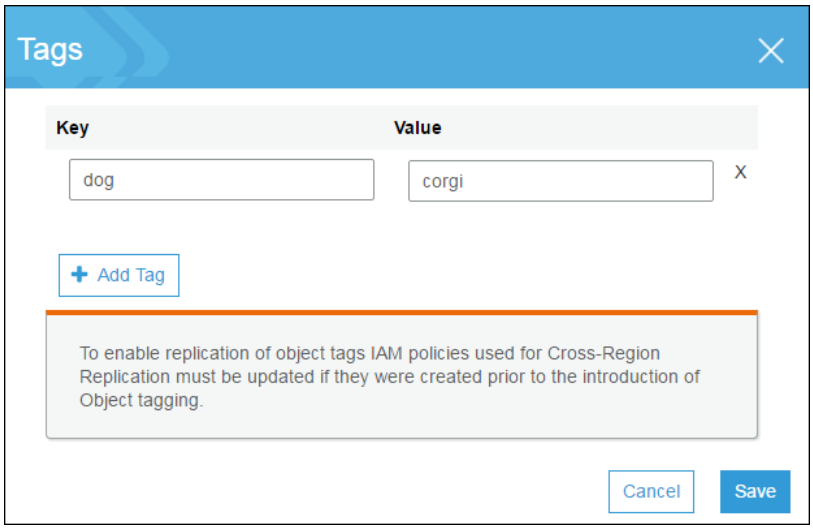


5. 태그를 선택한 후 태그 추가를 선택합니다.



6. 각 태그는 키-값 페어입니다. 키와 값을 입력합니다. 그런 다음 태그 추가를 선택해 다른 태그를 추가하거나 저장을 선택합니다.

   한 개체에 태그를 최대 10개까지 입력할 수 있습니다.



추가 정보

- 객체의 속성을 보려면? (p. 57)
- 객체 업로드, 다운로드 및 관리 (p. 34)

S3 버킷에서 폴더를 어떻게 사용합니까?

Amazon S3에서 버킷과 객체는 기본 리소스이며 객체가 버킷에 저장됩니다. Amazon S3는 파일 시스템에서와 같이 계층 대신 단순한 구조를 가지고 있습니다. 하지만 간결한 구성을 위해 Amazon S3 콘솔에서는 객체를 그룹화하는 수단으로 폴더 개념을 지원합니다. Amazon S3;에서 이 작업을 하려면 객체(즉 이름이 공통 문자열로 시작하는 객체)의 공유 이름 접두사를 사용합니다. 객체 이름을 키 이름이라고도 합니다.

예를 들어 `photos`라는 콘솔에 폴더를 만들고 여기에 `myphoto.jpg`라는 객체를 저장할 수 있습니다. 그러면 객체가 키 이름 `photos/myphoto.jpg`와 함께 저장됩니다. 여기서 `photos/`는 접두사입니다.

아래에 두 가지 예가 더 있습니다.

- 버킷에 3개의 객체(`logs/date1.txt`, `logs/date2.txt` 및 `logs/date3.txt`)가 있다면 콘솔은 `logs`라는 이름의 폴더를 표시합니다. 콘솔에서 폴더를 열면 세 객체 `date1.txt`, `date2.txt` 및 `date3.txt`가 표시됩니다.
- `photos/2017/example.jpg`라는 이름의 객체가 있다면 콘솔은 `photos` 폴더 및 `2017` 객체가 들어 있는 `example.jpg` 라는 이름의 폴더를 표시합니다.

주제

- 폴더 생성 (p. 70)
- S3 버킷에서 폴더는 어떻게 삭제합니까? (p. 71)
- 퍼블릭 폴더 설정 (p. 73)

폴더 안에 폴더를 만들 수 있지만 버킷 안에 버킷을 만들 수는 없습니다. 객체를 폴더로 직접 업로드 또는 복사할 수 있습니다. 폴더를 생성하고 삭제하고 퍼블릭으로 만들 수 있지만 폴더 이름을 바꿀 수는 없습니다. 객체를 다른 폴더로 복사할 수 있습니다.

Important

Amazon S3 콘솔에서는 키 이름의 마지막(후행) 문자가 슬래시("/") 문자인 모든 객체를 폴더(예: `examplekeyname/`)로 취급합니다. 따라서 Amazon S3 콘솔을 사용하여 후행 "/" 문자를 포함하는 키 이름을 가진 객체를 업로드할 수 없습니다. 이름에 후행 "/" 문자가 포함된 객체는 Amazon S3 API에서 AWS CLI, AWS SDK 또는 REST API를 사용하여 객체를 업로드할 수 있습니다.
이름에 후행 "/" 문자가 포함된 객체는 Amazon S3 콘솔에 폴더로 표시됩니다. Amazon S3 콘솔에서는 그런 객체에 대한 콘텐츠 및 메타데이터를 표시하지 않습니다. 콘솔을 사용하여 이름에 후행 "/" 문자가 포함된 객체를 복사할 경우 대상 위치에 새 폴더가 생성되지만 객체의 데이터와 메타데이터는 복사되지 않습니다.

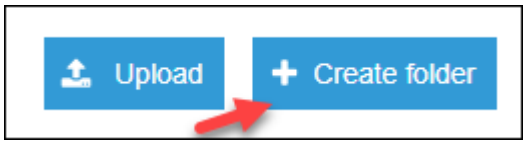
폴더 생성

이 단원에서는 Amazon S3 콘솔을 사용하여 폴더를 만드는 방법을 설명합니다.

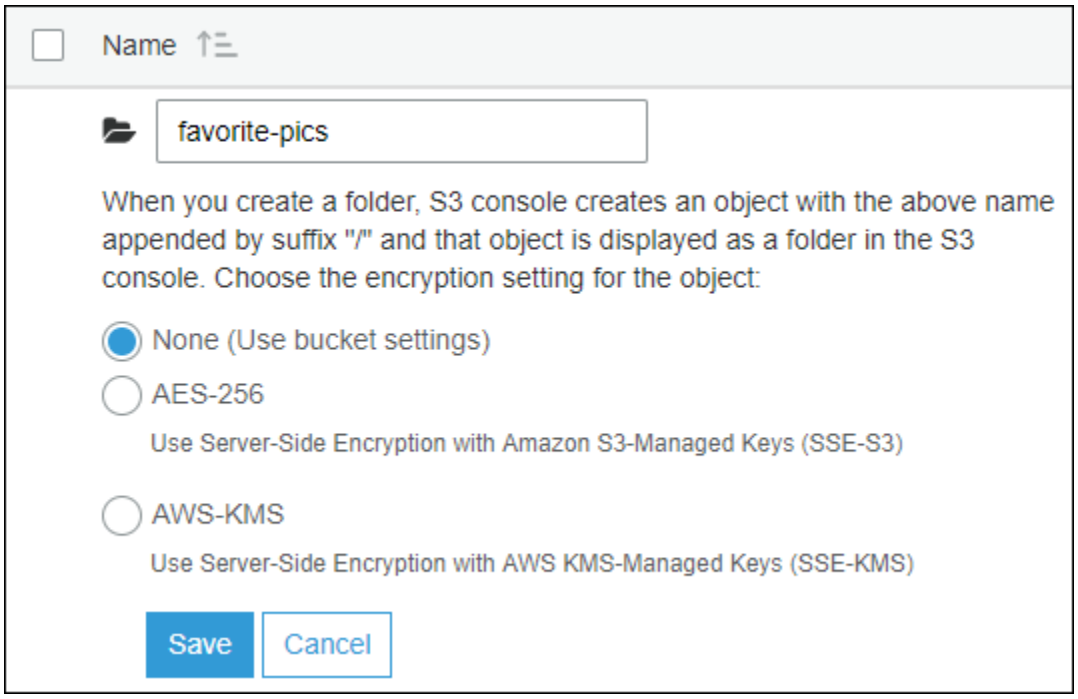
폴더를 만들려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 폴더를 만들 버킷 이름을 선택합니다.

3. [Create folder]를 선택합니다.



4. 폴더의 이름을 입력합니다(예: **`favorite-pics`**). 폴더 객체에서 암호화 설정을 선택하고 저장을 선택합니다.



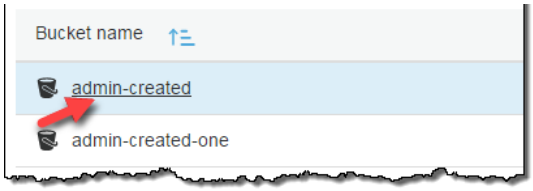
S3 버킷에서 폴더는 어떻게 삭제합니까?

이 단원에서는 Amazon S3 콘솔을 사용하여 S3 버킷에서 폴더를 삭제하는 방법을 설명합니다.

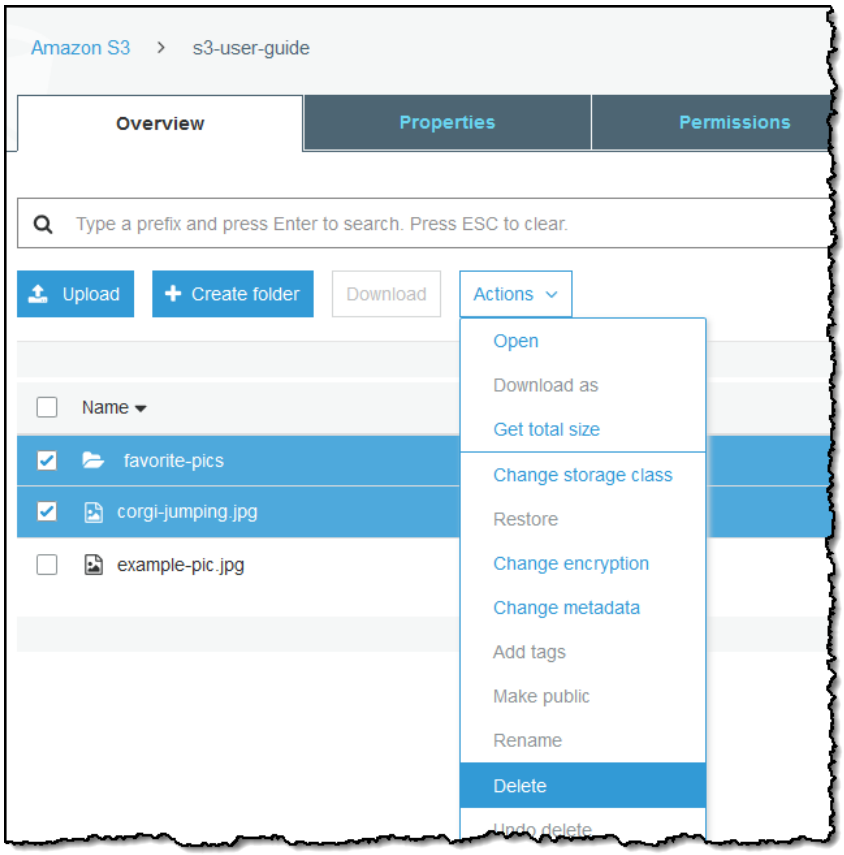
Amazon S3 기능 및 요금에 대한 자세한 내용은 Amazon S3를 참조하십시오.

S3 버킷에서 폴더 삭제 방법

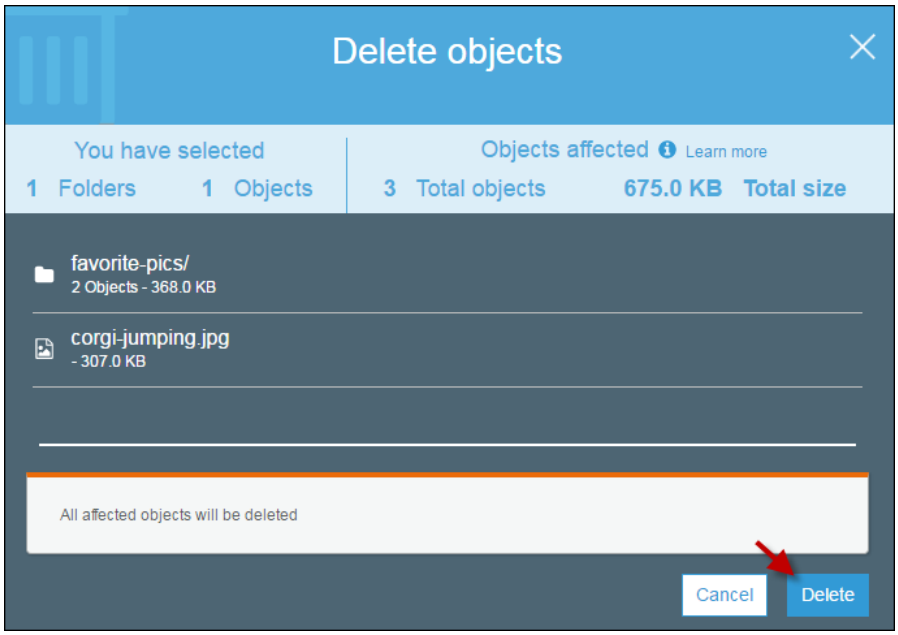
1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 폴더를 삭제하려는 버킷 이름을 선택합니다.



3. 이름 목록에서 삭제하려는 폴더 및 객체 옆에 있는 확인란을 선택하고, 더 보기를 선택한 후 삭제를 선택합니다.



Delete object(객체 삭제) 대화 상자에서 삭제를 선택한 폴더의 이름이 열거되어 있는지 확인한 후 삭제를 선택합니다.



관련 주제

- S3 버킷에서 객체를 삭제하려면? (p. 45)

퍼블릭 폴더 설정

Amazon S3는 일반적인 파일 시스템에서와 같이 계층 대신 단순한 구조를 가지고 있습니다. 하지만 간결한 구성을 위해 Amazon S3 콘솔에서는 객체를 그룹화하는 방법으로 폴더 개념을 지원합니다. Amazon S3에서 폴더는 객체 또는 객체의 그룹에 대한 명명 접두사입니다. 자세한 내용은 S3 버킷에서 폴더를 어떻게 사용합니까? (p. 69) 단원을 참조하십시오.

퍼블릭 폴더 또는 버킷이 특별히 필요하지 않은 경우에는 Amazon S3 폴더 및 버킷에 대한 모든 퍼블릭 액세스를 차단하는 것이 좋습니다. 폴더를 퍼블릭으로 설정하면 인터넷에서 누구나 해당 폴더에 있는 그룹화된 모든 객체를 볼 수 있습니다. Amazon S3 콘솔에서 폴더를 퍼블릭으로 설정할 수 있습니다. 또한 접두사별로 액세스를 제한하는 버킷 정책을 생성하여 폴더를 퍼블릭으로 설정할 수도 있습니다. 자세한 내용은 버킷 및 객체 액세스 권한 설정 (p. 110) 단원을 참조하십시오.

> Warning
>
> Amazon S3 콘솔에서 폴더를 퍼블릭으로 설정한 후에는 다시 프라이빗으로 설정할 수 없습니다. 대신에, 객체에 대한 퍼블릭 액세스가 허용되지 않도록 퍼블릭 폴더에 있는 각 개별 객체에 대한 권한을 설정해야 합니다. 자세한 내용은 객체에 대한 권한은 어떻게 설정하나요? (p. 115) 단원을 참조하십시오.

추가 정보

- S3 버킷에서 폴더는 어떻게 삭제합니까? (p. 71)
- ACL 버킷 권한을 설정하려면 어떻게 해야 합니까? (p. 118)
- S3 버킷에 대한 퍼블릭 액세스를 어떻게 차단합니까? (p. 110)

Amazon S3 배치 작업 소개

Amazon S3 Batch Operations는 Amazon S3 객체에 대해 대규모 배치 작업을 수행합니다. Amazon S3 Batch Operations를 사용하여 객체를 복사하거나, 객체 태그 또는 ACL(액세스 제어 목록)을 설정하거나, Amazon S3 Glacier에서 객체 복원을 시작하거나, 객체를 사용하여 사용자 지정 작업을 수행할 AWS Lambda 함수를 호출할 수 있습니다. 사용자 지정 객체 목록에서 이러한 작업을 수행하거나 Amazon S3 인벤토리 보고서를 사용하여 아주 큰 객체 목록도 쉽게 생성할 수 있습니다. 배치 작업은 이미 사용되는 것과 동일한 Amazon S3 API를 사용하므로 그 인터페이스가 익숙할 것입니다. AWS CLI, AWS SDK 및 Amazon S3 REST API를 사용하여 배치 작업을 수행하는 자세한 내용은 Amazon Simple Storage Service 개발자 가이드에서 배치 작업 수행을 참조하십시오.

다음 주제에서는 Amazon S3 콘솔을 사용하여 배치 작업을 구성 및 실행하는 방법에 대해 설명합니다.

주제

Amazon S3 배치 작업 건 생성

이 단원에서는 Amazon S3 배치 작업을 생성하는 방법을 설명합니다. AWS CLI, AWS SDK 및 Amazon S3 REST API를 사용하여 배치 작업을 수행하는 자세한 내용은 Amazon Simple Storage Service 개발자 가이드에서 배치 작업 수행을 참조하십시오.

배치 작업을 생성하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. Amazon S3 콘솔의 탐색 창에서 Batch Operations(배치 작업)을 선택합니다.
3. [Create job]을 선택합니다.
4. 작업을 생성하려는 리전을 선택합니다.
5. Manifest format(매니페스트 형식) 아래에서 사용할 매니페스트 객체의 형식을 선택합니다.
   - S3 Inventory report(S3 인벤토리 보고서)를 선택하는 경우 Amazon S3이 CSV 형식 인벤토리 보고서의 일부로 생성하는 manifest.json 객체의 경로를 입력하고, 선택적으로 최신 버전이 아닌 버전을 사용하려는 경우 매니페스트 객체의 버전 ID를 지정합니다.
   - CSV를 선택하는 경우 CSV 형식 매니페스트 객체의 경로를 입력합니다. 매니페스트 객체는 콘솔에 설명된 형식을 따라야 합니다. 선택적으로 최신 버전이 아닌 버전을 사용하려는 경우 매니페스트 객체의 버전 ID를 포함시킬 수 있습니다.
6. 작업 아래에서 매니페스트에 나열된 모든 객체에 수행할 작업을 선택합니다. 선택한 작업에 대한 정보를 입력하고 다음을 선택합니다.
7. Configure additional options(추가 옵션 구성)에 대한 정보를 입력하고 다음을 선택합니다.
8. 검토에서 설정을 확인합니다. 설정을 변경하려면 이전을 선택합니다 또는 작업 생성을 선택합니다.

추가 정보

- Amazon Simple Storage Service 개발자 가이드의 기본 사항: Amazon S3 Batch Operations 작업
- Amazon Simple Storage Service 개발자 가이드의 배치 작업 건 생성
- Amazon Simple Storage Service 개발자 가이드의 작업

배치 작업 건 관리

Amazon S3는 배치 작업을 생성한 후 관리하는 데 도움이 되는 도구 집합을 제공합니다. 배치 작업 관리에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드에서 배치 작업 건 관리를 참조하십시오.

추가 정보

- Amazon Simple Storage Service 개발자 가이드의 기본 사항: Amazon S3 Batch Operations 작업
- Amazon Simple Storage Service 개발자 가이드의 배치 작업 건 생성
- Amazon Simple Storage Service 개발자 가이드의 작업

스토리지 관리

이 단원에서는 Amazon S3 스토리지 관리 도구를 구성하는 방법을 설명합니다.

주제

S3 버킷에 대한 수명 주기 정책을 생성하려면 어떻게 해야 합니까?

수명 주기 정책을 사용하여 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의할 수 있습니다(예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).

공유 접두사를 사용하여 버킷의 모든 객체 또는 일부 객체, 즉 공통 문자열로 시작하는 이름을 가진 객체에 대해 수명 주기 정책을 정의할 수 있습니다.

버전 관리를 사용하는 버킷에는 1개의 최신 버전과 버전 0 이상의 비 최신(이전) 버전 등 동일 객체에 대해 여러 버전이 존재할 수 있습니다. 수명 주기 정책을 사용하여 현재 객체 버전과 최신이 아닌 객체 버전 관련 작업을 정의할 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 객체 수명 주기 관리, 객체 버전 관리 및 버전 관리 사용 단원을 참조하십시오.

수명 주기 정책 생성 방법

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 수명 주기 정책을 생성할 버킷의 이름을 선택합니다.

3. 관리 탭을 선택한 후 수명 주기 규칙 추가를 선택합니다.

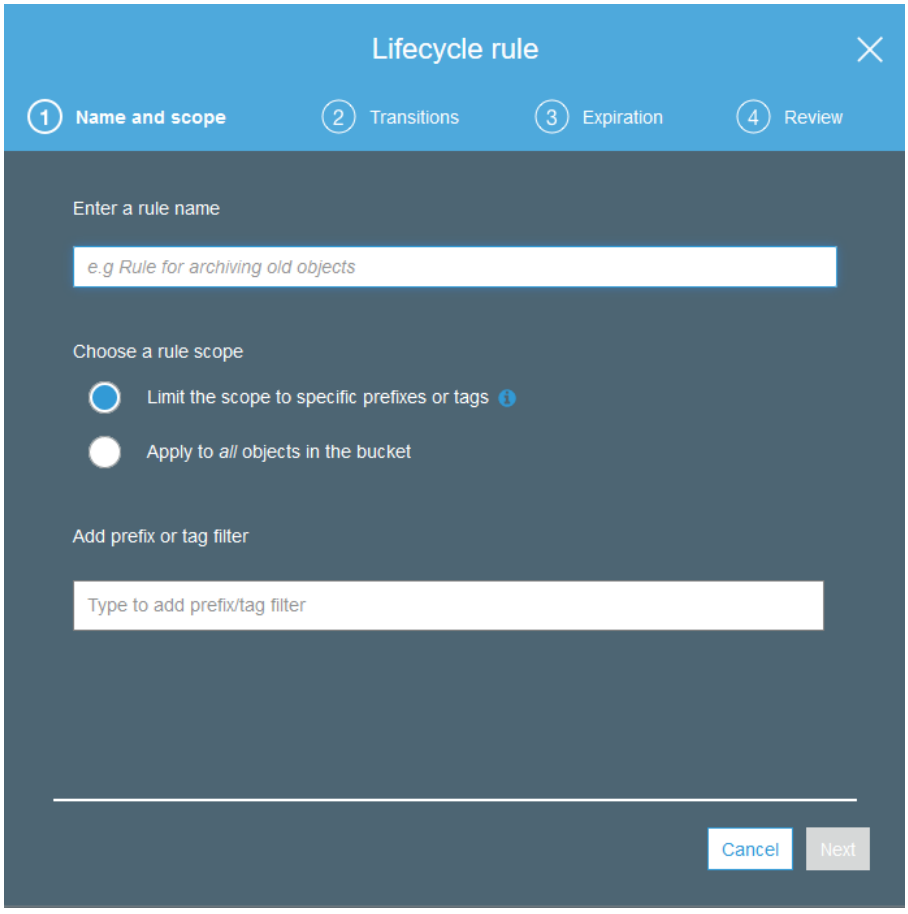
4. 나중에 규칙을 알아보기 쉽도록 수명 주기 규칙 대화 상자에 규칙 이름을 입력하십시오. 단, 버킷 내에서 고유한 이름을 갖도록 합니다. 다음과 같이 규칙을 구성하십시오.

   - 이 수명 주기 규칙을 지정된 이름 접두사(즉, 이름이 공통 문자열로 시작하는 객체)를 지닌 모든 객체에 적용하려면 상자에 접두사를 입력하고 드롭다운 목록에서 접두사를 선택한 다음 Enter(입력)를 누릅니다. 객체 이름 접두사에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 객체 키 단원을 참조하십시오.
   - 이 수명 주기 규칙을 객체 태그가 하나 이상인 모든 객체에 적용하려면 상자에 태그를 입력하고 드롭다운 목록에서 태그를 선택한 다음 Enter(입력)를 누릅니다. 절차를 반복하여 다른 태그를 추가합니다. 접두사와 태그를 결합할 수도 있습니다. 객체 태그에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 객체 태그 지정 단원을 참조하십시오.

     Warning

     접두사 또는 태그를 입력하여 수명 주기 규칙의 범위를 제한하지 않으면 버킷의 모든 객체에 적용됩니다.

   - [Next]를 선택합니다.

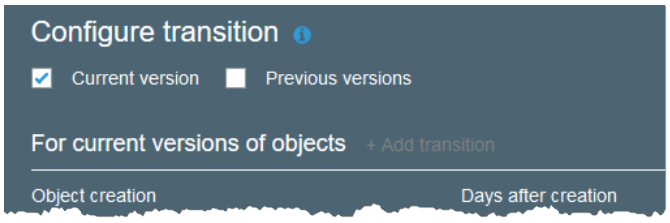


5. 객체를 Standard-IA, One Zone-IA, Glacier 및 Deep Archive 스토리지 클래스로 전환하는 규칙을 정의하여 수명 주기 규칙을 구성할 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 스토리지 클래스를 참조하십시오.

   최신 객체 버전 또는 이전 객체 버전의, 또는 두 버전 모두의 이전을 정의할 수도 있습니다. 버전 관리를 통해 하나의 버킷에서 객체의 여러 버전을 유지할 수 있습니다. 버전 관리에 대한 자세한 내용은 S3 버킷의 버전 관리 기능을 활성화하거나 해제하려면? (p. 7) 단원을 참조하십시오.

a. 현재 버전을 선택해 현재 객체 버전에 적용되는 전환을 정의하십시오.

   이전 버전을 선택해 모든 이전 객체 버전에 적용되는 전환을 정의합니다.

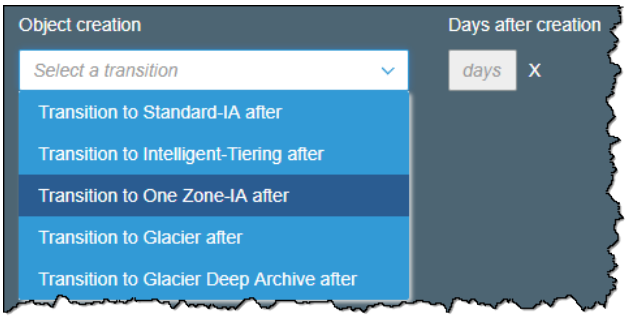


b. Add transitions(이전 추가)를 선택하고 다음 전환 중 하나를 지정합니다.

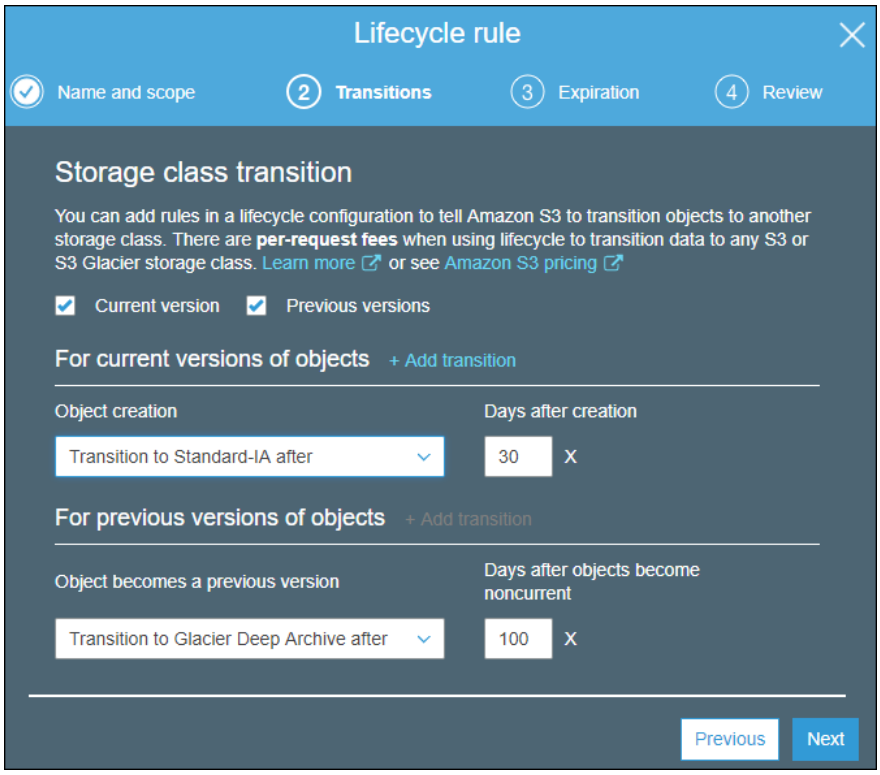
   - 다음 기간 후에 스탠다드-IA로 이전을 선택하고, 객체 생성으로부터 며칠이 지나면 전환을 적용할지 입력합니다(예: 30일).
   - Transition to One Zone-IA after(다음 기간 후에 단일 영역-IA로 이전) 를 선택하고, 객체 생성으로부터 며칠이 지나면 전환을 적용할지 입력합니다(예: 30일).
   - Transition to Glacier after(Glacier 전환 경과 기간)을 선택한 다음 전환 적용 객체 생성 경과 기간(일)(예: 100 일)을 입력합니다.
   - Transition to Glacier Deep Archive after(Glacier Deep Archive 전환 경과 기간)을 선택한 다음 전환 적용 객체 생성 경과 기간(일)(예: 100 일)을 입력합니다.

     Important

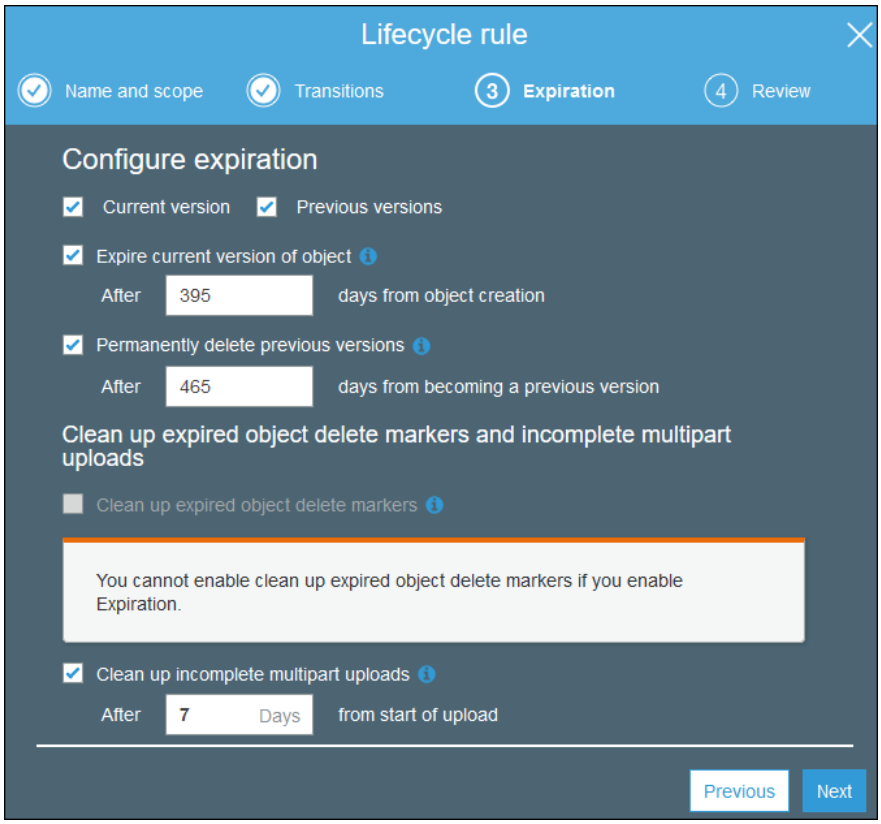
     Glacier 또는 Glacier Deep Archive 스토리지 클래스를 선택하면 객체가 Amazon S3에 그대로 유지됩니다. 별도의 Amazon S3 Glacier 서비스를 통해 직접 액세스할 수 없습니다. 자세한 내용은 Amazon S3 수명 주기를 사용하여 객체 전환 항목을 참조하십시오.



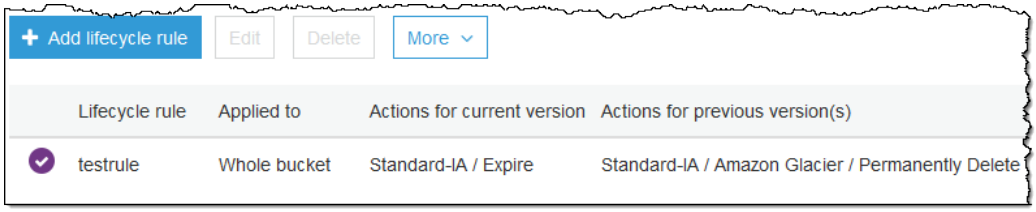
6. 전환 구성이 끝나면 다음을 선택합니다.



7. 이 예제에서는 현재 버전과 이전 버전을 모두 선택합니다.
8. 객체의 현재 버전 만료를 선택한 다음 객체 생성으로부터 며칠이 지나면 객체를 삭제할지 입력합니다(예: 395일). 이 만료 옵션을 선택할 경우 만료된 삭제 마커를 정리하는 옵션을 선택할 수 없습니다.
9. 이전 버전 영구 삭제를 선택한 다음 객체가 이전 버전이 된지 며칠이 지나면 영구 삭제할지 입력합니다(예: 465일).
10. 권장 모범 사례는 언제나 불완전 멀티파트 업로드 정리를 선택하는 것입니다. 예를 들어, 멀티파트 업로드 시작일 이후 완료되지 않은 멀티파트 업로드를 종료하고 제거하고자 하는 일수를 **7**로 입력합니다. 멀티파트 업로드에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 멀티파트 업로드 개요 단원을 참조하십시오.
11. [Next]를 선택합니다.



12. 복습에서는 규칙 설정을 확인합니다. 설정을 변경하려면 이전을 선택합니다 그렇지 않은 경우 [Save]를 선택합니다.
13. 규칙에 아무런 오류가 없으면, 수명 주기 페이지에 표시되고 활성화됩니다.



S3 버킷에서 복제 규칙을 추가하는 방법

복제는 동일한 AWS 리전 또는 서로 다른 AWS 리전의 버킷 간에 객체를 비동기식으로 자동 복사하는 것을 말합니다. 복제는 새로 생성된 객체 및 객체 업데이트를 원본 버킷에서 지정된 대상 버킷으로 복사합니다. 복제 개념과 이를 AWS CLI, AWS SDK 및 Amazon S3 REST API와 함께 사용하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 복제 단원을 참조하십시오.

복제를 위해서는 원본 버킷과 대상 버킷 모두에서 버전 관리를 활성화해야 합니다. 요구 사항의 전체 목록을 확인하려면 Amazon Simple Storage Service 개발자 가이드의 복제 요구 사항 단원을 참조하십시오. 버전 관리에 대한 자세한 내용은 S3 버킷의 버전 관리 기능을 활성화하거나 해제하려면? (p. 7) 단원을 참조하십시오.

대상 버킷의 객체 복제본은 원본 버킷 내 객체와 동일합니다. 이 복제본은 생성 시간, 소유자, 사용자 정의 메타데이터, 버전 ID, ACL(액세스 통제 목록), 스토리지 클래스 등을 나타내는 동일한 메타데이터와 키 이름을 갖습니다. 경우에 따라 객체 복제본에 대해 다른 스토리지 클래스를 명시적으로 지정할 수 있습니다. 또한 원

본 버킷 또는 원본 객체의 소유자에 상관없이 대상 버킷을 소유한 AWS 계정으로 복제본 소유권을 변경하도록 선택할 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 복제본 소유자 변경을 참조하십시오.

S3 Replication Time Control (S3 RTC)를 사용하여 예측 가능한 기간 내에 동일한 AWS 리전에 또는 여러 AWS 리전 간에 데이터를 복제할 수 있습니다. S3 RTC는 Amazon S3에 저장된 새 객체의 99.99%를 15분 내에 복제하고 대부분의 객체를 몇 초 만에 복제합니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 S3 Replication Time Control(S3 RTC)을 사용하여 객체 복제를 참조하십시오.

복제본 및 수명 주기 규칙에 대한 참고 사항

원본 객체와 복제 객체 간 객체에 따른 메타데이터는 여전히 동일합니다. 수명 주기 규칙은 복제된 객체를 대상 버킷에서 사용할 수 있게 되는 시간이 아니라 원본 객체의 생성 시간을 따릅니다. 하지만 복제가 보류 중인 객체에는 복제가 완료될 때까지 수명 주기가 작동하지 않습니다.

Amazon S3 콘솔을 사용하면 원본 버킷에 복제 규칙을 추가할 수 있습니다. 복제 규칙은 복제할 원본 버킷 객체와 복제된 객체가 저장된 대상 버킷을 정의합니다. 특정 키 이름 접두사, 하나 이상의 객체 태그 또는 이 두 가지를 모두 포함하는 버킷 또는 객체 하위 집합에 있는 모든 객체를 복제하는 규칙을 작성할 수 있습니다. 대상 버킷은 원본 버킷과 동일한 AWS 계정에 있거나 다른 계정에 존재할 수 있습니다.

대상 버킷이 원본 버킷과 다른 계정에 있는 경우, 원본 버킷 계정의 소유자에게 대상 버킷의 객체를 복제할 수 있는 권한을 부여하려면 대상 버킷에 하나의 버킷 정책을 추가해야 합니다. Amazon S3 콘솔은 이 필수 버킷 정책을 빌드하여 다른 계정의 대상 버킷에 복사 및 추가할 수 있습니다.

버킷에 복제 규칙을 추가하면 이 규칙이 기본적으로 활성화되므로 이 규칙을 저장하면 그 즉시 작업이 시작됩니다.

주제

대상 버킷이 동일한 AWS 계정에 있는 경우 복제 규칙 추가

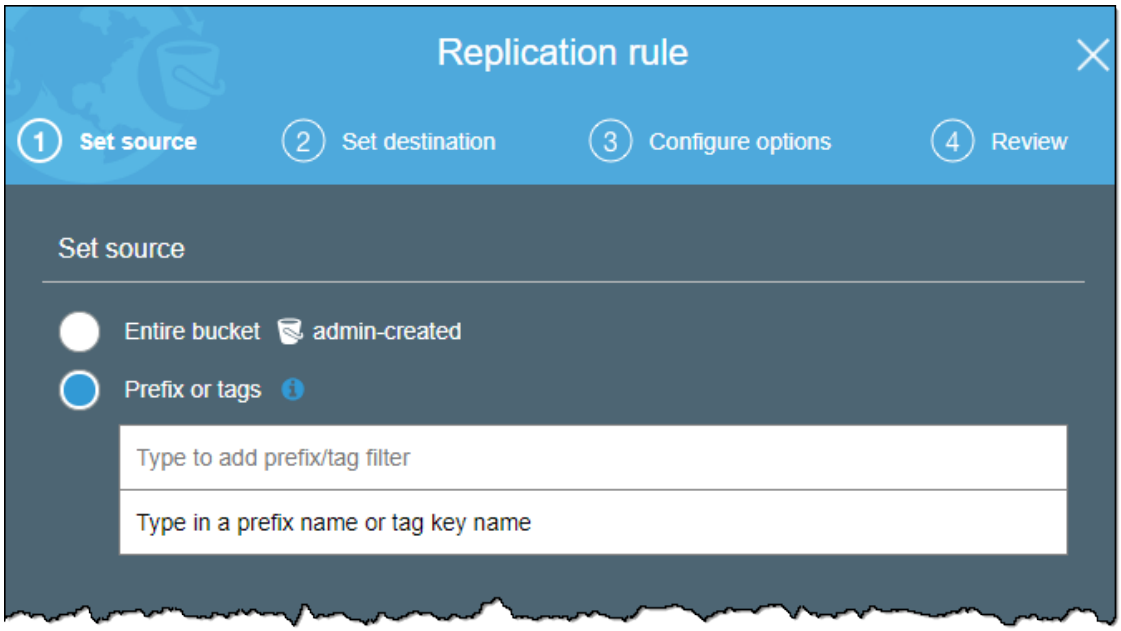
대상 버킷이 원본 버킷과 동일한 AWS 계정에 있는 경우 복제 규칙을 구성하려면 다음 단계를 따릅니다.

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 원하는 버킷의 이름을 선택합니다.

3. 관리와 복제를 차례대로 선택한 다음, 규칙 추가를 선택합니다.

4. 복제 규칙 마법사에서 Set source(원본 설정) 아래에 복제 원본을 설정하기 위한 옵션이 있습니다.

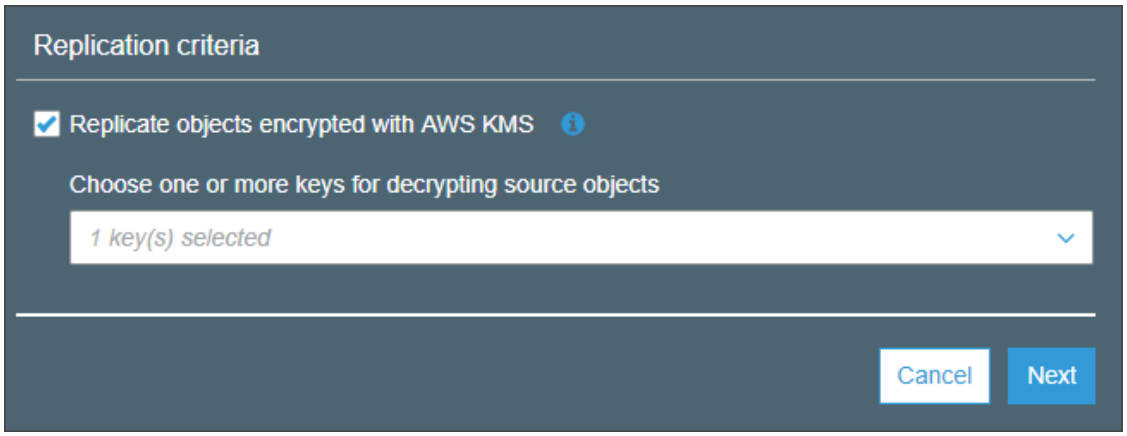
   - 전체 버킷을 복제하려면 전체 버킷 ***bucket-name***을 선택합니다.
   - 동일한 접두사를 가진 모든 객체(예를 들면 문자열 `pictures`로 시작하는 이름을 가진 모든 객체)를 복제하려면 Prefix or tags(접두사 또는 태그)를 선택합니다. 상자에 접두사를 입력하고, 드롭다운 목록에서 접두사를 선택한 다음 Enter(입력)를 누릅니다. 어떤 폴더의 이름에 해당하는 접두사를 입력할 경우, /(슬래시)를 마지막 문자(예: `pictures/`)로 사용해야 합니다. 접두사에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 객체 키 단원을 참조하십시오.
   - 하나 이상의 객체 태그가 있는 모든 객체를 복제하려면 상자에 태그를 입력하고 드롭다운 목록에서 태그를 선택한 다음 Enter를 누릅니다. 태그 값을 입력하고 Enter(입력)를 누릅니다. 절차를 반복하여 다른 태그를 추가합니다. 접두사와 태그를 결합할 수도 있습니다. 객체 태그에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 객체 태그 지정 단원을 참조하십시오.



   새로운 스키마는 접두사 및 태그 필터링과 규칙 우선 순위 지정을 지원합니다. 새로운 스키마에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 복제 구성 이전 버전과의 호환성을 참조하십시오. 개발자 안내서에서는 사용자 인터페이스의 배후에서 작동하는, Amazon S3 API와 함께 사용되는 XML을 설명합니다. 개발자 안내에서에서 새로운 스키마는 복제 구성 XML V2로 기술됩니다.

5. AWS Key Management Service(AWS KMS)로 암호화되는 원본 버킷의 객체를 복제하려면 복제 기준에서 AWS KMS로 암호화된 객체 복제를 선택합니다. Choose one or more keys for decrypting source objects(원본 객체 암호 해독을 위해 하나 이상의 키 선택) 아래에는 복제를 사용할 수 있는 원본 AWS KMS 고객 마스터 키(CMK)가 있습니다. 기본적으로 모든 원본 CMK가 포함됩니다. CMK 선택 범위를 좁히도록 선택할 수 있습니다.

선택하지 않은 AWS KMS CMK로 암호화된 객체는 복제되지 않습니다. CMK 또는 CMK 그룹이 자동으로 선택되지만 원하는 경우 CMK를 선택할 수 있습니다. 복제에 AWS KMS를 사용하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 AWS KMS에 저장된 암호화 키를 사용한 서버 측 암호화(SSE)로 생성된 객체 복제를 참조하십시오.



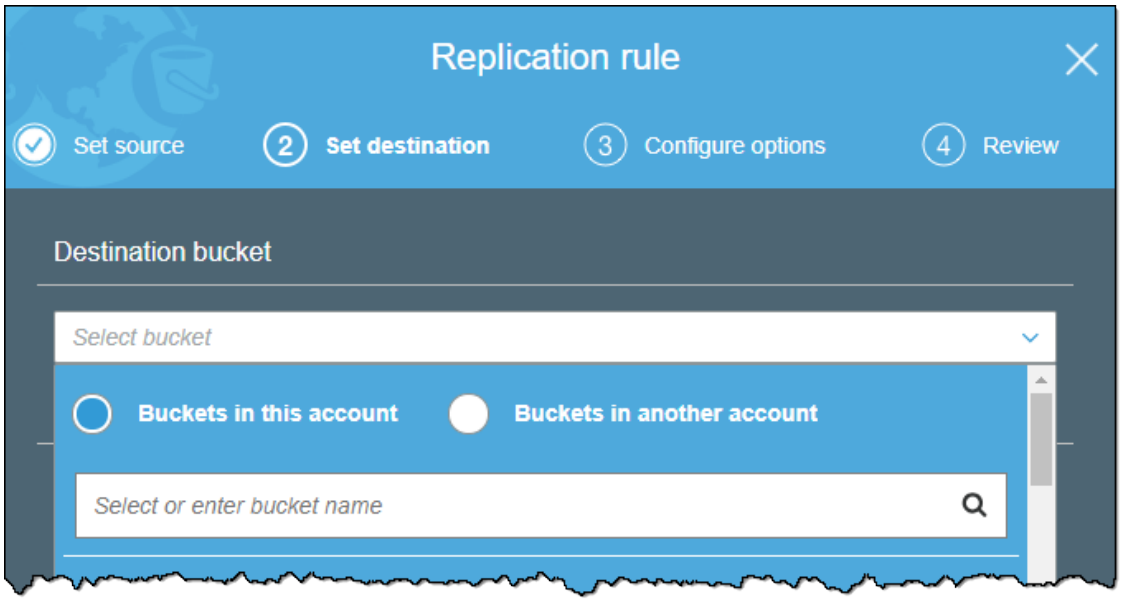
Important

AWS KMS를 사용하여 암호화된 객체를 복제하는 경우 AWS KMS 요청 빈도는 소스 리전에서 두 배가 되고 대상 리전에서는 같은 양만큼 늘어납니다. AWS KMS에 대해 늘어난 호출 빈도는 복제 대상 리전에 대해 정의한 CMK(고객 마스터 키)를 사용하여 데이터가 다시 암호화되는 방식 때문입니다. AWS KMS에는 리전당 호출 계정에 따른 요청 속도 제한이 있습니다. 제한 기본값에 대한 자세한 내용은 AWS Key Management Service Developer Guide의 AWS KMS 제한 - 초당 요청: 달라짐을 참조하십시오.
복제 중 현재 Amazon S3 PUT 객체 요청 속도가 계정에 대한 기본 AWS KMS 속도 제한의 절반보다 큰 경우 AWS KMS 요청 속도 제한 증가를 요청하는 것이 좋습니다. 증가를 요청하려면 문의처의 AWS 지원 센터에서 케이스를 생성합니다. 예를 들어 현재 PUT 객체 요청 빈도가 초당 1,000개 요청이고 AWS KMS를 사용하여 객체를 암호화한다고 가정합니다. 이 경우 AWS KMS에서 조절이 발생하지 않도록 AWS Support에 소스 리전과 대상 리전 둘 다에서 AWS KMS 속도 제한을 초당 2,500개 요청으로 올려달라고 요청하는 것이 좋습니다.
원본 버킷에서 PUT 객체 요청 빈도를 확인하려면 Amazon S3에 대한 Amazon CloudWatch 요청 지표 중에서 `PutRequests`를 확인합니다. CloudWatch 지표 보기에 대한 자세한 내용은 요청 지표를 S3 버킷용으로 구성하려면 어떻게 해야 합니까? (p. 103) 단원을 참조하십시오.

다음을 선택합니다.

6. 현재 사용 중인 계정에서 대상 버킷을 선택하려면 Set destination(대상 설정) 페이지의 대상 버킷에서 이 계정의 버킷을 선택합니다. 해당 복제에 대한 대상 버킷의 이름을 입력하거나 드롭다운 목록에서 이름을 선택합니다.

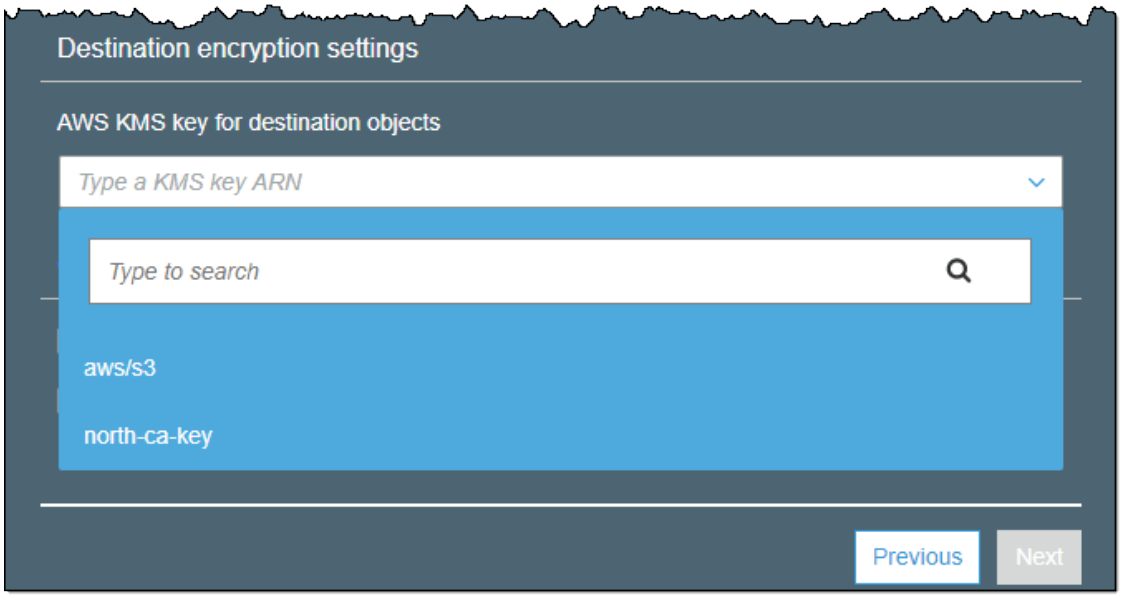
   다른 AWS 계정에서 대상 버킷을 선택하려는 경우 대상 버킷이 다른 AWS 계정에 있는 경우 복제 규칙 추가 (p. 87) 단원을 참조하십시오.



대상 버킷에서 버전 관리가 활성화되어 있지 않을 경우, 버전 관리 가능 버튼이 포함된 경고 메시지가 나타납니다. 이 버튼을 선택하면 버킷의 버전 관리가 활성화됩니다.

7. AWS KMS로 암호화된 객체를 복제하도록 선택한 경우 Destination encryption settings(대상 암호화 설정) 아래에 대상 버킷의 복제본을 암호화하는 데 사용할 AWS KMS CMK의 Amazon 리소스 이름(ARN)을 입력합니다. IAM 콘솔의 Encryption keys(암호화 키) 아래에서 AWS KMS CMK의 ARN을 찾을 수 있습니다. 또는 드롭다운 목록에서 CMK 이름을 선택할 수 있습니다.

   AWS KMS CMK 생성에 대한 자세한 내용은 AWS Key Management Service Developer Guide의 키 생성을 참조하십시오.



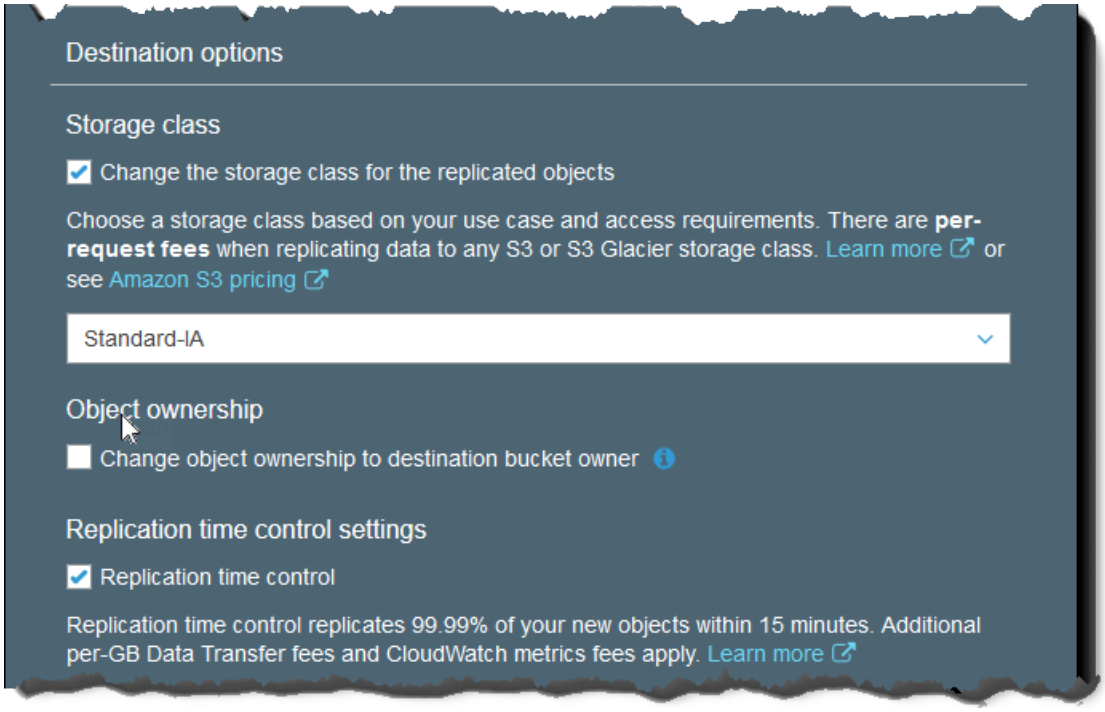
8. 대상 버킷의 특정 스토리지 클래스로 데이터를 복제하려는 경우 대상 설정 페이지의 대상 옵션에서 복제된 객체의 스토리지 클래스를 변경합니다.를 선택합니다. 그런 다음, 대상 버킷의 복제된 객체에 사용할 스토리지 클래스를 선택합니다. 이 옵션을 선택하지 않을 경우, 복제된 객체의 스토리지 클래스는 원본 객체와 동일한 클래스에 해당됩니다.

마찬가지로 대상 버킷에서 객체 소유권을 변경하려면 객체 소유권을 대상 버킷 소유자로 변경을 선택합니다. 이 옵션에 대한 자세한 내용은 대상 버킷이 다른 AWS 계정에 있는 경우 복제 규칙 추가 (p. 87) 단원을 참조하십시오.

복제 구성에서 S3 Replication Time Control (S3 RTC)를 활성화하려면 복제 시간 제어를 선택합니다.

Note

S3-RTC를 사용하는 경우 GB당 데이터 전송 요금 및 CloudWatch 지표 요금이 추가로 적용됩니다.



다음을 선택합니다.

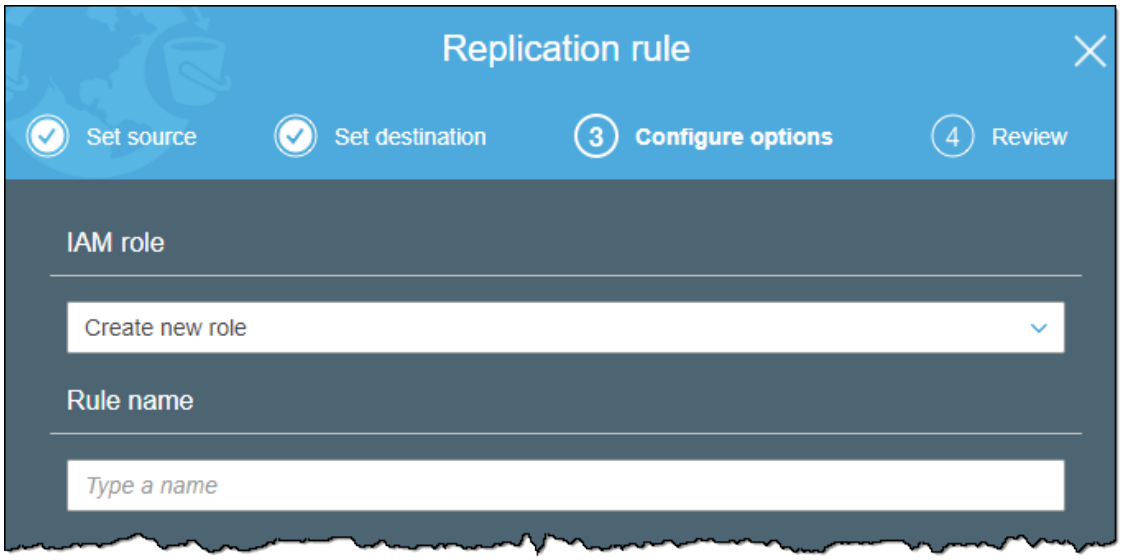
9. Amazon S3가 사용자 대신 객체를 복제하기 위해 수임할 수 있는 AWS Identity and Access Management(IAM) 역할을 설정합니다.

   IAM 역할을 설정하려면 Configure options(옵션 구성) 페이지의 역할 선택 아래에서 다음 중 한 가지를 수행합니다.

   - 새 역할 생성을 선택하여 Amazon S3에서 자동으로 새 IAM 역할을 생성하는 것이 좋습니다. 규칙을 저장하면 선택한 원본 및 대상 버킷과 일치하는 IAM 역할에 대해 새 정책이 생성됩니다. 생성된 역할의 이름은 버킷 이름을 기반으로 명명되며 다음과 같은 이름 지정 규칙을 사용합니다. replication_role_for_***source-bucket***_to_***destination-bucket***
   - 기존 IAM 역할을 사용할 수 있습니다. 이 경우 복제에 필요한 권한을 에 부여하는 역할을 선택해야 합니다. 이 역할이 복제 규칙을 따를 수 있는 충분한 권한을 Amazon S3에 부여하지 않으면 복제가 실패합니다.

     Important

     버킷에 복제 규칙을 추가하려면 Amazon S3에 복제 권한을 부여하는 IAM 역할을 전달할 수 있는 `iam:PassRole` 권한이 있어야 합니다. 자세한 내용은 IAM 사용 설명서의 사용자에게 AWS 서비스에 역할을 전달할 수 있는 권한 부여 단원을 참조하십시오.

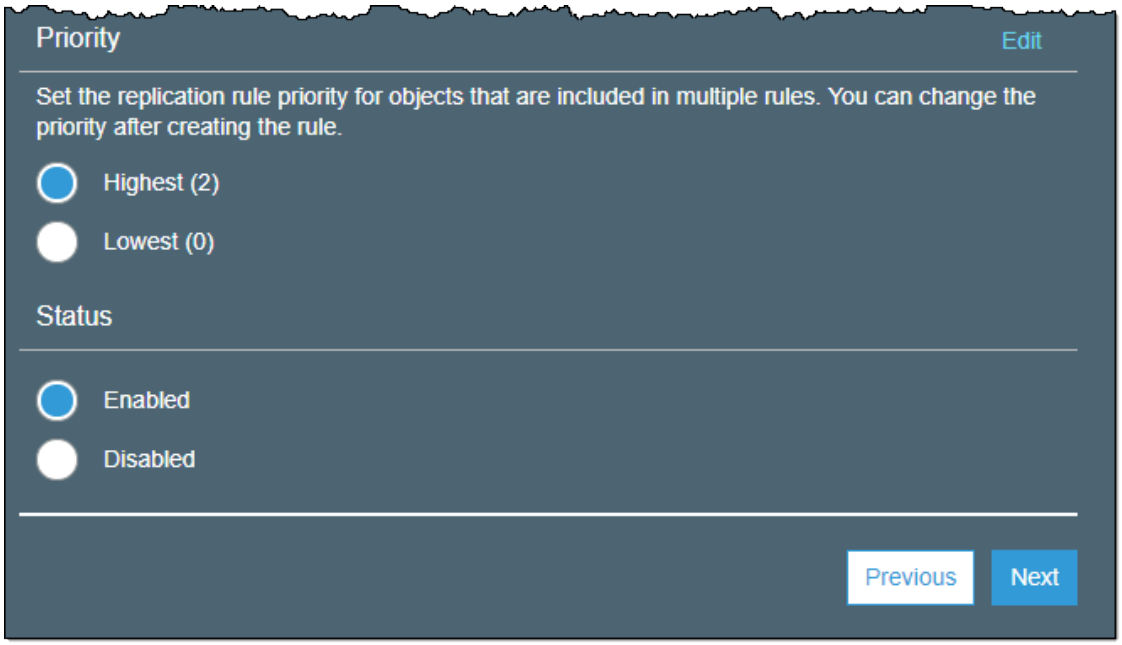


규칙 이름에 나중에 규칙을 쉽게 식별할 수 있는 규칙 이름을 입력합니다. 이름은 필수 항목이며 버킷 내에서 고유해야 합니다.

10. 버킷에 기존 복제 규칙이 있는 경우 규칙에 우선 순위를 설정하라는 메시지가 표시됩니다. 여러 규칙의 범위에 포함된 객체로 인해 발생하는 충돌을 방지하기 위해 규칙의 우선 순위를 설정해야 합니다. 중첩 규칙의 경우, Amazon S3는 규칙 우선 순위를 사용하여 어느 규칙을 적용할지 결정합니다. 숫자가 클수록 우선 순위가 높아집니다. 규칙 우선 순위에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 복제 구성 개요 단원을 참조하십시오.

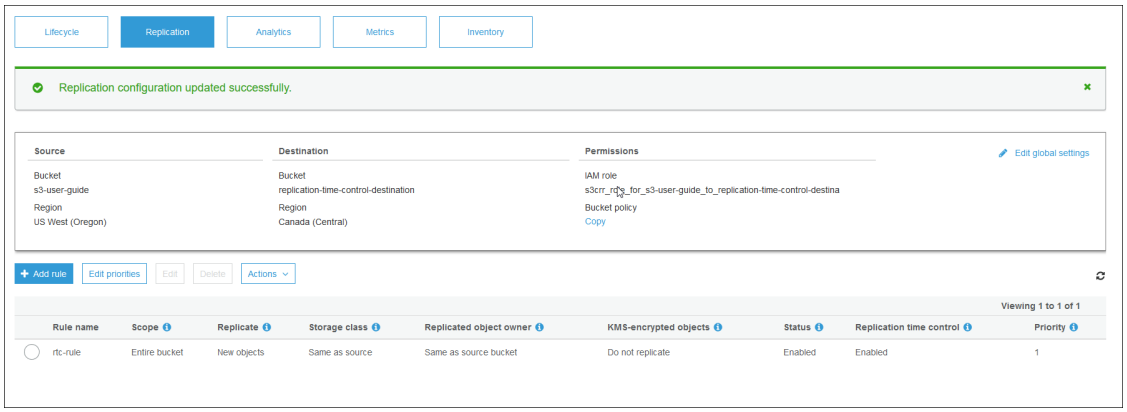
    상태 아래의 활성이 기본적으로 선택됩니다. 활성화된 규칙은 저장하는 즉시 적용되기 시작합니다. 나중에 규칙을 활성화하고 싶다면 Disabled(비활성화됨)를 선택하십시오.

    다음을 선택합니다.



11. 복습 페이지에서 복제 규칙을 검토합니다. 이 규칙이 올바르게 보인다면 저장을 선택합니다. 그렇지 않으면 이전을 선택해 해당 규칙을 편집한 후 저장합니다.

12. 규칙을 저장하면 복제 페이지에서 규칙을 편집, 활성화, 비활성화하거나 삭제할 수 있습니다.

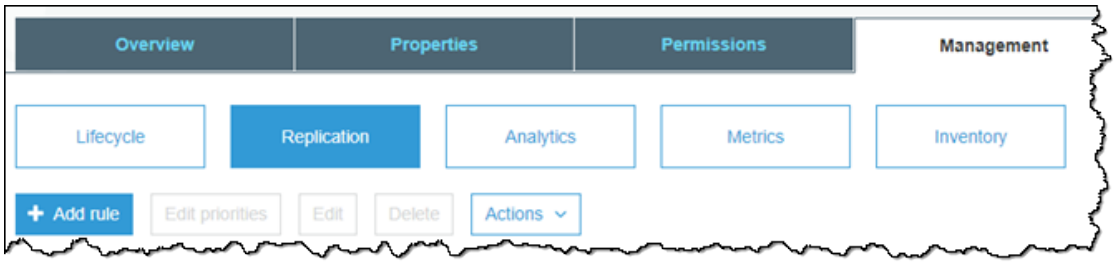


대상 버킷이 다른 AWS 계정에 있는 경우 복제 규칙 추가

대상 버킷이 원본 버킷과 다른 AWS 계정에 있는 경우 복제 규칙을 구성하려면 다음 단계를 따릅니다.

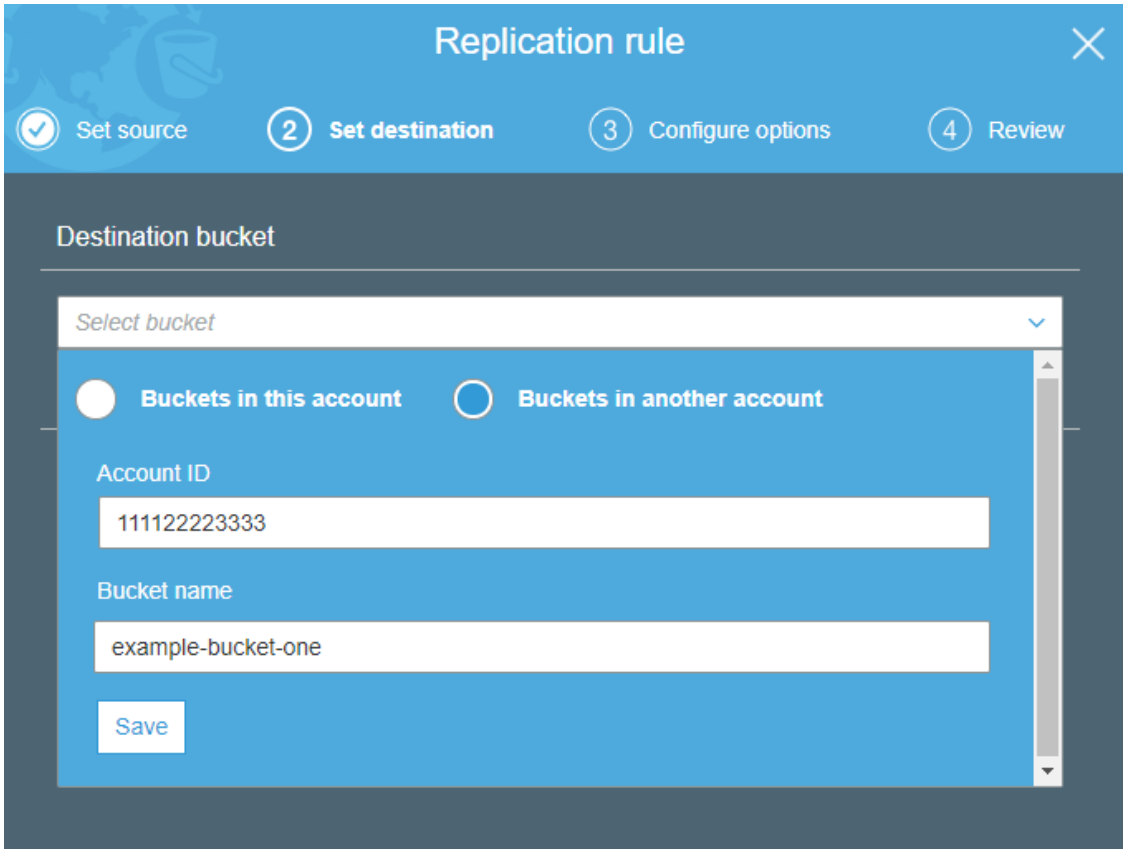
1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 원하는 버킷의 이름을 선택합니다.

3. 관리와 복제를 차례대로 선택한 다음, 규칙 추가를 선택합니다.

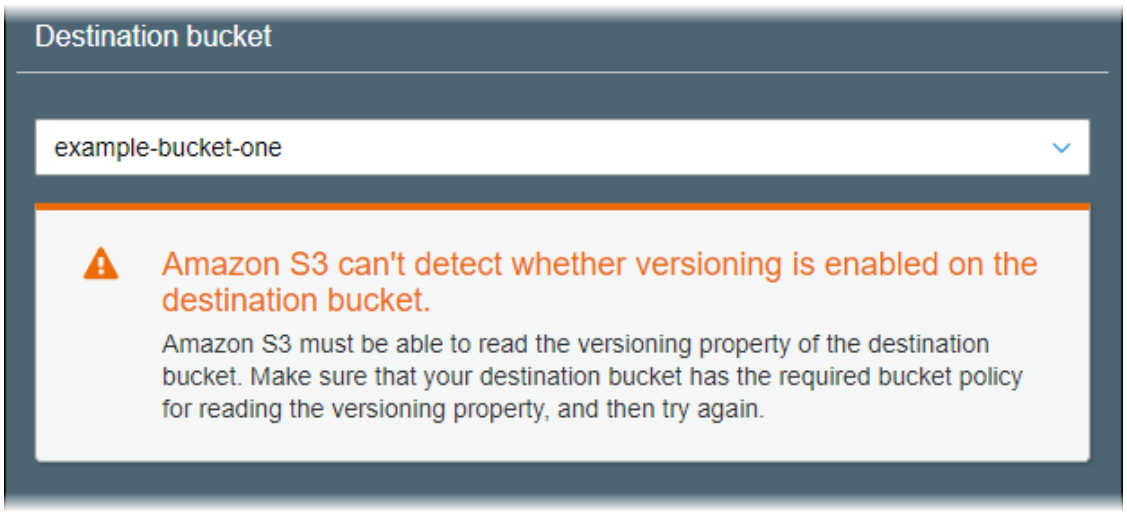


4. 이전에 복제 규칙을 생성한 적이 없는 경우 대상 버킷이 동일한 AWS 계정에 있는 경우 복제 규칙 추가 (p. 81) 단원으로 시작합니다.

   복제 규칙 마법사에서 Set destination(대상 설정) 페이지의 대상 버킷에 대해 다른 계정의 버킷을 선택합니다. 그런 다음 대상 버킷의 이름 및 다른 AWS 계정의 계정 ID를 입력합니다. Save를 선택합니다.

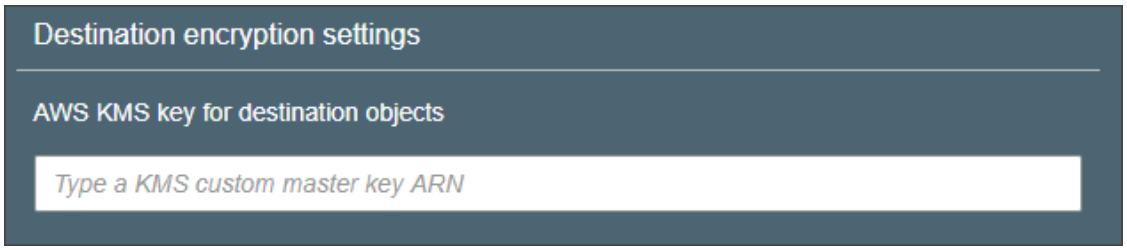


대상 버킷 이름과 계정 ID를 저장하면 Amazon S3가 해당 버킷에서 버전 관리가 활성화되었는지 여부를 확인할 수 있도록 버킷 정책을 대상 버킷에 추가해야 함을 나타내는 경고 메시지가 나타날 수 있습니다. 복사하여 다른 계정의 대상 버킷에 추가할 수 있는 몇 단계의 버킷 정책이 나타납니다. 버킷 정책을 S3 버킷에 추가 및 버전 관리에 대한 자세한 내용은 S3 버킷 정책을 추가하려면 어떻게 해야 합니까? (p. 121) 및 S3 버킷의 버전 관리 기능을 활성화하거나 해제하려면? (p. 7)을 참조하십시오.



5. AWS KMS로 암호화된 객체를 복제하도록 선택한 경우 Destination encryption settings(대상 암호화 설정) 아래에 대상 버킷의 복제본을 암호화하는 데 사용할 AWS KMS CMK의 Amazon 리소스 이름(ARN)을 입력합니다.

AWS KMS CMK 생성에 대한 자세한 내용은 AWS Key Management Service Developer Guide의 키 생성을 참조하십시오.



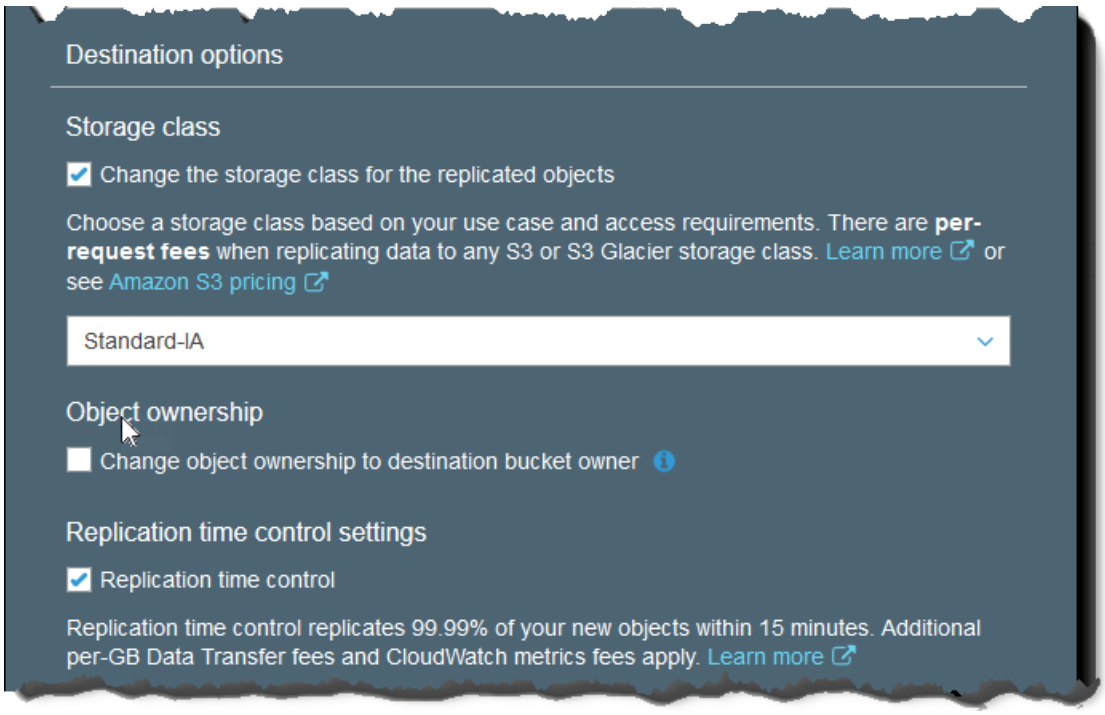
6. 대상 설정 페이지의 대상 옵션에서 다음을 수행합니다.

   - 대상 버킷의 특정 스토리지 클래스로 데이터를 복제하려면 복제된 객체의 스토리지 클래스를 변경합니다.를 선택합니다. 그런 다음, 대상 버킷의 복제된 객체에 사용할 스토리지 클래스를 선택합니다. 이 옵션을 선택하지 않을 경우, 복제된 객체의 스토리지 클래스는 원본 객체와 동일한 클래스에 해당됩니다.
   - 복제본 객체의 객체 소유권을 대상 버킷 소유자로 변경하려면 Change object ownership to destination owner(객체 소유권을 대상 소유자로 변경)를 선택합니다. 이 옵션을 선택하면 복제된 데이터의 객체 소유권을 원본과 분리할 수 있습니다. 요청되면 대상 버킷의 계정 ID를 입력합니다.

     이 옵션을 선택하면 원본 버킷 또는 원본 객체를 누가 소유하든 상관없이 대상 버킷을 소유하는 AWS 계정에 복제본 객체에 대한 전체 권한이 부여됩니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 복제본 소유자 변경을 참조하십시오.
   - S3 Replication Time Control (S3 RTC)를 복제 구성에 추가하려면 복제 시간 제어를 선택합니다.

     Note

     S3 RTC를 사용하는 경우 GB당 데이터 전송 요금 및 CloudWatch 지표 요금이 추가로 적용됩니다.

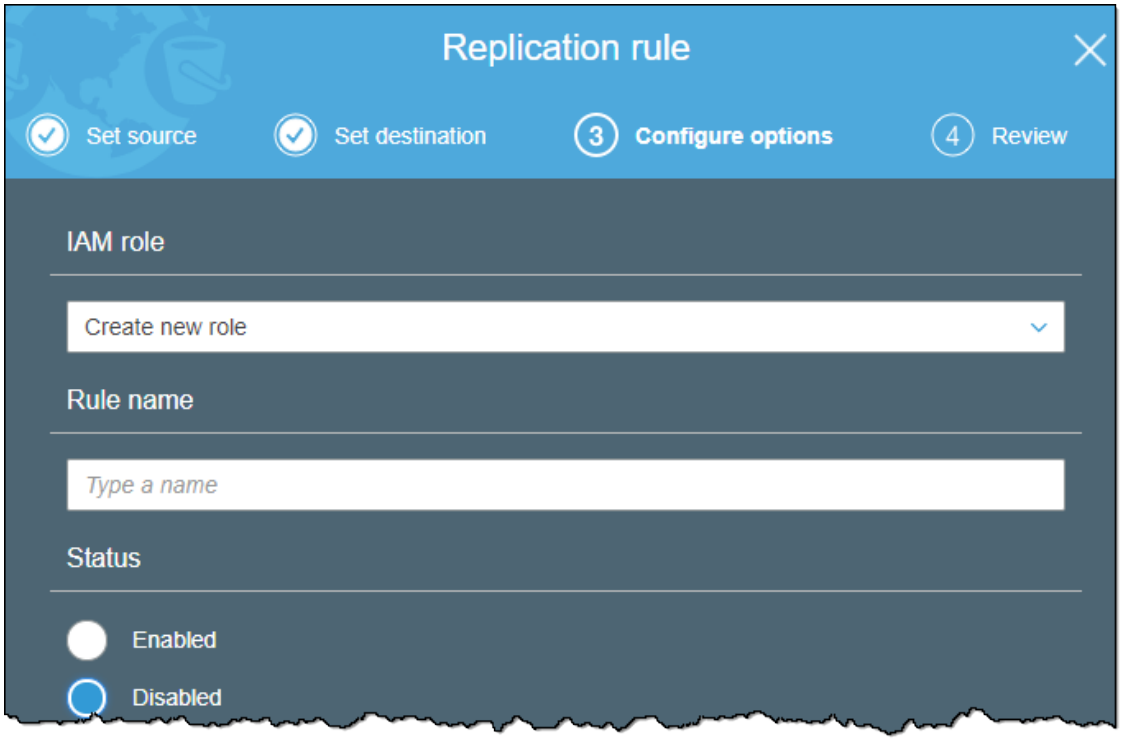


다음을 선택합니다.

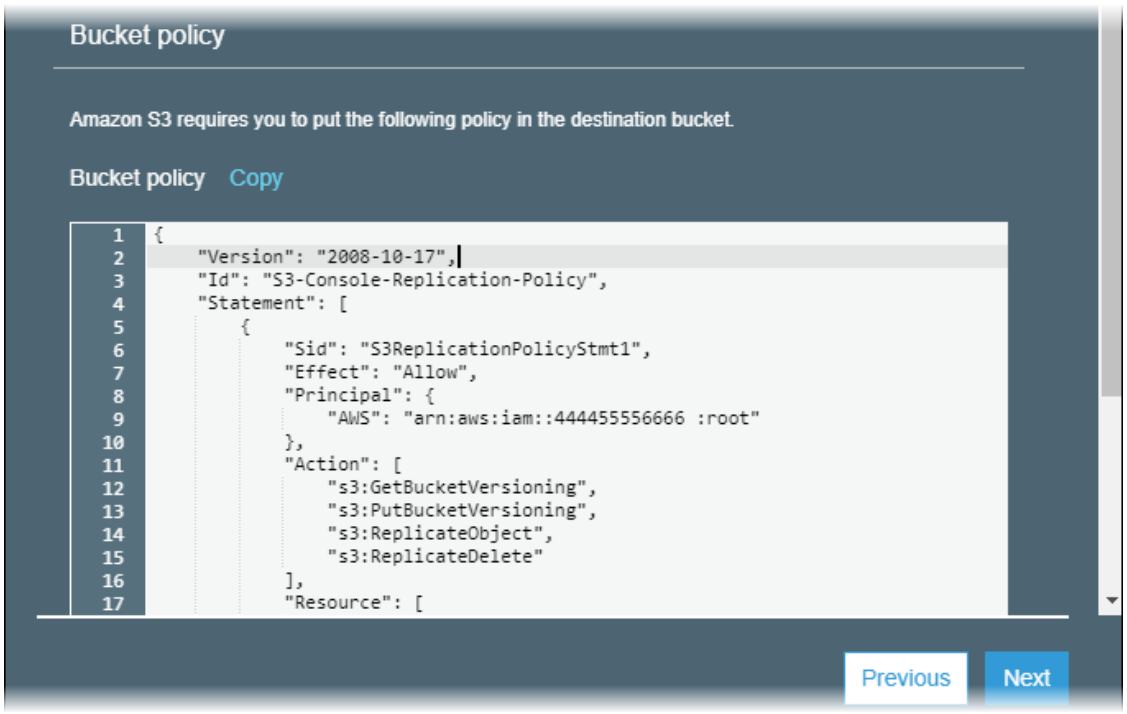
7. 사용자를 대신하여 객체의 복제를 수행하기 위해 Amazon S3가 수임할 수 있는 AWS Identity and Access Management(IAM) 역할을 설정합니다.

   IAM 역할을 설정하려면 Configure options(옵션 구성) 페이지의 역할 선택 아래에서 다음 중 한 가지를 수행합니다.

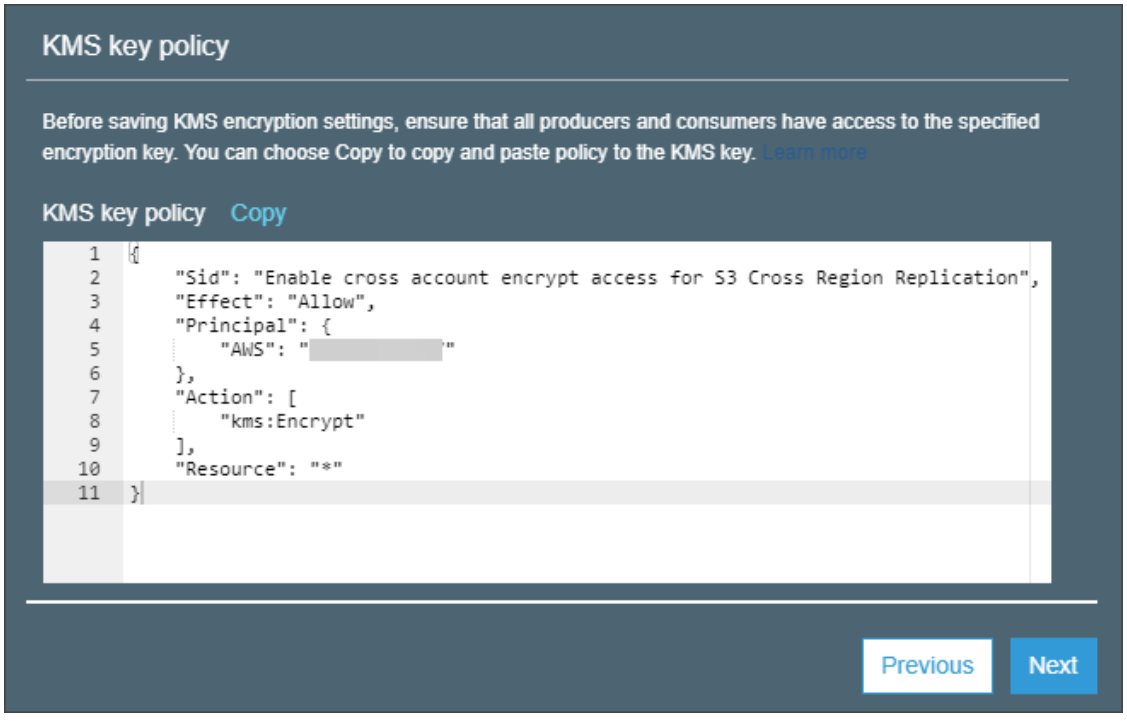
   - 새 역할 생성을 선택하여 Amazon S3에서 자동으로 새 IAM 역할을 생성하는 것이 좋습니다. 규칙을 저장하면 선택한 원본 및 대상 버킷과 일치하는 IAM 역할에 대해 새 정책이 생성됩니다. 생성된 역할의 이름은 버킷 이름을 기반으로 명명되며 다음과 같은 이름 지정 규칙을 사용합니다. replication_role_for_***source-bucket***_to_***destination-bucket***
   - 기존 IAM 역할을 사용할 수 있습니다. 이렇게 하는 경우 Amazon S3가 사용자를 대신하여 원본 버킷에서 대상 버킷으로 객체를 복제하도록 허용하는 역할을 선택해야 합니다.



8. 복사하여 다른 계정의 대상 버킷에 추가할 수 있는 버킷 정책은 Configure options(옵션 구성) 페이지에 제공됩니다. 버킷 정책을 S3 버킷에 추가하는 방법에 관한 자세한 내용은 S3 버킷 정책을 추가하려면 어떻게 해야 합니까? (p. 121) 단원을 참조하십시오.

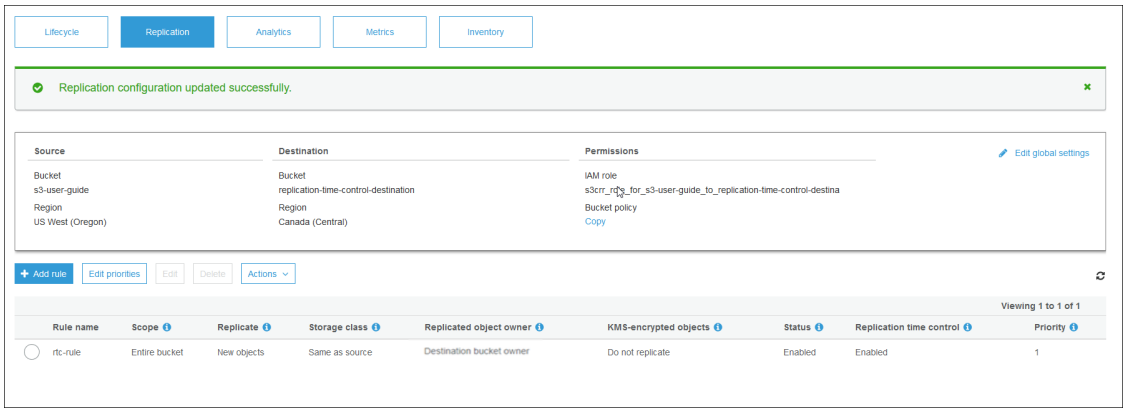


9. AWS KMS로 암호화된 객체를 복제하도록 선택한 경우 Configure options(옵션 구성) 페이지에 AWS KMS 키 정책이 제공됩니다. 이 정책을 복사하여 사용 중인 AWS KMS CMK에 대한 키 정책에 추가할 수 있습니다. 이 키 정책은 원본 버킷 소유자에게 CMK를 사용할 수 있는 권한을 부여합니다. 키 정책 업데이트에 대한 자세한 내용은 원본 버킷 소유자에게 AWS KMS CMK를 사용하여 암호화할 수 있는 권한 부여 (p. 93) 단원을 참조하십시오.



10. 복습 페이지에서 복제 규칙을 검토합니다. 이 규칙이 올바르게 보인다면 저장을 선택합니다. 그렇지 않으면 이전을 선택해 해당 규칙을 편집한 후 저장합니다.

11. 규칙을 저장하면 복제 페이지에서 규칙을 편집, 활성화, 비활성화하거나 삭제할 수 있습니다.



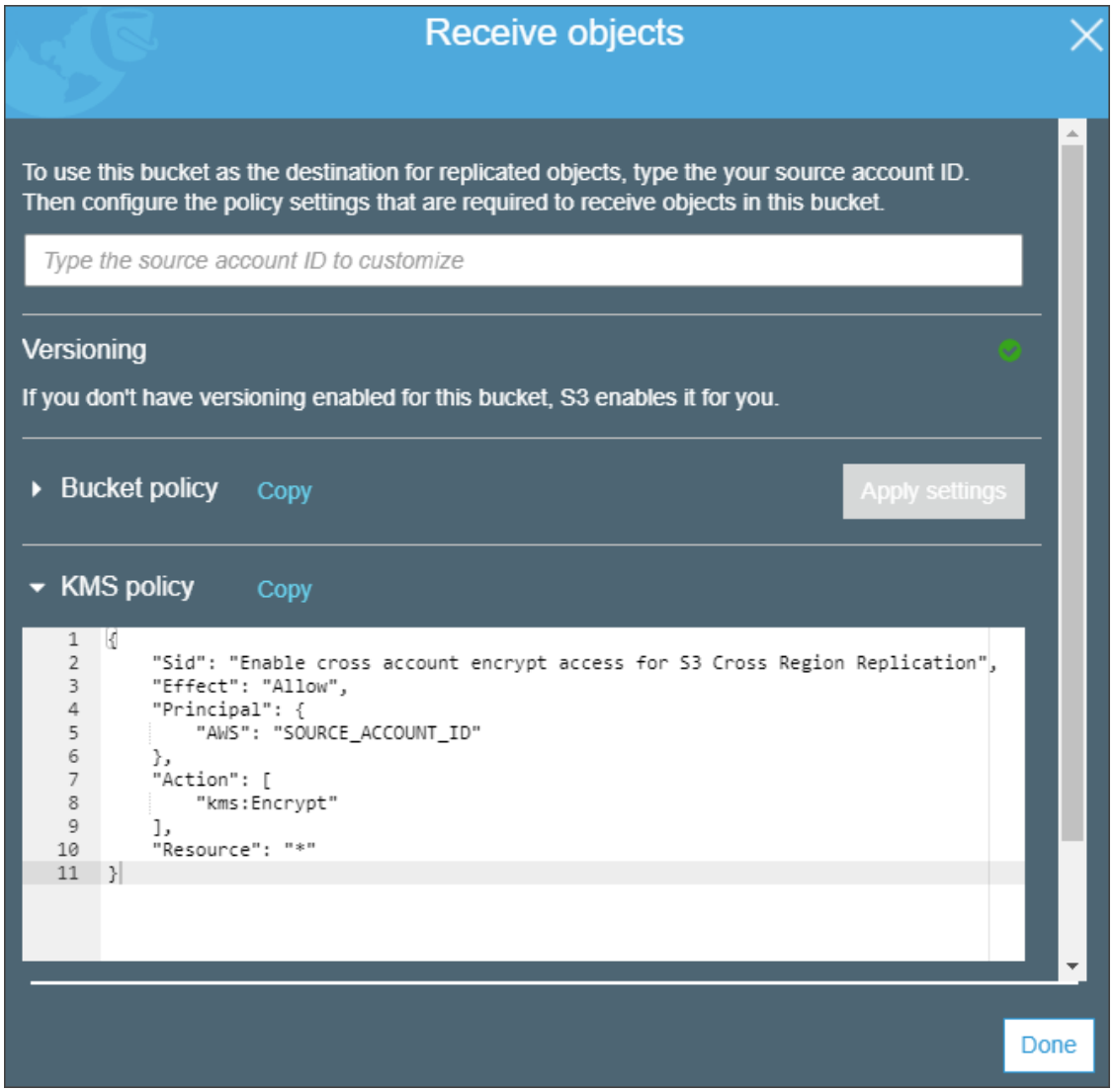
12. 복제 페이지의 경고 메시지 The replication rule is saved, but additional settings are required in the destination account.(복제 규칙이 저장되었지만 대상 계정에 추가 설정이 필요합니다.) 아래에 제시된 지침을 따릅니다. 아래에 제공된 지침을 따릅니다. 현재 로그인하고 있는 AWS 계정에서 로그아웃한 다음, 대상 계정에 로그인합니다.

    Important

    대상 계정에 로그인하고 다음 단계를 완료할 때까지 복제가 실패합니다.

13. 대상 계정에 로그인한 후 관리 탭을 선택하고, 복제를 선택한 다음, 작업 메뉴에서 객체 받기를 선택합니다.
14. 객체 받기 페이지에서 다음을 수행할 수 있습니다.

    - 대상 버킷의 버전 관리를 활성화합니다.
    - Amazon S3가 제공하는 버킷 정책을 대상 버킷에 적용합니다.
    - 대상 버킷의 복제본 객체를 암호화하는 데 사용되는 AWS KMS CMK를 업데이트하기 위해 필요한 AWS KMS 키 정책을 복사합니다. 키 정책 업데이트에 대한 자세한 내용은 원본 버킷 소유자에게 AWS KMS CMK를 사용하여 암호화할 수 있는 권한 부여 (p. 93) 단원을 참조하십시오.



원본 버킷 소유자에게 AWS KMS CMK를 사용하여 암호화할 수 있는 권한 부여

원본 버킷 소유자 계정에 키 정책과 함께 AWS KMS CMK를 사용하여 암호화할 수 있는 권한을 부여해야 합니다. 다음 절차에서는 AWS Identity and Access Management(IAM) 콘솔을 사용하여 대상 버킷의 복제본 객체를 암호화하는 데 사용되는 AWS KMS CMK에 대한 키 정책을 수정하는 방법을 설명합니다.

AWS KMS CMK를 사용하여 암호화할 수 있는 권한을 부여하려면

1. AWS KMS CMK를 소유한 AWS 계정을 사용하여 AWS Management 콘솔에 로그인합니다. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 Encryption keys(암호화 키)를 선택합니다.
3. 리전에서 적절한 AWS 리전을 선택합니다. 탐색 모음(오른쪽 상단 모서리)에서 리전 선택기를 사용하지 마십시오.
4. 암호화할 CMK의 별칭을 선택합니다.

5. 페이지의 Key Policy(키 정책) 섹션에서 Switch to policy view(정책 보기로 전환)를 선택합니다.
6. 키 정책 편집기를 사용하여 Amazon S3가 제공하는 키 정책을 기존 키 정책에 삽입한 다음 변경 사항 저장을 선택합니다. 기존 정책의 끝에 정책을 추가할 수 있습니다.

AWS KMS CMK 생성 및 편집에 대한 자세한 내용은 AWS Key Management Service Developer Guide의 시작하기 단원을 참조하십시오.

추가 정보

- S3 버킷에서 복제 규칙을 관리하는 방법 (p. 94)
- S3 버킷의 버전 관리 기능을 활성화하거나 해제하려면? (p. 7)
- Amazon Simple Storage Service 개발자 가이드의 복제

S3 버킷에서 복제 규칙을 관리하는 방법

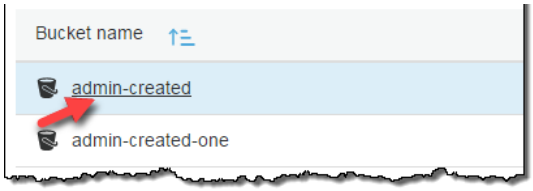
복제는 동일한 AWS 리전 또는 서로 다른 AWS 리전의 버킷 간에 객체를 비동기식으로 자동 복사하는 것을 말합니다. 새로 생성된 객체 및 객체 업데이트를 원본 버킷에서 지정된 대상 버킷으로 복제합니다.

Amazon S3 콘솔을 사용하면 원본 버킷에 복제 규칙을 추가할 수 있습니다. 복제 규칙은 복제할 원본 버킷 객체와 복제된 객체가 저장된 대상 버킷을 각각 정의합니다. 복제에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 복제 단원을 참조하십시오.

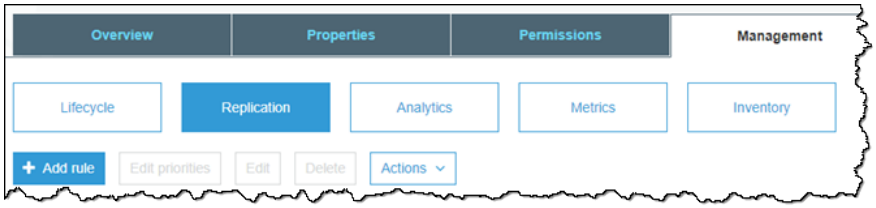
복제 규칙은 복제 페이지에서 관리할 수 있습니다. 복제 규칙은 추가, 보기, 활성화, 비활성화 및 삭제하고 우선 순위를 변경할 수 있습니다. 복제 규칙을 버킷에 추가하는 방법에 관한 자세한 내용은 S3 버킷에서 복제 규칙을 추가하는 방법 (p. 80) 단원을 참조하십시오.

S3 버킷에서 복제 규칙을 관리하려면

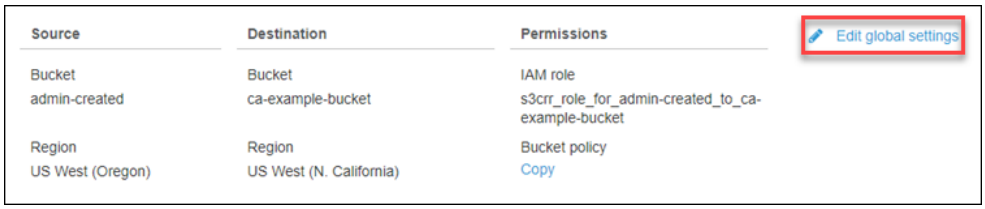
1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 원하는 버킷의 이름을 선택합니다.



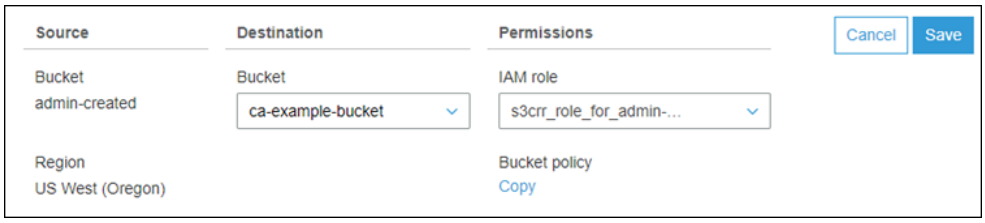
3. 관리를 선택한 다음, 복제를 선택합니다.



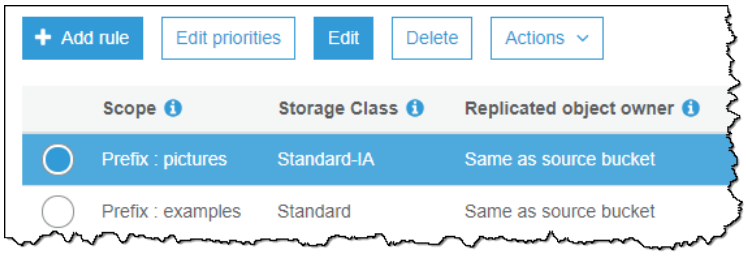
4. 복제 규칙은 다음과 같은 방법으로 변경합니다.
   - 버킷에서 모든 복제 규칙에 영향을 미치는 설정들을 변경하려면 Edit global settings를 선택합니다.



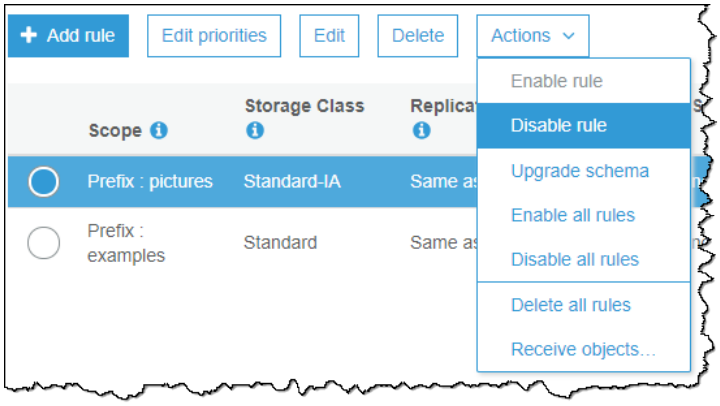
대상 버킷과 IAM 역할을 변경할 수 있습니다. 필요하다면 교차 계정 대상 버킷에 대해 필요한 버킷 정책을 복사할 수 있습니다.



- 복제 규칙을 변경하려면 해당 규칙을 선택하고 편집을 선택합니다. 이렇게 하면 복제 마법사가 시작되어 규칙을 변경하는 데 필요한 도움을 제공합니다. 마법사 사용에 대한 자세한 내용은 다음(S3 버킷에서 복제 규칙을 추가하는 방법 (p. 80))을 참조하십시오.

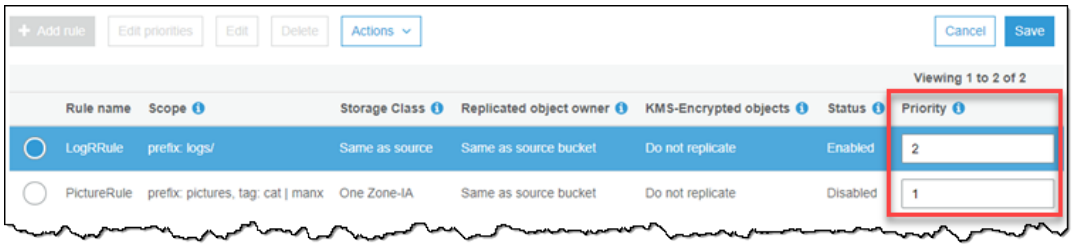


- 복제 규칙을 활성화하거나 비활성화하려면 해당 규칙을 선택하고 More를 선택한 다음, 드롭다운 목록에서 규칙 활성화 또는 규칙 비활성화를 선택합니다. 더 보기 드롭다운 목록의 해당 버킷에 있는 모든 규칙들을 비활성화 및 활성화하거나 삭제할 수도 있습니다.



- 규칙 우선 순위를 변경하려면 Edit priorities(우선 순위 편집)를 선택합니다. 그러면 Priority(우선 순위) 열 제목 아래에서 각 규칙의 우선 순위를 변경할 수 있습니다. [Save]를 선택하여 변경 사항을 저장합니다.

  여러 규칙의 범위에 포함된 객체로 인해 발생하는 충돌을 방지하기 위해 규칙 우선 순위를 설정합니다. 중첩 규칙의 경우, Amazon S3는 규칙 우선 순위를 사용하여 어느 규칙을 적용할지 결정합니다. 숫자가 클수록 우선 순위가 높아집니다. 규칙 우선 순위에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 복제 구성 개요 단원을 참조하십시오.



추가 정보

- S3 버킷에서 복제 규칙을 추가하는 방법 (p. 80)
- Amazon Simple Storage Service 개발자 가이드의 복제

스토리지 클래스 분석을 구성하려면 어떻게 해야 합니까?

Amazon S3 분석 스토리지 클래스 분석 도구를 사용하면 스토리지 액세스 패턴을 분석하여 언제 적합한 데이터를 적절한 스토리지 클래스로 옮길지를 결정할 수 있습니다. 스토리지 클래스 분석은 데이터 액세스 패턴을 관찰해 자주 액세스하지 않는 STANDARD 스토리지를 STANDARD_IA (IA는 자주 액세스하지 않는다는 뜻입니다) 스토리지 클래스로 옮길 시점을 알려줍니다. STANDARD_IA에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 FAQ 및 스토리지 클래스를 참조하십시오.

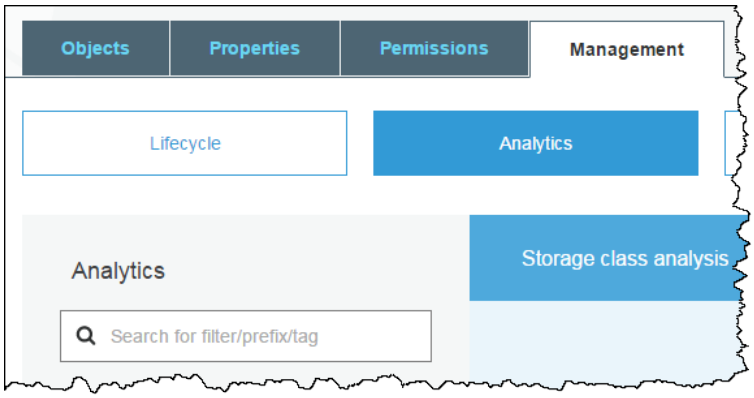
> **Important**
>
> 스토리지 클래스 분석은 ONEZONE_IA 또는 GLACIER 스토리지 클래스로의 전환을 권장하지 않습니다.

분석에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3분석 - 스토리지 클래스 분석 단원을 참조하십시오.

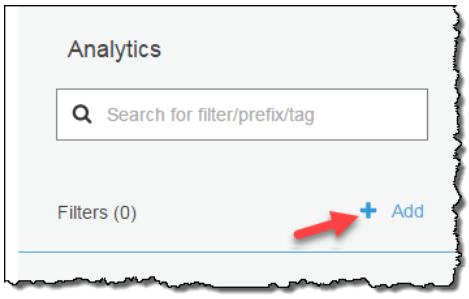
스토리지 클래스 분석 구성 방법

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 스토리지 클래스 분석을 구성할 버킷 이름을 선택합니다.

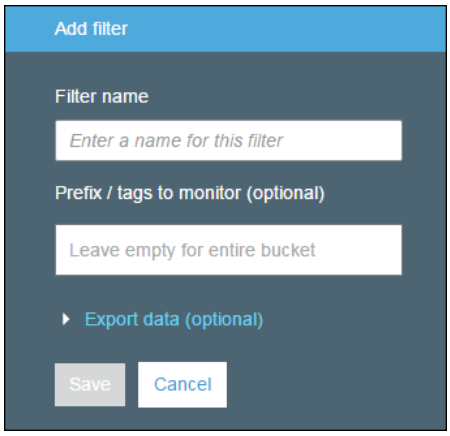
3. 관리 탭을 선택한 후 Analytics를 선택합니다.



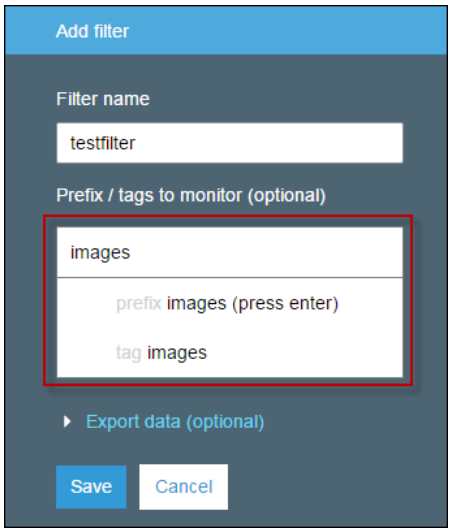
4. 추가를 선택합니다.



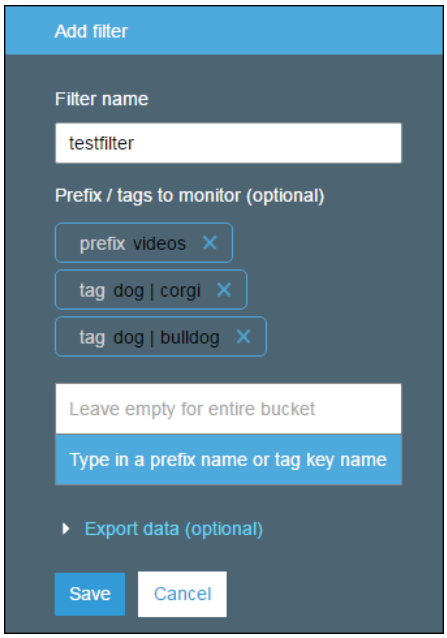
5. 필터 이름을 입력합니다. 버킷 전체를 분석하려면 Prefix / tags(접두사 / 태그) 필드에 아무것도 입력하지 마십시오.



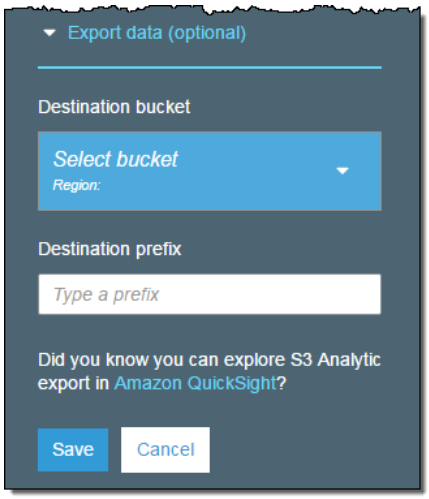
6. Prefix / tags(접두사 / 태그) 필드에 분석할 객체의 접두사 텍스트 또는 태그를 입력하거나, 입력을 시작하면 나타나는 드롭다운 목록에서 선택합니다.



7. 태그를 선택할 경우 태그 값을 입력합니다. 접두사 한 개와 태그 여러 개를 입력할 수 있습니다.



8. 데이터 내보내기를 선택하여 스토리지 클래스 분석을 통해 쉼표로 구분된 값(.csv)이 들어 있는 파일 분석 보고서를 내보내는 방법도 있습니다. 파일을 저장할 수 있는 대상 버킷을 선택합니다. 대상 버킷의 접두사를 입력하면 됩니다. 대상 버킷은 분석 대상 버킷과 같은 AWS 리전에 있어야 합니다. 대상 버킷은 다른 AWS 계정에 속할 수 있습니다.



9. Save를 선택합니다.

Amazon S3는 대상 버킷에서 Amazon S3 쓰기 권한을 부여하는 버킷 정책을 생성합니다. 이렇게 하면 내보내기 데이터를 해당 버킷에 쓸 수 있습니다.

버킷 정책을 생성하는 동안 오류가 발생하는 경우, 해결 지침이 제시됩니다. 예를 들어, 다른 AWS 계정의 대상 버킷을 선택하는 바람에 해당 버킷 정책에 대한 읽기 및 쓰기 권한이 없는 경우, 다음과 같은 메시지가 나타납니다. 대상 버킷 소유자가 표시된 버킷 정책을 대상 버킷에 추가해 주어야만 합니다. Amazon S3는 대상 버킷에 대한 쓰기 권한이 없기 때문에, 이 정책을 대상 버킷에 추가하지 않으면 내보내기 데이터를 받을 수 없게 됩니다. 원본 버킷이 현재 사용자가 아닌 다른 계정의 소유물인 경우, 정책에서 원본 버킷의 올바른 계정 ID로 바꿔야 합니다.

내보낸 데이터와 필터 작동 방식에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 분석 - 스토리지 클래스 분석 단원을 참조하십시오.

추가 정보

스토리지 관리 (p. 76)

Amazon S3 인벤토리를 구성하려면?

Amazon S3 인벤토리는 객체 및 메타데이터 플랫 파일의 목록을 제공하며, Amazon S3 동기식 `List` API 작업 대신 이 예약된 목록을 사용할 수 있습니다. Amazon S3 인벤토리는 S3 버킷 또는 동일한 접두사를 공유하는 객체(동일한 문자열로 시작하는 이름을 가진 객체)에 대해 일별 또는 주별로 객체 및 해당 메타데이터를 나열하는 쉼표로 구분된 값(CSV)이니 Apache ORC(Optimized Row Columnar) 또는 Apache Parquet(Parquet) 출력 파일을 제공합니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 인벤토리 단원을 참조하십시오.

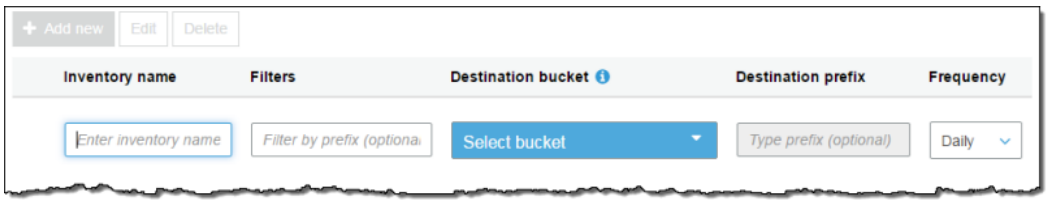
인벤토리를 구성하려면

Note

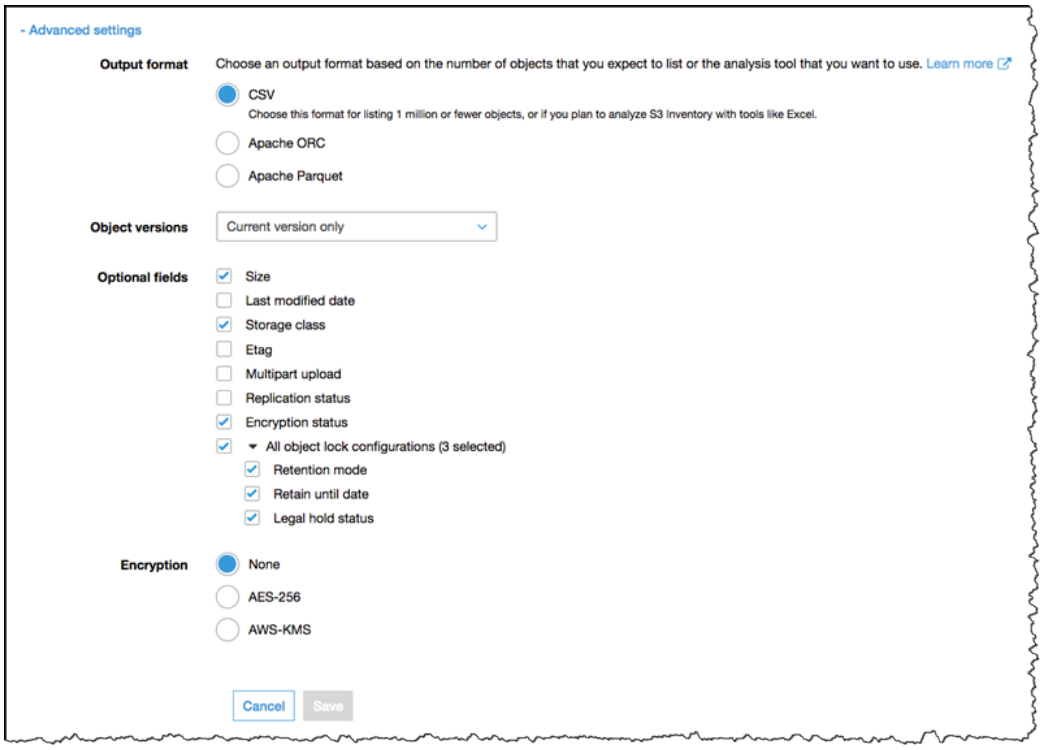
첫 번째 보고서를 전달하는 데 최대 48시간이 걸릴 수 있습니다.

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 Amazon S3 인벤토리를 구성할 버킷의 이름을 선택합니다.

3. 관리 탭을 선택한 후 인벤토리를 선택합니다.
4. 새로 추가를 선택합니다.
5. 인벤토리의 이름을 입력하고 다음과 같이 설정합니다.
   - 또는 필터에 대한 접두사를 동일한 문자열로 시작하는 이름을 가진 객체 인벤토리에 추가합니다.
   - 보고서를 저장할 대상 버킷을 선택합니다. 대상 버킷은 인벤토리를 설정할 버킷과 같은 AWS 리전에 있어야 합니다. 대상 버킷은 다른 AWS 계정에 속할 수 있습니다.
   - 또는 대상 버킷의 접두사를 선택합니다.
   - 인벤토리를 생성할 빈도를 선택합니다.



6. 고급 설정에서 다음을 설정할 수 있습니다.
   a. 인벤토리에 대한 CSV, ORC 또는 Parquet 출력 파일 형식을 선택합니다. 이러한 형식에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 인벤토리 단원을 참조하십시오.



b. 인벤토리에 있는 객체의 모든 버전을 포함시키려면 객체 버전 목록에서 모든 버전 포함을 선택합니다. 기본적으로 인벤토리에는 객체의 현재 버전만 포함됩니다.

c. Optional fields(선택 필드)에 대해 다음 중 하나 이상을 선택하여 인벤토리 보고서에 추가합니다.

- Size – 객체 크기(바이트).
- 마지막 수정 날짜 – 객체 생성일 또는 최종 수정일 중 최근 날짜입니다.
- 스토리지 클래스 – 객체 저장에 사용되는 스토리지 클래스.
- ETag – 개체 태그는 객체의 해시입니다. ETag는 객체의 콘텐츠에 대한 변경 사항만 반영하고 메타데이터에 대한 변경을 반영하지 않습니다. ETag는 객체 데이터의 MD5 다이제스트일 수도 아닐 수도 있습니다. 다이제스트인지 여부는 객체 생성 방식 및 암호화 방식에 좌우됩니다.
- 멀티파트 업로드 – 객체가 멀티파트 업로드로 업로드되도록 지정합니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 멀티파트 업로드 개요를 참조하십시오.
- 복제 상태 – 객체의 복제 상태입니다. 자세한 내용은 S3 버킷에서 복제 규칙을 추가하는 방법 (p. 80) 단원을 참조하십시오.
- 암호화 상태 – 객체를 암호화하는 데 사용된 서버 측 암호화입니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 서버 측 암호화를 사용하여 데이터 보호 단원을 참조하십시오.
- Object lock configurations(객체 잠금 구성) – 다음 설정을 포함한 객체의 객체 잠금 상태:
  - 보존 모드 – 객체에 적용된 보호 수준: 거버넌스 또는 규정 준수.
  - Retain until date(보관 종료일) – 잠긴 객체를 삭제할 수 없는 기한.
  - Legal hold status(법적 보존 상태) – 잠긴 객체의 법적 보존 상태입니다.

  객체 잠금에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 객체 잠금 개요를 참조하십시오.

인벤토리 보고서의 내용에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 인벤토리에 포함된 항목은 무엇입니까? 단원을 참조하십시오.

d. Encryption에 대해 인벤토리 보고서를 암호화하기 위한 서버 측 암호화 옵션을 선택하거나 없음을 선택합니다.

- 없음 – 인벤토리 보고서를 암호화하지 않습니다.
- AES-256 – Amazon S3 관리형 키(SSE-S3)와 함께 서버 측 암호화를 사용하여 인벤토리 보고서를 암호화합니다. Amazon S3 서버 측 암호화는 256비트 고급 암호화 표준(AES-256)을 사용합니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 관리형 암호화 키(SSE-S3) 단원을 참조하십시오.
- AWS-KMS – AWS Key Management Service(AWS KMS) 고객 마스터 키(CMK)를 사용한 서버 측 암호화로 보고서를 암호화합니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 AWS KMS CMK를 참조하십시오.

  Note

  SSE-KMS를 사용하여 인벤토리 목록 파일을 암호화하려면 Amazon S3에 AWS KMS CMK 사용 권한을 부여해야 합니다. 자세한 내용은 Amazon S3에 AWS KMS CMK를 사용하여 암호화할 수 있는 권한 부여 (p. 103)를 참조하십시오.

7. Save를 선택합니다.

대상 버킷 정책

Amazon S3는 대상 버킷에서 Amazon S3 쓰기 권한을 부여하는 버킷 정책을 생성합니다. Amazon S3는 이를 통해 재고 보고서에 대한 데이터를 해당 버킷에 쓸 수 있습니다.

버킷 정책을 생성하는 동안 오류가 발생하는 경우, 해결 지침이 제시됩니다. 예를 들어, 다른 AWS 계정의 대상 버킷을 선택하는 바람에 해당 버킷 정책에 대한 읽기 및 쓰기 권한이 없는 경우, 다음과 같은 메시지가 나타납니다.

이 경우 대상 버킷 소유자는 표시된 버킷 정책을 대상 버킷에 추가해야 합니다. Amazon S3는 대상 버킷에 대한 쓰기 권한이 없기 때문에, 이 정책을 대상 버킷에 추가하지 않으면 인벤토리 보고서를 받을 수 없게 됩니다. 원본 버킷이 현재 사용자가 아닌 다른 계정의 소유물인 경우, 정책에서 원본 버킷의 올바른 계정 ID로 바꿔야 합니다.

자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 인벤토리 단원을 참조하십시오.

Amazon S3에 AWS KMS CMK를 사용하여 암호화할 수 있는 권한 부여

Amazon S3에 키 정책에 따라 AWS KMS CMK를 사용하여 암호화할 수 있는 권한을 부여해야 합니다. 다음 절차에서는 AWS Identity and Access Management(IAM) 콘솔을 사용하여 인벤토리 파일을 암호화하는 데 사용되는 AWS KMS CMK에 대한 키 정책을 수정하는 방법을 설명합니다.

AWS KMS CMK를 사용하여 암호화할 수 있는 권한을 부여하려면

1. AWS KMS CMK를 소유한 AWS 계정을 사용하여 AWS Management 콘솔에 로그인합니다. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 Encryption keys(암호화 키)를 선택합니다.
3. 리전에서 적절한 AWS 리전을 선택합니다. 탐색 모음(오른쪽 상단 모서리)에서 리전 선택기를 사용하지 마십시오.
4. 인벤토리를 암호화할 CMK의 별칭을 선택합니다.
5. 페이지의 Key Policy(키 정책) 섹션에서 Switch to policy view(정책 보기로 전환)를 선택합니다.
6. Key Policy(키 정책) 편집기를 사용하여 기존 정책에 다음 키 정책을 삽입한 다음 변경 사항 저장을 선택합니다. 기존 정책의 끝에 정책을 복사할 수도 있습니다.

```
{
    "Sid": "Allow Amazon S3 use of the key",
    "Effect": "Allow",
    "Principal": {
        "Service": "s3.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey*"
    ],
    "Resource": "*"
}
```

AWS KMS CMK 생성 및 편집에 대한 자세한 내용은 AWS Key Management Service Developer Guide의 시작하기 단원을 참조하십시오.

추가 정보

스토리지 관리 (p. 76)

요청 지표를 S3 버킷용으로 구성하려면 어떻게 해야 합니까?

Amazon S3에 대한 다음과 같은 세 가지 유형의 Amazon CloudWatch 지표가 있습니다.

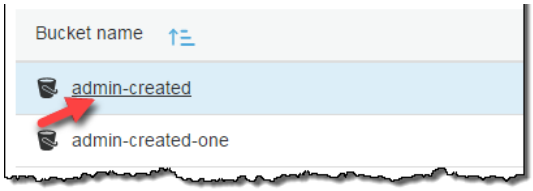
- 스토리지 지표는 하루에 한 번 보고되고 추가 비용 없이 모든 고객에게 제공됩니다.
- 복제 지표는 S3 Replication Time Control (S3 RTC)가 있는 복제 규칙을 활성화한 후 15분이 지나면 제공됩니다. 자세한 내용은 복제 지표를 보려면 어떻게 해야 합니까? (p. 108) 단원을 참조하십시오.
- 요청 지표는 약간의 처리 지연 시간 후에 1분 간격으로 제공되며, 표준 CloudWatch 요금으로 청구됩니다.

Amazon S3용 CloudWatch 지표에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon CloudWatch로 지표 모니터링을 참조하십시오.

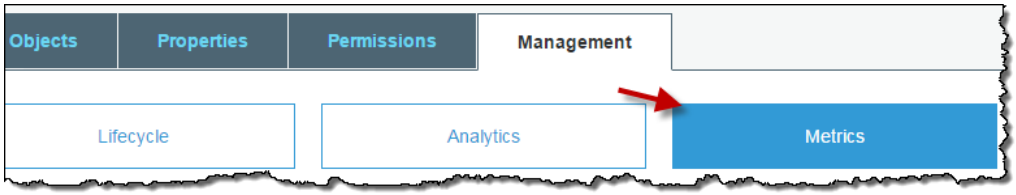
요청 지표를 획득하려면 AWS Management 콘솔에서 또는 Amazon S3 API를 사용해 요청 지표를 구성하여 지표를 선택해야 합니다.

버킷의 요청 지표 구성 방법

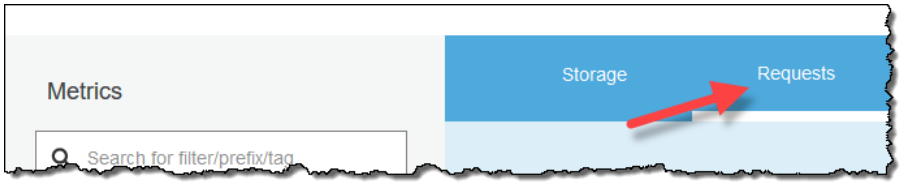
1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 요청 지표를 구성하려는 객체가 있는 버킷 이름을 선택합니다.



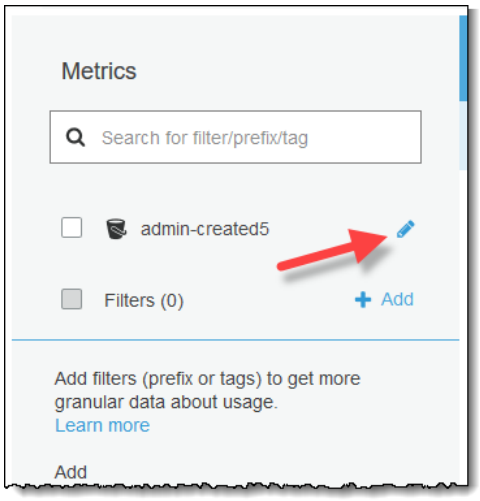
3. 관리 탭을 선택한 후 지표를 선택합니다.



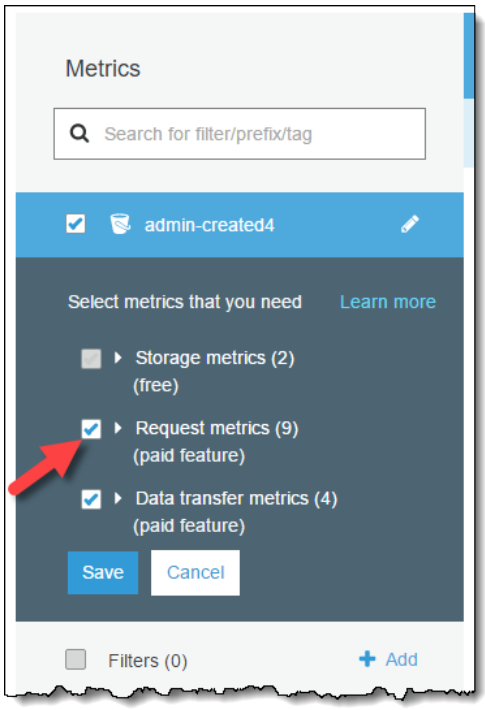
4. 요청을 선택합니다.



5. 왼쪽 창에서 버킷 이름 옆에 있는 편집 아이콘을 선택합니다.



6. 요청 지표 확인란을 선택합니다. 그러면 데이터 전송 지표도 활성화됩니다.



7. Save를 선택합니다.

이제 Amazon S3 버킷에 있는 모든 객체의 지표 구성을 생성했습니다. CloudWatch가 요청 지표 추적을 시작한 지 약 15분이 지나면 Amazon S3 또는 CloudWatch 콘솔에서 해당 지표의 그래프를 확인할 수 있습니다.

지표가 버킷의 객체 하위 세트에 대해서만 수집 및 보고되도록 필터를 정의할 수도 있습니다. 자세한 내용은 요청 지표 필터는 어떻게 구성합니까? (p. 105) 단원을 참조하십시오.

요청 지표 필터는 어떻게 구성합니까?

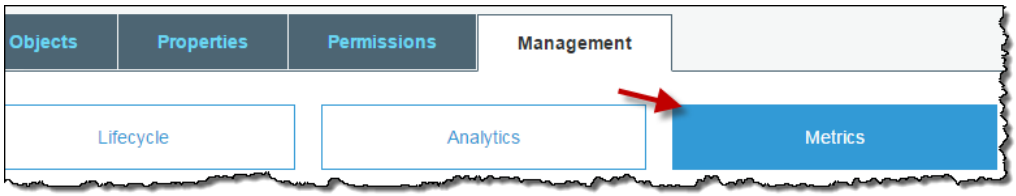
Amazon S3용 Amazon CloudWatch 지표에는 스토리지 지표, 요청 지표 및 복제 지표의 세 가지 유형이 있습니다. 스토리지 지표는 하루에 한 번 보고되고 추가 비용 없이 모든 고객에게 제공됩니다. 요청 지표는 약간의 처리 지연 시간 후에 1분 간격으로 제공되며, 표준 CloudWatch 환율로 청구됩니다. 요청 지표를 획득하려면 콘솔에서 혹은 Amazon S3 API를 통해 요청 지표를 구성하여 지표를 선택해야 합니다.

Amazon S3용 CloudWatch 지표에 대한 자세한 개념적 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon CloudWatch로 지표 모니터링 단원을 참조하십시오.

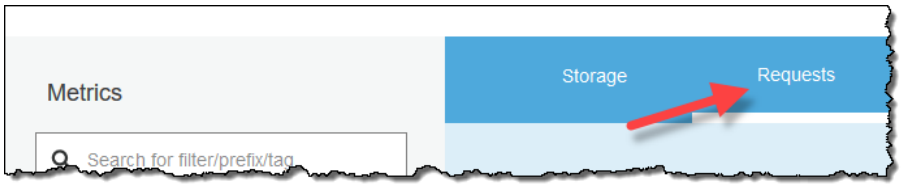
버킷에 있는 객체 하위 세트에 대한 요청 지표 필터링 방법

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서, 요청 지표를 획득하려는 객체가 있는 버킷 이름을 선택합니다.

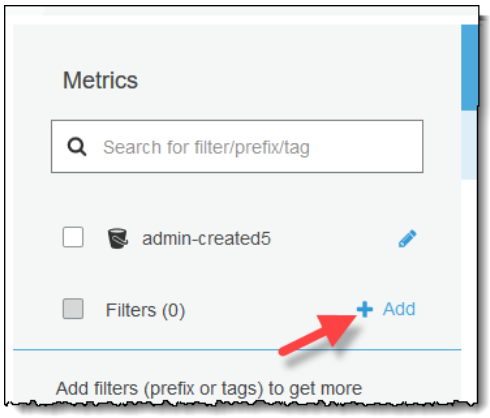
3. 관리 탭을 선택한 후 지표를 선택합니다.



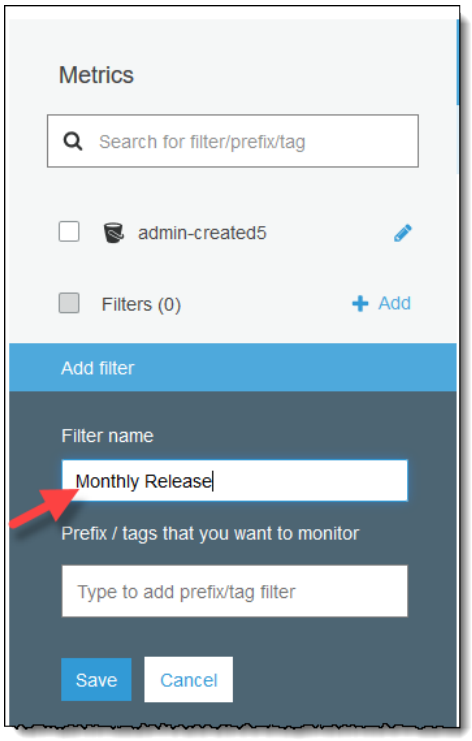
4. 요청을 선택합니다.



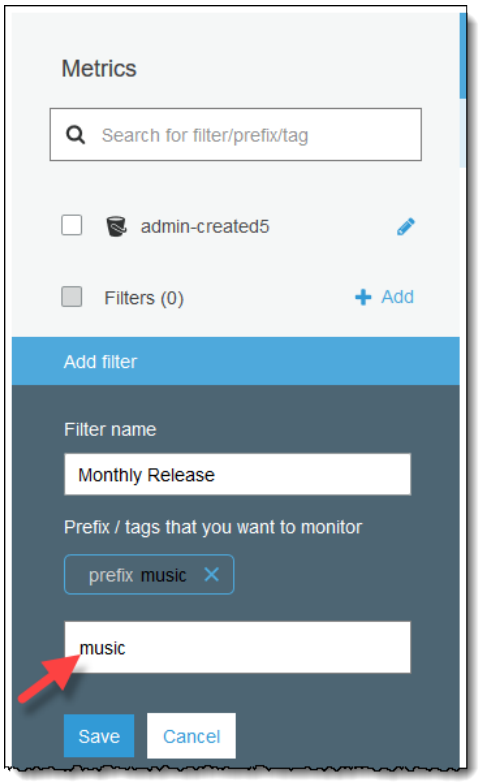
5. 왼쪽 탐색 창의 필터에서 추가를 선택합니다.



6. 이 지표 구성의 이름을 작성합니다.



7. Prefix /tags that you want to monitor(모니터링하기 원하는 접두사 /태그)에서 쉼표로 구분되는 하나 이상의 접두사 또는 태그를 작성합니다. 드롭다운 메뉴에서 좀 전에 작성한 값이 태그인지 혹은 접두사인지 선택합니다.



8. Save를 선택합니다.

이제 Amazon S3 버킷에 있는 객체 하위 세트에 대한 요청 지표의 지표 구성을 생성했습니다. CloudWatch가 요청 지표 추적을 시작한 지 약 15분이 지나면 Amazon S3 또는 CloudWatch 콘솔에서 해당 지표의 그래프를 확인할 수 있습니다. 버킷 수준에서도 지표를 요청할 수 있습니다. 자세한 정보는 요청 지표를 S3 버킷용으로 구성하려면 어떻게 해야 합니까? (p. 103) 단원을 참조하십시오.

복제 지표를 보려면 어떻게 해야 합니까?

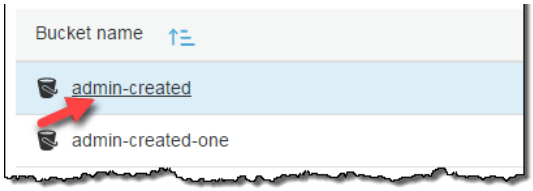
Amazon S3용 Amazon CloudWatch 지표에는 스토리지 지표, 요청 지표 및 복제 지표의 세 가지 유형이 있습니다. 복제 지표는 S3 Replication Time Control (S3 RTC)가 있는 복제 규칙이 활성화된 후 15분이 지나면 제공됩니다. 복제 지표는 표준 Amazon CloudWatch 요금으로 청구됩니다. AWS Management 콘솔 또는 Amazon S3 API를 사용하여 S3 RTC가 있는 복제를 활성화하면 자동으로 활성화됩니다.

복제 지표는 복제 구성의 규칙 ID를 추적합니다. 복제 규칙 ID는 접두사, 태그 또는 둘의 조합에 대해 고유할 수 있습니다. S3 Replication Time Control (S3 RTC)에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 S3 Replication Time Control(S3 RTC)을 사용하여 객체 복제를 참조하십시오.

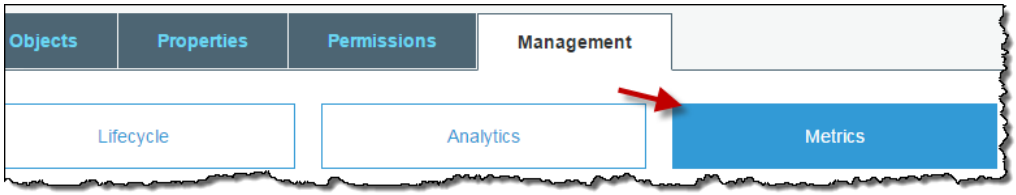
Amazon S3용 CloudWatch 지표에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon CloudWatch로 지표 모니터링을 참조하십시오.

복제 지표를 보려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 복원 지표를 보려는 객체가 들어 있는 버킷 이름을 선택합니다.

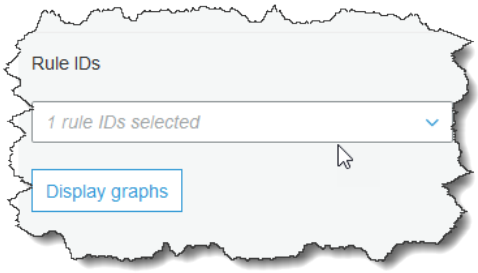


3. 관리 탭을 선택한 후 지표를 선택합니다.



4. 복제를 선택합니다.
복제 옵션을 보여주는 콘솔 스크린샷
5. 왼쪽 창의 규칙 ID 목록에서 원하는 규칙 ID를 선택합니다. 선택할 규칙 ID가 여러 개인 경우 원하는 ID를 검색할 수 있습니다.

6. 원하는 규칙 ID를 선택한 후 규칙 ID 선택 상자 아래에 그래프 표시를 선택합니다.



그런 다음 선택한 규칙에 대한 복제 지표 복제 대기 시간(초), 복제 보류 중인 작업 및 복제 보류 바이트를 볼 수 있습니다. Amazon CloudWatch는 각 복제 규칙에서 S3 RTC를 활성화한 후 15분이 지나면 복제 지표 보고를 시작합니다. Amazon S3 또는 CloudWatch 콘솔에서 복제 지표를 볼 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 복제 지표를 사용하여 복제 구성 모니터링을 참조하십시오.

버킷 및 객체 액세스 권한 설정

이 단원에서는 Amazon Simple Storage Service(Amazon S3) 콘솔을 사용하여 버킷과 객체에 액세스 권한을 부여하는 방법에 대해 설명합니다. Amazon S3 퍼블릭 액세스 차단을 사용해 S3 버킷 내에서 데이터에 대한 퍼블릭 액세스를 허용하는 모든 설정의 적용을 차단하는 방법도 설명합니다.

버킷 및 객체는 Amazon S3 리소스입니다. 리소스 기반 액세스 정책을 사용하여 버킷과 객체에 액세스 권한을 부여합니다. 액세스 정책을 리소스와 연결할 수 있습니다. 액세스 정책은 리소스에 액세스할 수 있는 대상을 설명합니다. 리소스 소유자는 리소스를 생성한 AWS 계정입니다. 리소스 소유권과 액세스 정책에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 액세스 관리 개요 단원을 참조하십시오.

버킷 액세스 권한을 통해 버킷의 객체에 액세스할 수 있는 사용자와 그러한 사용자가 갖는 액세스 유형을 지정할 수 있습니다. 객체 액세스 권한을 통해 객체에 액세스할 수 있는 사용자와 그러한 사용자가 갖는 액세스 유형을 지정할 수 있습니다. 예를 들어, 어떤 사용자는 읽기 권한만 갖고, 다른 사용자는 읽기 및 쓰기 권한을 가질 수 있습니다.

버킷 및 객체 권한은 서로 독립적입니다. 객체는 해당 버킷으로부터 권한을 상속하지 않습니다. 예를 들어, 버킷을 만들고 사용자에게 쓰기 액세스 권한을 부여하는 경우 사용자로부터 명시적으로 권한을 부여 받지 않는 한 해당 사용자의 객체에 액세스할 수 없습니다.

다른 AWS 계정 및 일반 사용자에게 버킷과 객체에 대한 액세스 권한을 부여하려면, 액세스 통제 목록(ACL)이라는 리소스 기반 액세스 정책을 사용합니다.

버킷 정책은 다른 AWS 계정 또는 IAM 사용자에게 S3 버킷에 대한 액세스 권한을 부여하는 리소스 기반 AWS Identity and Access Management(IAM) 정책입니다. 버킷 정책은 ACL 기반 액세스 정책을 보완하며 대부분의 경우 액세스 정책을 대신합니다. Amazon S3에서 IAM 사용에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 리소스에 대한 액세스 권한 관리 단원을 참조하십시오.

액세스 권한 관리에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 리소스에 대한 액세스 권한 관리 소개 단원을 참조하십시오.

이 단원에서는 Amazon S3 콘솔을 사용하여 S3 버킷에 cross-origin 리소스 공유(CORS) 구성을 추가하는 방법도 설명합니다. CORS는 한 도메인에서 로드되어 다른 도메인에 있는 리소스와 상호 작용하는 클라이언트 웹 애플리케이션을 허용합니다.

주제

S3 버킷에 대한 퍼블릭 액세스를 어떻게 차단합니까?

Amazon S3 퍼블릭 액세스 차단은 S3 버킷 내에서 데이터에 대한 퍼블릭 액세스를 허용하는 모든 설정의 적용을 차단합니다. 개별 S3 버킷 또는 계정의 모든 버킷에 대한 퍼블릭 액세스 차단 설정을 구성할 수 있습니다. AWS CLI, AWS SDK 및 Amazon S3 REST API를 사용하여 퍼블릭 액세스를 차단하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드에서 Amazon S3 퍼블릭 액세스 차단 사용을 참조하십시오.

다음 주제에서는 Amazon S3 콘솔을 사용하여 퍼블릭 액세스 차단 설정을 구성하는 방법을 살펴봅니다.

- S3 버킷에 대한 퍼블릭 액세스 설정을 어떻게 편집합니까? (p. 112)
- AWS 계정의 모든 S3 버킷에 대한 퍼블릭 액세스 설정을 어떻게 편집합니까? (p. 114)

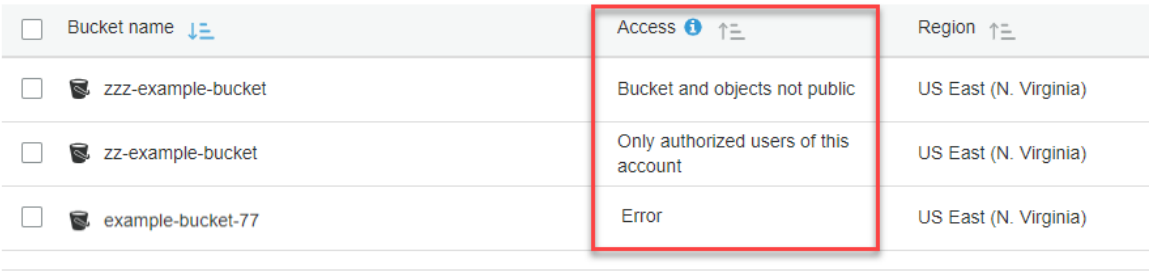
다음 섹션에서는 버킷 액세스 상태 보기 및 액세스 유형별 검색에 대해 설명합니다.

액세스 상태 보기

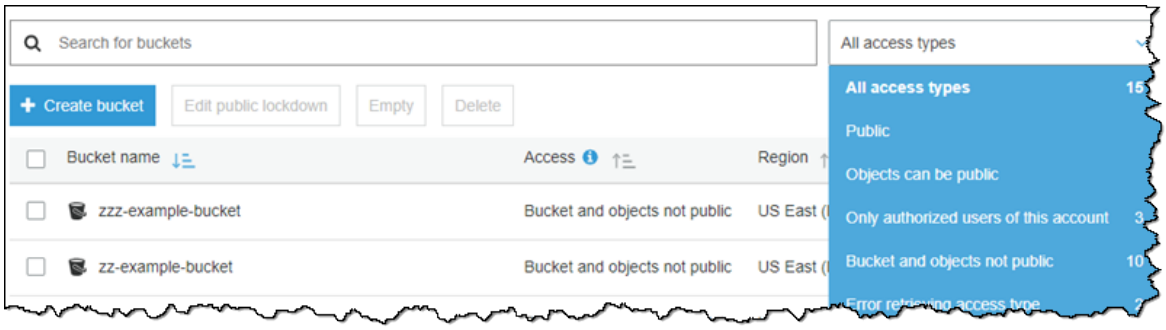
버킷 나열 보기에 버킷이 공개 액세스 가능한지 여부가 표시됩니다. Amazon S3에서는 버킷에 대한 권한을 다음과 같이 표시합니다.

- 퍼블릭 – 누구나 객체 목록 생성, 객체 쓰기, 읽기 및 쓰기 권한 중 하나 이상에 액세스할 수 있습니다.
- 객체는 퍼블릭일 수 있음 –버킷은 퍼블릭이 아니지만 적절한 권한이 있는 사람은 객체에 퍼블릭 액세스 권한을 부여할 수 있습니다.
- 버킷과 객체는 퍼블릭이 아님 – 버킷 및 객체에는 퍼블릭 액세스가 없습니다.
- 이 계정의 권한 있는 사용자만 – 퍼블릭 액세스를 부여하는 정책이 있기 때문에, 액세스는 이 계정과 AWS 서비스 보안 주체의 IAM 사용자 및 역할로 격리됩니다.

액세스 열에는 나열된 버킷의 액세스 상태가 표시됩니다.



액세스 유형별로 버킷 검색을 필터링할 수도 있습니다. 버킷 검색 막대 옆에 있는 드롭다운 목록에서 액세스 유형을 선택하십시오.



추가 정보

- S3 버킷에 대한 퍼블릭 액세스 설정을 어떻게 편집합니까? (p. 112)
- AWS 계정의 모든 S3 버킷에 대한 퍼블릭 액세스 설정을 어떻게 편집합니까? (p. 114)
- 버킷 및 객체 액세스 권한 설정 (p. 110)

S3 버킷에 대한 퍼블릭 액세스 설정을 어떻게 편집합니까?

Amazon S3 퍼블릭 액세스 차단은 S3 버킷 내에서 데이터에 대한 퍼블릭 액세스를 허용하는 모든 설정의 적용을 차단합니다. 이 단원에서는 하나 이상의 S3 버킷에 대한 퍼블릭 액세스 차단 설정을 편집하는 방법에 대해 설명합니다. AWS CLI, AWS SDK 및 Amazon S3 REST API를 사용하여 퍼블릭 액세스를 차단하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드에서 Amazon S3 퍼블릭 액세스 차단 사용을 참조하십시오.

주제

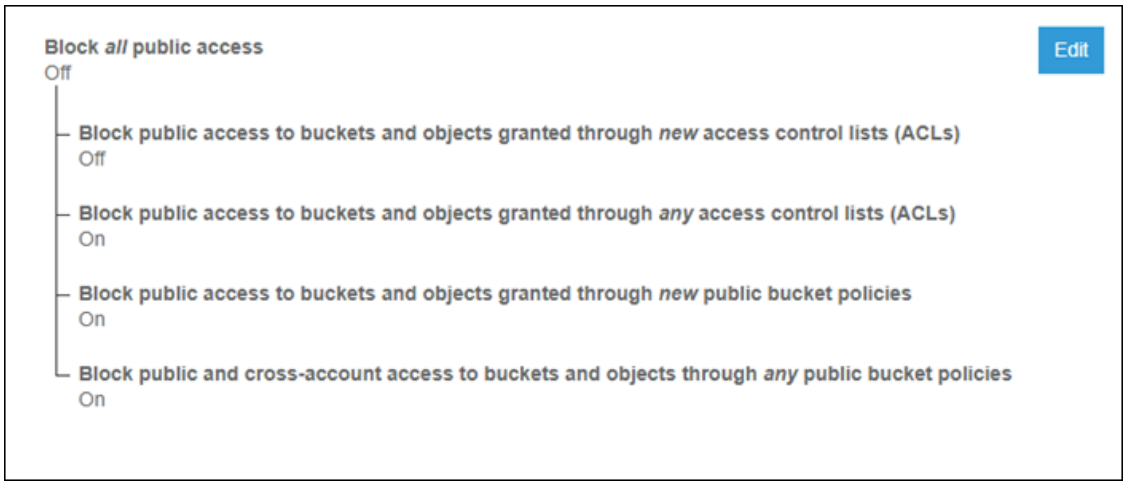
S3 버킷의 퍼블릭 액세스 설정을 편집하는 방법

단일 S3 버킷에 대한 퍼블릭 액세스 설정을 변경해야 하는 경우 다음 단계를 따르십시오.

S3 버킷의 Amazon S3 퍼블릭 액세스 차단 설정을 편집하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 원하는 버킷의 이름을 선택합니다.

3. Permissions를 선택합니다.
4. 버킷의 퍼블릭 액세스 설정을 변경하려면 편집을 선택하십시오. 4가지 Amazon S3 퍼블릭 액세스 차단 설정에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 퍼블릭 액세스 차단 설정을 참조하십시오.



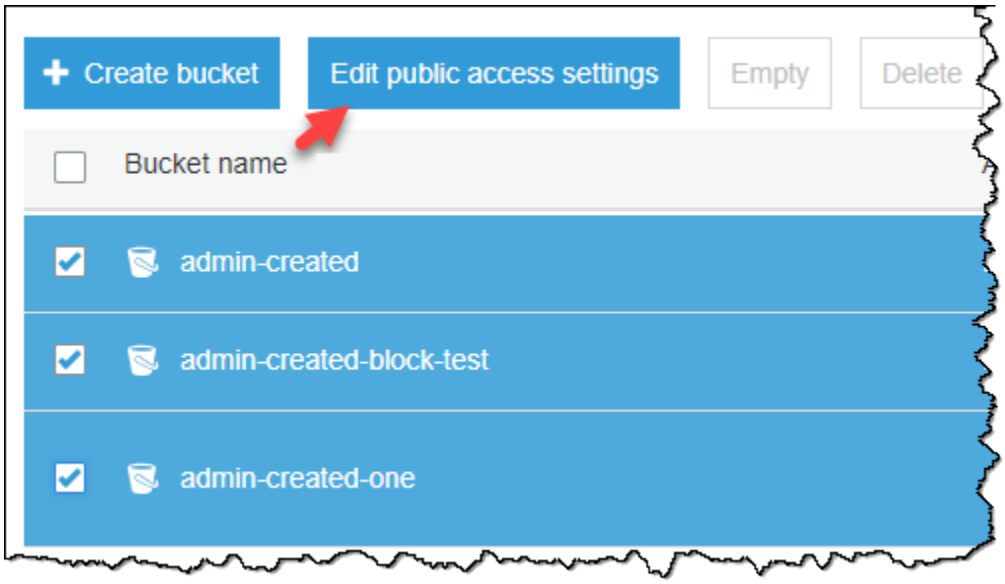
5. 변경할 설정을 선택한 다음 저장을 선택합니다.
6. 확인 메시지가 표시되면 **`confirm`**을 입력합니다. 그런 다음확인을 선택해 변경 사항을 저장합니다.

여러 S3 버킷의 퍼블릭 액세스 설정을 편집하는 방법

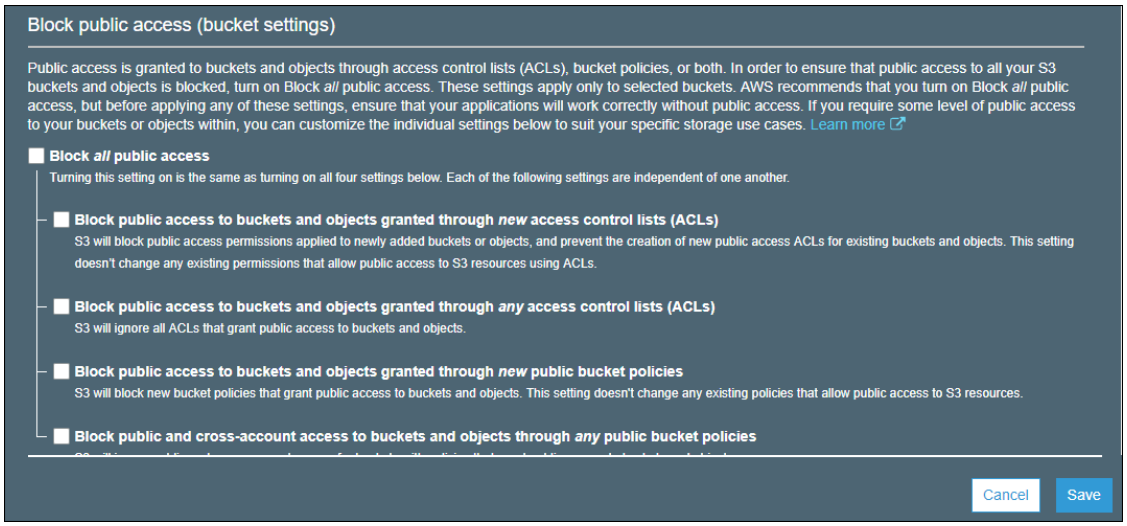
둘 이상의 S3 버킷에 대한 퍼블릭 액세스 설정을 변경해야 하는 경우 다음 단계를 따르십시오.

여러 S3 버킷의 Amazon S3 퍼블릭 액세스 차단 설정을 편집하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 원하는 버킷을 선택한 다음 Edit public access settings(퍼블릭 액세스 설정 편집)를 선택하십시오.



3. 변경할 설정을 선택한 다음 저장을 선택합니다.



4. 확인 메시지가 표시되면 **`confirm`**을 입력합니다. 그런 다음확인을 선택해 변경 사항을 저장합니다.

버킷을 생성할 때 Amazon S3 퍼블릭 액세스 차단 설정을 변경할 수 있습니다. 자세한 내용은 S3 버킷을 생성하려면 어떻게 해야 합니까? (p. 3) 단원을 참조하십시오.

추가 정보

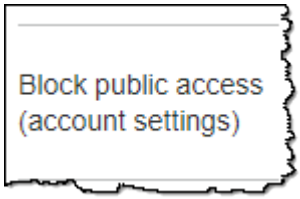
- S3 버킷에 대한 퍼블릭 액세스를 어떻게 차단합니까? (p. 110)
- AWS 계정의 모든 S3 버킷에 대한 퍼블릭 액세스 설정을 어떻게 편집합니까? (p. 114)
- 버킷 및 객체 액세스 권한 설정 (p. 110)

AWS 계정의 모든 S3 버킷에 대한 퍼블릭 액세스 설정을 어떻게 편집합니까?

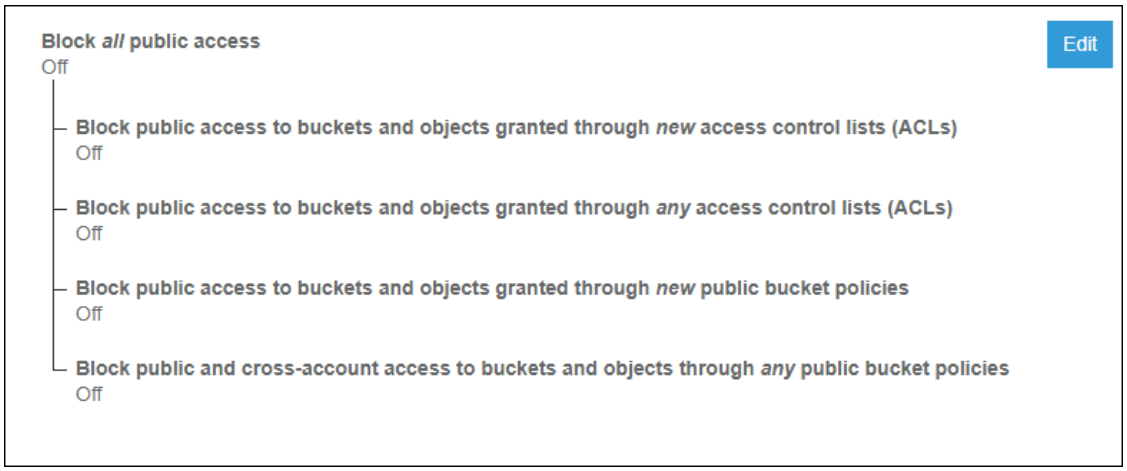
Amazon S3 퍼블릭 액세스 차단은 S3 버킷 내에서 데이터에 대한 퍼블릭 액세스를 허용하는 모든 설정의 적용을 차단합니다. 이 단원에서는 AWS 계정의 모든 S3 버킷에 대한 퍼블릭 액세스 차단 설정을 편집하는 방법에 대해 설명합니다. AWS CLI, AWS SDK 및 Amazon S3 REST API를 사용하여 퍼블릭을 차단하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드에서 Amazon S3 퍼블릭 액세스 차단 사용을 참조하십시오.

AWS 계정의 모든 S3 버킷에 대한 퍼블릭 액세스 차단 설정을 편집하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. Block public access (account settings)(퍼블릭 액세스 차단(계정 설정))을 선택합니다.



3. AWS 계정의 모든 버킷에 대한 퍼블릭 액세스 차단 설정을 변경하려면 편집을 선택합니다.



4. 변경할 설정을 선택한 다음 저장을 선택합니다.
5. 확인 메시지가 표시되면 **confirm**을 입력합니다. 그런 다음확인을 선택해 변경 사항을 저장합니다.

추가 정보

- S3 버킷에 대한 퍼블릭 액세스를 어떻게 차단합니까? (p. 110)
- S3 버킷에 대한 퍼블릭 액세스 설정을 어떻게 편집합니까? (p. 112)
- 버킷 및 객체 액세스 권한 설정 (p. 110)

객체에 대한 권한은 어떻게 설정하나요?

이 단원에서는 Amazon Simple Storage Service(Amazon S3) 콘솔에서 ACL(액세스 제어 목록)을 사용하여 Amazon S3 객체에 대한 액세스 권한을 관리하는 방법을 설명합니다. ACL은 버킷과 객체에 액세스 권한을 부여하는 리소스 기반 액세스 정책입니다. 리소스 기반 정책으로 액세스 권한을 관리하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 액세스 관리 개요 단원을 참조하십시오.

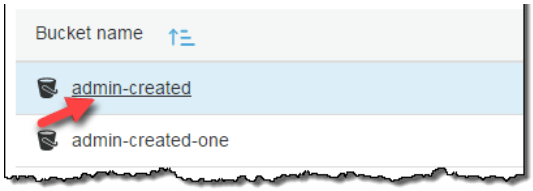
버킷 및 객체 권한은 서로 독립적입니다. 객체는 해당 버킷으로부터 권한을 상속하지 않습니다. 예를 들어, 버킷을 만들고 사용자에게 쓰기 액세스 권한을 부여하는 경우 사용자로부터 명시적으로 권한을 부여 받지 않는 한 해당 사용자의 객체에 액세스할 수 없습니다.

다른 AWS 계정이나 사전 정의된 그룹에 권한을 부여할 수 있습니다. 권한을 부여하는 사용자 또는 그룹을 피부여자라고 합니다. 기본적으로 소유자, 즉 버킷을 만든 AWS 계정에는 모든 권한이 있습니다.

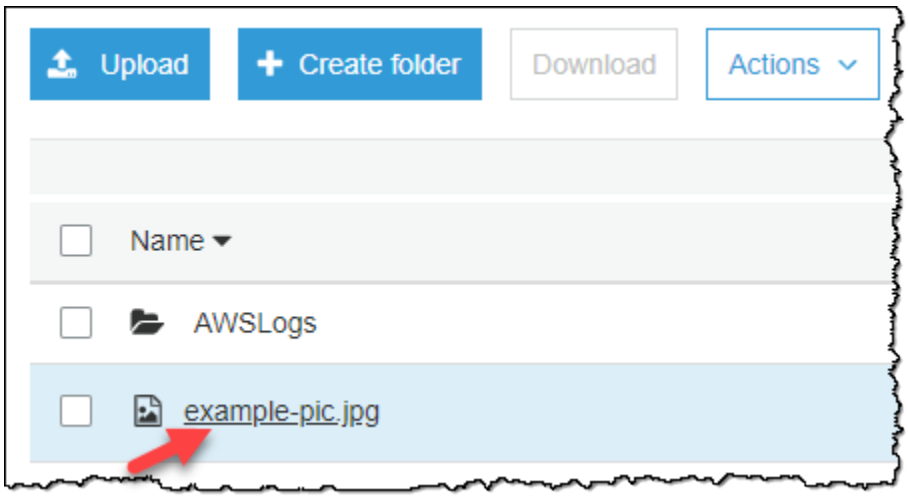
사용자 또는 그룹에 부여하는 각 권한에 대해 객체와 연결된 ACL에 항목이 추가됩니다. ACL은 피부여자와 그에 부여된 권한을 식별하는 권한 부여를 나열합니다. ACL에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 ACL을 사용한 액세스 관리 단원을 참조하십시오.

객체에 대한 권한을 설정하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 객체가 포함된 버킷의 이름을 선택합니다.



3. 이름 목록에서 권한을 설정하려는 객체의 이름을 선택합니다.



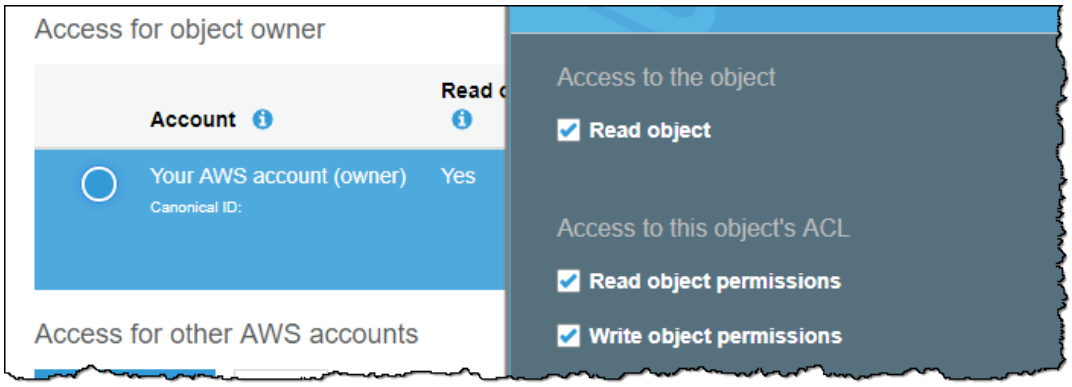
4. Permissions를 선택합니다.
5. 다음에 대한 객체 액세스 권한을 관리할 수 있습니다.

   a. 객체 소유자의 액세스

      소유자란 AWS Identity and Access Management(IAM) 사용자가 아닌 AWS 계정 루트 사용자를 지칭합니다. 루트 사용자에 대한 자세한 내용은 IAM 사용 설명서의 AWS 계정 루트 사용자 단원을 참조하십시오.

      소유자의 객체 액세스 권한을 변경하려면 Access for object owner(객체 소유자 액세스)에서 AWS 계정(소유자)을 선택하십시오.

      변경하려는 권한에 대한 확인란을 선택한 다음, 저장을 선택합니다.

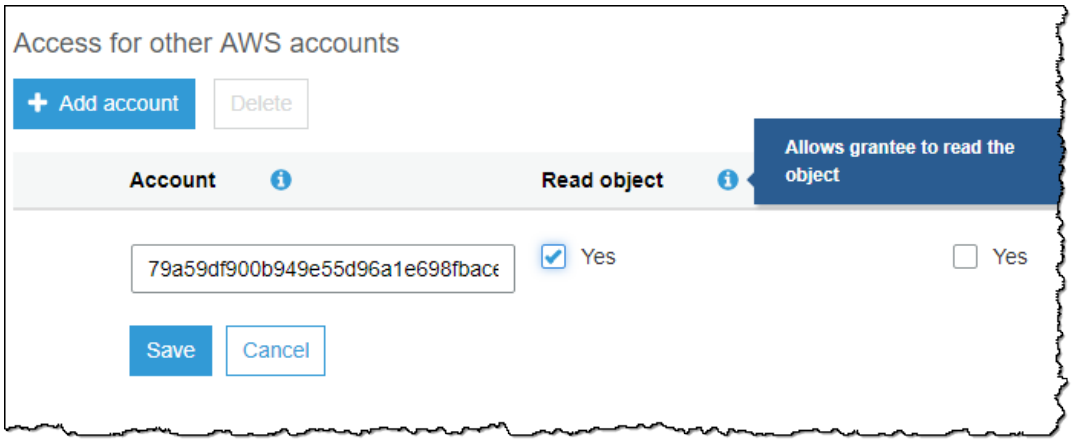


   b. 다른 AWS 계정에 대한 액세스

      다른 AWS 계정의 AWS 사용자에게 권한을 부여하려면 다른 AWS 계정에 대한 액세스 아래에서 계정 추가를 선택합니다. Enter an ID(ID 입력) 필드에 객체 권한을 부여할 AWS 사용자의 정식 ID를

입력합니다. 정식 ID를 찾는 방법에 대한 자세한 내용은 Amazon Web Services 일반 참조의 AWS 계정 식별자 단원을 참조하십시오. 사용자는 최대 99명까지 추가할 수 있습니다.

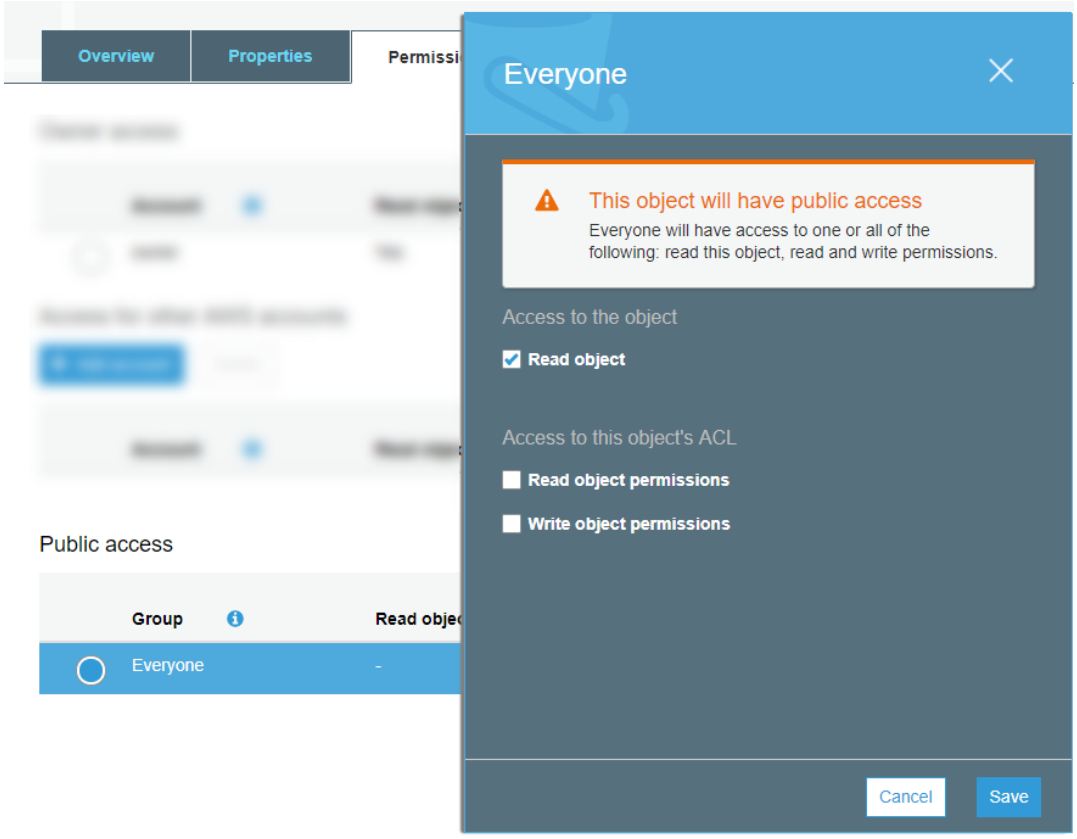
사용자에게 부여할 권한의 확인란을 선택한 다음, 저장을 선택합니다. 권한에 대한 정보를 표시하려면 도움말 아이콘을 선택합니다.



c. 퍼블릭 액세스

일반 대중(전 세계 모든 사람)에게 객체 액세스 권한을 부여하려면 퍼블릭 액세스에서 모든 사람을 선택합니다. 퍼블릭 액세스 권한을 부여한다는 것은 전 세계 누구든 객체에 액세스할 수 있다는 뜻입니다.

부여하려는 권한에 대한 확인란을 선택한 다음, 저장을 선택합니다.



Warning

Amazon S3 객체에 모든 사람 그룹에 익명 액세스 권한을 부여할 때 주의하십시오. 이 그룹에 대해 액세스 권한을 부여하면 전 세계 누구나 객체에 액세스할 수 있습니다. 모두에게 액세스 권한을 부여해야 하는 경우, Read objects(객체 읽기)에 대한 권한만 부여하는 것이 좋습니다.
모든 사람 그룹에 객체 쓰기 권한을 부여하지 않는 것이 좋습니다. 이렇게 하면 누구든지 객체에 대한 ACL 권한을 덮어쓸 수 있습니다.

객체를 업로드할 때 객체 권한을 설정할 수도 있습니다. 객체를 업로드할 때 권한을 설정하는 방법에 대한 자세한 내용은 S3 버킷에 파일 및 폴더를 업로드하려면 어떻게 해야 합니까? (p. 34) 단원을 참조하십시오.

추가 정보

- 버킷 및 객체 액세스 권한 설정 (p. 110)
- ACL 버킷 권한을 설정하려면 어떻게 해야 합니까? (p. 118)

ACL 버킷 권한을 설정하려면 어떻게 해야 합니까?

이 단원에서는 Amazon Simple Storage Service(Amazon S3) 콘솔에서 ACL(액세스 제어 목록)을 사용하여 S3 버킷에 대한 액세스 권한을 관리하는 방법을 설명합니다. ACL은 버킷과 객체에 액세스 권한을 부여하는 리소스 기반 액세스 정책입니다. 리소스 기반 정책으로 액세스 권한을 관리하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 액세스 관리 개요 단원을 참조하십시오.

다른 AWS 계정 사용자나 사전 정의된 그룹에 권한을 부여할 수 있습니다. 권한을 부여하는 사용자 또는 그룹을 피부여자라고 합니다. 기본적으로 소유자, 즉 버킷을 만든 AWS 계정에는 모든 권한이 있습니다.

사용자 또는 그룹에 부여하는 각 권한에 대해 버킷과 연결된 ACL에 항목이 추가됩니다. ACL은 피부여자와 그에 부여된 권한을 식별하는 권한 부여를 나열합니다. ACL에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 ACL을 사용한 액세스 관리 단원을 참조하십시오.

S3 버킷에 대한 ACL 액세스 권한을 설정하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 권한을 설정하려는 버킷의 이름을 선택합니다.

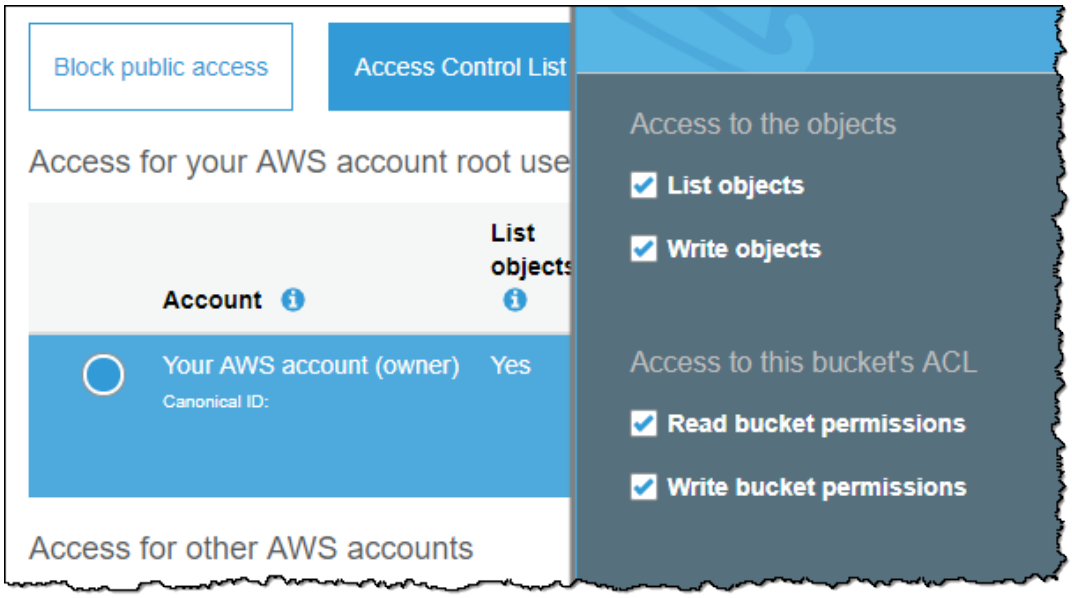
3. 권한을 선택한 다음 액세스 제어 목록을 선택합니다.
4. 다음에 대한 버킷 액세스 권한을 관리할 수 있습니다.

   a. AWS 계정 루트 사용자의 액세스

      소유자란 AWS Identity and Access Management(IAM) 사용자가 아닌 AWS 계정 루트 사용자를 지칭합니다. 루트 사용자에 대한 자세한 내용은 IAM 사용 설명서의 AWS 계정 루트 사용자 단원을 참조하십시오.

소유자의 버킷 액세스 권한을 변경하려면 Access for your AWS accounted root user(AWS 계정 루트 사용자의 액세스)에서 AWS 계정(소유자)을 선택하십시오.

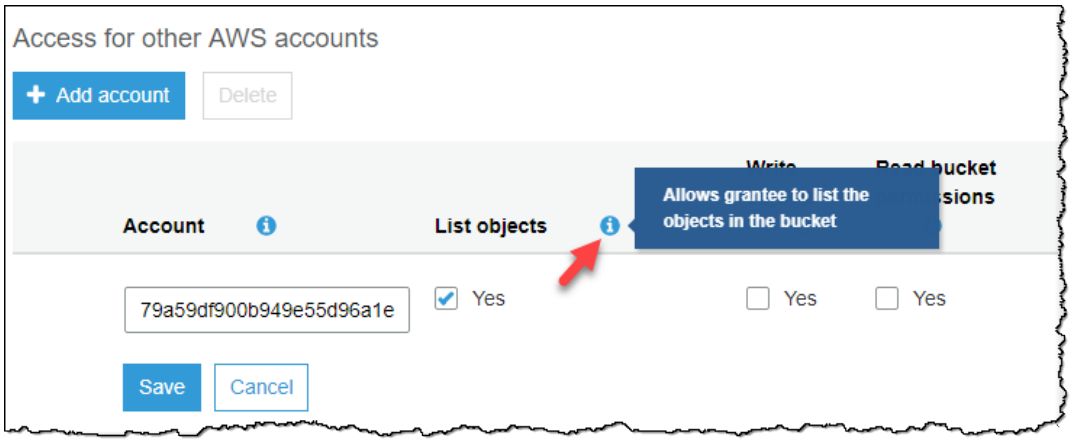
변경하려는 권한에 대한 확인란을 선택한 다음, 저장을 선택합니다.



b. 다른 AWS 계정에 대한 액세스

다른 AWS 계정의 AWS 사용자에게 권한을 부여하려면 다른 AWS 계정에 대한 액세스 아래에서 계정 추가를 선택합니다. Enter an ID(ID 입력) 필드에 버킷 권한을 부여할 AWS 사용자의 정식 ID를 입력합니다. 정식 ID를 찾는 방법에 대한 자세한 내용은 Amazon Web Services 일반 참조의 AWS 계정 식별자 단원을 참조하십시오. 사용자는 최대 99명까지 추가할 수 있습니다.

사용자에게 부여할 권한 옆의 확인란을 선택한 다음, 저장을 선택합니다. 권한에 대한 정보를 표시하려면 도움말 아이콘을 선택합니다.



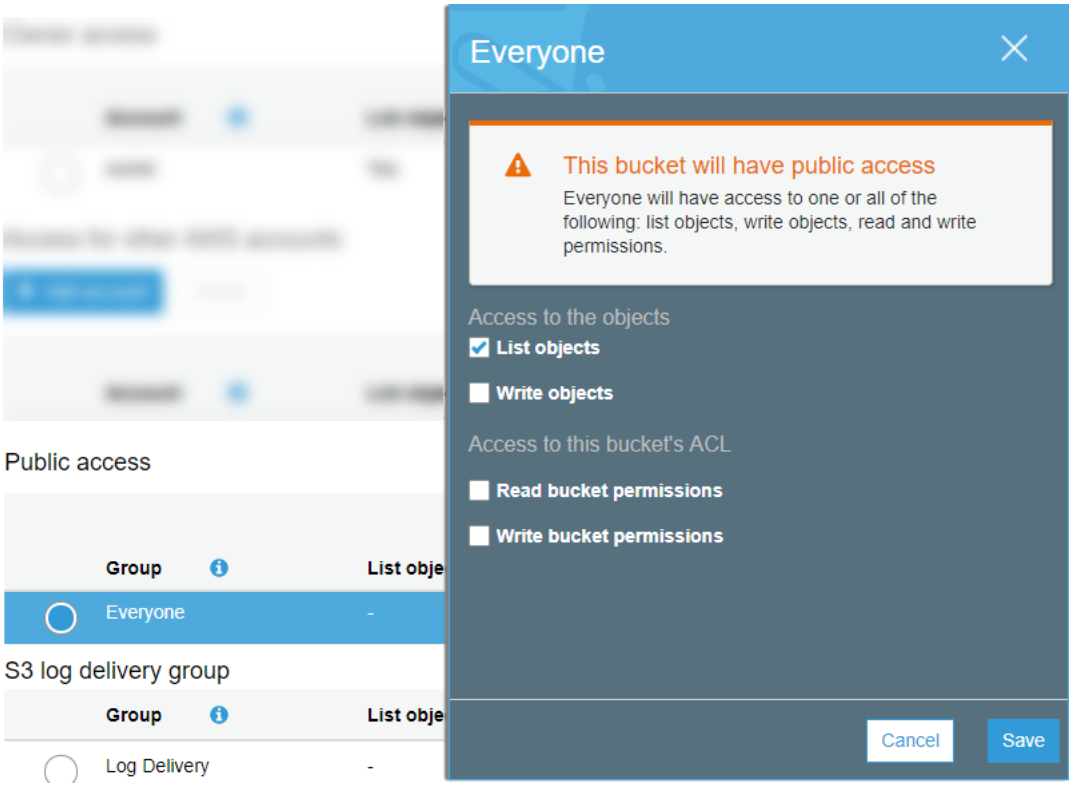
Warning

다른 AWS 계정에 본인의 리소스 액세스를 허용하는 경우, AWS 계정이 자신의 계정에 속한 사용자에게 그 권한을 위임할 수도 있다는 사실을 염두에 두어야 합니다. 이것을 교차 계정 액세스라고 합니다. 교차 계정 액세스를 사용하는 자세한 방법은 IAM 사용 설명서의 역할을 만들어 IAM 사용자에게 권한 위임 단원을 참조하십시오.

c. 퍼블릭 액세스

일반 대중(전 세계 모든 사람)에게 버킷 액세스 권한을 부여하려면 퍼블릭 액세스에서 모든 사람을 선택합니다. 퍼블릭 액세스 권한을 부여한다는 것은 전 세계 누구든 버킷에 액세스할 수 있다는 뜻입니다. 부여하려는 권한에 대한 확인란을 선택한 다음, 저장을 선택합니다.

버킷에 대한 퍼블릭 액세스를 실행 취소하려면 퍼블릭 액세스에서 모든 사람을 선택합니다. 모든 권한 확인란의 선택을 취소한 다음 저장을 선택합니다.



Warning

S3 버킷에 모든 사람 그룹 퍼블릭 액세스 권한을 부여할 때 주의하십시오. 이 그룹에 액세스 권한을 부여하면 전 세계 누구나 버킷에 액세스할 수 있습니다. S3 버킷에 대한 퍼블릭 쓰기 액세스 권한을 부여하지 않는 것이 좋습니다.

d. S3 로그 전달 그룹

버킷에 서버 액세스 로그를 기록하도록 Amazon S3에 액세스 권한을 부여하려면 S3 로그 전달 그룹을 선택한 다음, 로그 전달을 선택합니다.

버킷이 액세스 로그를 수신할 대상 버킷으로 설정되면 버킷 권한을 통해 로그 전달 그룹에게 버킷에 대한 쓰기 액세스 권한을 허용해야 합니다. 버킷에서 서버 액세스 로깅을 활성화하면 로그 수신을 위해 선택한 대상 버킷에서 Amazon S3 콘솔이 로그 전달 그룹에게 쓰기 액세스 권한을 부여합니다. 서버 액세스 로깅에 대한 자세한 내용은 S3 버킷에 대한 서버 액세스 로깅을 활성화하려면 어떻게 해야 합니까? (p. 11) 단원을 참조하십시오.

버킷을 생성할 때 버킷 권한을 설정할 수도 있습니다. 객체를 생성할 때 권한을 설정하는 방법에 대한 자세한 내용은 S3 버킷을 생성하려면 어떻게 해야 합니까? (p. 3) 단원을 참조하십시오.

추가 정보

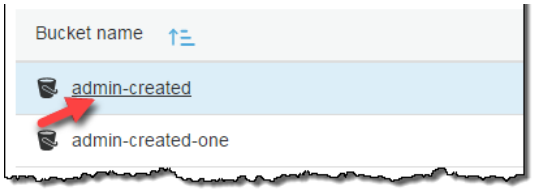
S3 버킷 정책을 추가하려면 어떻게 해야 합니까?

이 단원에서는 Amazon Simple Storage Service(Amazon S3) 콘솔을 사용하여 새 버킷 정책을 추가하거나 기존 버킷 정책을 편집하는 방법을 설명합니다. 버킷 정책은 리소스 기반 AWS Identity and Access Management(IAM) 정책입니다. 다른 AWS 계정이나 IAM 사용자에게 버킷과 버킷에 포함된 객체에 대한 액세스 권한을 부여하는 버킷 정책을 버킷에 추가할 수 있습니다. 객체 권한은 해당 버킷 소유자가 생성하는 객체에만 적용됩니다. 버킷 정책에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 액세스 관리 개요 단원을 참조하십시오.

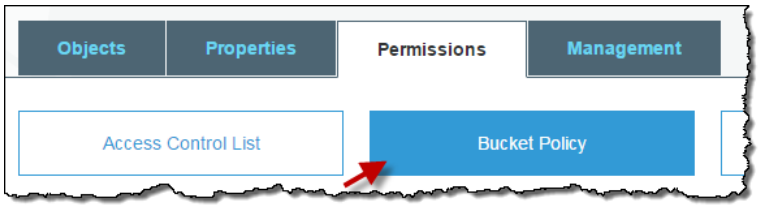
Amazon S3 버킷 정책에 대한 예제는 Amazon Simple Storage Service 개발자 가이드의 버킷 정책 예제를 참조하십시오.

버킷 정책을 만들거나 편집하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름목록에서 버킷 정책을 만들 버킷 이름 또는 버킷 정책을 편집할 버킷 이름을 선택합니다.



3. 권한을 선택하고 버킷 정책을 선택합니다.



4. 버킷 정책 편집기 텍스트 상자에 새 버킷 정책을 입력하거나 복사하여 붙여넣거나, 기존 정책을 편집합니다. 버킷 정책은 JSON 파일입니다. 편집기에 입력하는 텍스트는 유효한 JSON이어야 합니다.

5. Save를 선택합니다.

   Note

   Amazon S3는 버킷 정책 편집기 제목 옆에 버킷의 Amazon 리소스 이름(ARN)을 표시합니다. ARN에 대한 자세한 내용은 Amazon Web Services 일반 참조의 Amazon 리소스 이름(ARN) 및 AWS 서비스 네임스페이스 단원을 참조하십시오.
   버킷 정책 편집기 텍스트 상자 바로 아래의 정책 생성기 링크를 사용하여 버킷 정책을 만들 수 있습니다.

추가 정보

- 버킷 및 객체 액세스 권한 설정 (p. 110)
- ACL 버킷 권한을 설정하려면 어떻게 해야 합니까? (p. 118)

CORS와의 교차 도메인 리소스 공유를 추가하려면 어떻게 해야 합니까?

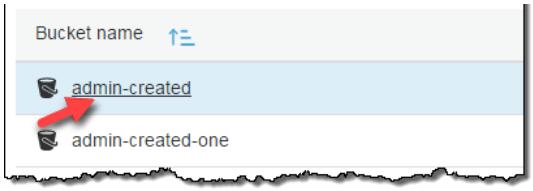
이 단원에서는 Amazon S3 콘솔을 사용하여 S3 버킷에 cross-origin 리소스 공유(CORS) 구성을 추가하는 방법을 설명합니다. CORS는 한 도메인에서 로드되어 다른 도메인에 있는 리소스와 상호 작용하는 클라이언트 웹 애플리케이션을 허용합니다.

cross-origin 요청을 허용하도록 버킷을 구성하려면 해당 버킷에 CORS 구성을 추가합니다. CORS 구성은 버킷에 대한 액세스를 허용할 오리진과 각 오리진에 대해 지원되는 작업(HTTP 메서드)을 식별하는 규칙과 기타 작업별 정보를 포함하는 XML 문서입니다. CORS에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Cross-Origin 리소스 공유 활성화(CORS) 단원을 참조하십시오.

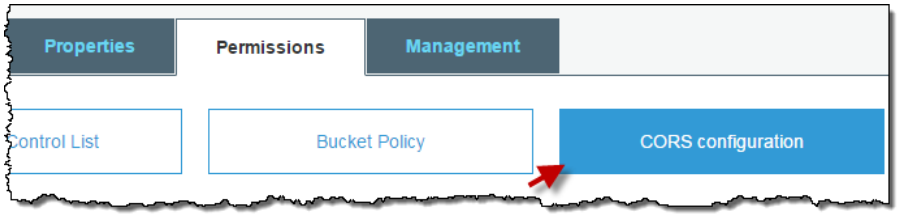
버킷에 대해 CORS를 활성화하면 ACL(액세스 제어 목록)과 기타 액세스 권한 정책이 계속 적용됩니다.

S3 버킷에 CORS 구성을 추가하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 이름 목록에서 버킷 정책을 만들 버킷의 이름을 선택합니다.



3. 권한을 선택하고 CORS 구성을 선택합니다.



4. CORS 구성 편집기 텍스트 상자에 새 CORS 구성을 입력하거나 복사하여 붙여넣거나, 기존 구성을 편집합니다. CORS 구성은 XML 파일입니다. 편집기에 입력하는 텍스트는 유효한 XML이어야 합니다. 자세한 내용은 내 버킷에서 CORS를 구성하려면 어떻게 해야 합니까?를 참조하십시오.
5. Save를 선택합니다.

   Note

   Amazon S3는 CORS 구성 편집기 제목 옆에 버킷의 Amazon 리소스 이름(ARN)을 표시합니다. ARN에 대한 자세한 내용은 Amazon Web Services 일반 참조의 Amazon 리소스 이름(ARN) 및 AWS 서비스 네임스페이스 단원을 참조하십시오.

추가 정보

- 버킷 및 객체 액세스 권한 설정 (p. 110)
- ACL 버킷 권한을 설정하려면 어떻게 해야 합니까? (p. 118)
- S3 버킷 정책을 추가하려면 어떻게 해야 합니까? (p. 121)

사용 Access Analyzer for S3

Amazon S3에 대한 액세스 분석기는 인터넷상의 모든 사용자 또는 조직 외부의 AWS 계정을 포함한 다른 AWS 계정에 대한 액세스를 허용하도록 구성된 S3 버킷에 대한 알림을 제공합니다. 각 퍼블릭 버킷 또는 공유 버킷에 대해 퍼블릭 액세스 또는 공유 액세스의 수준과 원본을 보고하는 결과가 수신됩니다. 예를 들어 Access Analyzer for S3는 버킷에 버킷 ACL(액세스 제어 목록), 버킷 정책 또는 둘 다를 통해 제공된 읽기 액세스 권한 또는 쓰기 액세스 권한이 있음을 나타낼 수 있습니다. 이러한 지식을 바탕으로 즉각적이고 정확한 시정 조치를 취하여 버킷 액세스를 원하는 대로 복원할 수 있습니다.

Access Analyzer for S3에서 위험 버킷을 검토할 때 클릭 한 번으로 버킷에 대한 모든 퍼블릭 액세스를 차단할 수 있습니다. 특정 사용 사례를 지원하기 위해 퍼블릭 액세스가 필요하지 않은 경우 버킷에 대한 모든 액세스를 차단하는 것이 좋습니다. 모든 퍼블릭 액세스를 차단하기 전에 애플리케이션이 퍼블릭 액세스 없이 계속 올바르게 작동하는지 확인하십시오. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 퍼블릭 액세스 차단 사용 단원을 참조하십시오.

또한 버킷 수준 권한 설정으로 드릴다운하여 세부적인 액세스 수준을 구성할 수 있습니다. 정적 웹 사이트 호스팅, 공개 다운로드 또는 교차 계정 공유와 같이 퍼블릭 액세스가 필요한 것으로 확인된 특정 사용 사례의 경우, 버킷에 대한 결과를 보관하여 버킷을 퍼블릭 상태로 유지할 것인지 공유 상태로 유지할 것인지 확인하고 기록할 수 있습니다. 언제든지 재방문하여 해당 버킷 구성을 수정할 수 있습니다. 감사 목적으로 결과를 CSV 보고서로 다운로드할 수도 있습니다.

Access Analyzer for S3는 Amazon S3 콘솔에서 추가 비용 없이 사용할 수 있습니다. Access Analyzer for S3는 AWS Identity and Access Management(IAM)Access Analyzer에서 제공합니다. Amazon S3 콘솔에서 Access Analyzer for S3를 사용하려면 IAM 콘솔을 방문하여 리전별로 IAM Access Analyzer을 활성화해야 합니다.

IAM Access Analyzer에 대한 자세한 내용은 IAM 사용 설명서의 Access Analyzer이란 무엇입니까?를 참조하십시오. Access Analyzer for S3에 대한 자세한 내용은 다음 단원을 검토하십시오.

> **Important**
>
> 버킷 정책 또는 버킷 ACL이 추가되거나 수정되면 Access Analyzer이 30분 이내에 변경 사항을 기반으로 결과를 생성하고 업데이트합니다. 계정 수준 퍼블릭 액세스 차단 설정과 관련된 결과는 설정을 변경한 후 최대 6시간 동안 생성되거나 업데이트되지 않을 수 있습니다.

주제

Access Analyzer for S3는 어떤 정보를 제공합니까?

Access Analyzer for S3에서는 AWS 계정 외부에서 액세스할 수 있는 버킷에 대한 결과를 제공합니다. 퍼블릭 액세스가 가능한 버킷 아래에 나열된 버킷은 인터넷상의 모든 사용자가 액세스할 수 있습니다. Access Analyzer for S3가 퍼블릭 버킷을 식별하면 페이지 상단에 리전의 퍼블릭 버킷 수를 보여주는 경고가 표시됩니다. 타사 AWS 계정을 포함한 다른 AWS 계정 —에서 액세스할 수 있는 버킷 아래에 나열된 버킷은 조직 외부의 계정을 비롯한 다른 AWS 계정과 조건부로 공유됩니다.

Access Analyzer for S3에서는 각 버킷에 대한 다음 정보를 제공합니다.

- Bucket name
- 액세스 분석기에서 검색됨 - Access Analyzer for S3가 퍼블릭 버킷 액세스 또는 공유 버킷 액세스를 검색한 경우입니다.
- 공유 - 버킷 정책, 버킷 ACL 또는 둘 다를 통해 버킷이 공유되는 방법입니다. 버킷 액세스에 대한 소스를 찾고 검토하려는 경우 이 열의 정보를 즉각적이고 정확한 시정 조치를 취하기 위한 시작점으로 사용할 수 있습니다.
- 상태 - 버킷 결과의 상태입니다. Access Analyzer for S3에는 모든 퍼블릭 버킷 및 공유 버킷에 대한 결과가 표시됩니다.
  - 활성 - 결과가 검토되지 않았습니다.
  - 보관됨 - 결과가 의도한 대로 검토 및 확인되었습니다.
  - 모두 - 조직 외부의 AWS 계정을 포함한 다른 AWS 계정과 공유되는 버킷이나 퍼블릭 버킷에 대한 모든 결과입니다.
- 액세스 수준 - 버킷에 부여된 액세스 권한입니다.

- 목록 - 리소스를 나열합니다.
- 읽기 - 리소스 콘텐츠 및 속성을 읽기만 하고 편집하지 않습니다.
- 쓰기 - 리소스를 생성, 삭제 또는 수정합니다.
- 권한 - 리소스 권한을 부여하거나 수정합니다.
- 태그 지정 - 리소스와 연결된 태그를 업데이트합니다.

Access Analyzer for S3 활성화

Amazon S3 콘솔에서 Access Analyzer for S3를 사용하려면 IAM 콘솔을 방문하여 다음을 수행해야 합니다.

- 권한을 설정합니다.
- 사용할 각 리전에 IAM Access Analyzer을 활성화합니다.

자세한 내용은 IAM 사용 설명서의 Access Analyzer 시작하기를 참조하십시오.

모든 퍼블릭 액세스 차단

클릭 한 번으로 버킷에 대한 모든 액세스를 차단하려는 경우 Access Analyzer for S3에서 모든 퍼블릭 액세스 차단 버튼을 사용할 수 있습니다. 버킷에 대한 모든 퍼블릭 액세스를 차단하면 퍼블릭 액세스 권한이 부여되지 않습니다. 확인된 특정 사용 사례를 지원하기 위해 퍼블릭 액세스가 필요하지 않은 경우 버킷에 대한 모든 공개 액세스를 차단하는 것이 좋습니다. 모든 퍼블릭 액세스를 차단하기 전에 애플리케이션이 퍼블릭 액세스 없이 계속 올바르게 작동하는지 확인하십시오.

버킷에 대한 모든 퍼블릭 액세스를 차단하지 않으려면 Amazon S3 콘솔에서 퍼블릭 액세스 차단 설정을 편집하여 버킷에 대한 세분화된 액세스 수준을 구성할 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon S3 퍼블릭 액세스 차단 사용 단원을 참조하십시오.

드문 경우이지만 Access Analyzer for S3에서는 Amazon S3 퍼블릭 액세스 차단 평가에서 공개적으로 보고하는 버킷에 대한 결과를 보고되지 않을 수 있습니다. 이는 Amazon S3 퍼블릭 액세스 차단이 현재 작업 및 향후 추가될 수 있는 모든 잠재적 작업에 대한 정책을 검토하기 때문에 발생하므로 버킷이 퍼블릭이 됩니다. 반면에 Access Analyzer for S3는 액세스 상태를 평가할 때 Amazon S3 서비스에 대해 지정된 현재 작업만 분석합니다.

Access Analyzer for S3를 사용하여 버킷에 대한 모든 퍼블릭 액세스를 차단하려면

1. AWS Management 콘솔에 로그인한 다음 https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 왼쪽의 탐색 창의 대시보드, 아래에서 S3에 대한 액세스 분석기를 선택합니다.
3. Access Analyzer for S3에서 버킷을 선택합니다.
4. 모든 퍼블릭 액세스 차단을 선택합니다.
5. 버킷에 대한 모든 퍼블릭 액세스를 차단할 것인지 확인하려면 모든 퍼블릭 액세스 차단(버킷 설정)에 **`confirm`**을 입력합니다.

   Amazon S3는 버킷에 대한 모든 퍼블릭 액세스를 차단합니다. 버킷 결과의 상태가 해결됨으로 업데이트되고 버킷이 Access Analyzer for S3 목록에서 사라집니다. 해결된 버킷을 검토하려면 IAM 콘솔에서 IAM Access Analyzer를 엽니다.

버킷 정책 또는 버킷 ACL 검토 및 변경

조직 외부의 계정을 포함한 퍼블릭 계정 또는 다른 AWS 계정에 대한 액세스 권한을 부여하지 않으려는 경우 버킷 ACL, 버킷 정책 또는 둘 다를 수정하여 버킷에 대한 액세스 권한을 제거할 수 있습니다.

Access Analyzer for S3에서 버킷 정책 또는 버킷 ACL을 변경하려면

1. https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 탐색 창에서 S3에 대한 액세스 분석기를 선택합니다.
3. 버킷 정책, 버킷 ACL 또는 둘 다를 통해 퍼블릭 액세스 또는 공유 액세스가 부여되는지 확인하려면 공유 열을 참조하십시오.
4. 버킷 이름에서 변경 또는 검토하려는 버킷 정책 또는 버킷 ACL이 있는 버킷의 이름을 선택합니다.
5. Permissions를 선택합니다.
6. 버킷 ACL을 변경하거나 보려면 액세스 제어 목록을 선택합니다.
7. 버킷 정책을 변경하거나 보려면 버킷 정책을 선택합니다.

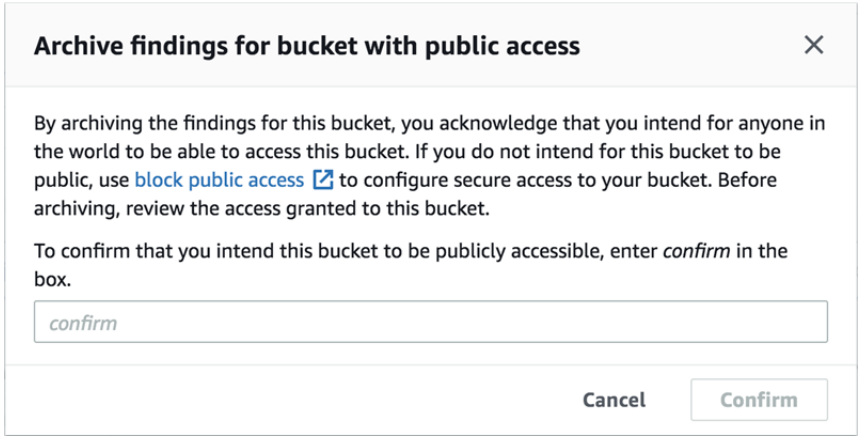
   버킷 ACL 또는 버킷 정책을 편집하거나 제거하여 퍼블릭 또는 공유 액세스를 제거하면 버킷 결과의 상태가 해결됨으로 업데이트됩니다. 해결된 버킷 결과는 Access Analyzer for S3 목록에서 사라지지만 IAM Access Analyzer에서 확인할 수 있습니다.

버킷 결과 보관

버킷이 특정 사용 사례(예: 정적 웹 사이트, 공개 다운로드 또는 교차 계정 공유)를 지원하기 위해 조직 외부의 계정을 포함하여 퍼블릭 계정 또는 다른 AWS 계정에 대한 액세스 권한을 부여하는 경우 버킷에 대한 결과를 보관할 수 있습니다. 버킷 결과를 보관할 때 버킷을 퍼블릭 상태로 유지할 것인지 공유 상태로 유지할 것인지 확인하고 기록할 수 있습니다. 보관된 버킷 결과는 Access Analyzer for S3 목록에 남아 있으므로 어떤 버킷이 퍼블릭 버킷인지 또는 공유 버킷인지 항상 알 수 있습니다.

버킷 결과를 Access Analyzer for S3에 보관하려면

1. https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 탐색 창에서 S3에 대한 액세스 분석기를 선택합니다.
3. Access Analyzer for S3에서 활성 버킷을 선택합니다.
4. 조직 외부의 계정을 포함하여 퍼블릭 계정 또는 다른 AWS 계정에서 이 버킷에 액세스하도록 할 것인지 확인하려면 아카이브를 선택합니다.
5. **`confirm`**을 입력하고 아카이브를 선택합니다.



보관된 버킷 결과 활성화

결과를 보관한 후에는 언제든지 다시 방문하여 상태를 다시 활성으로 변경할 수 있습니다. 이는 버킷에 다른 검토가 필요함을 나타냅니다.

Access Analyzer for S3에 보관된 버킷 결과를 활성화하려면

1. https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 탐색 창에서 S3에 대한 액세스 분석기를 선택합니다.
3. 보관된 버킷 결과를 선택합니다.
4. 활성으로 표시를 선택합니다.

결과 세부 정보 보기

버킷에 대한 자세한 정보가 필요한 경우 IAM 콘솔의 IAM Access Analyzer에서 버킷 결과 세부 정보를 열 수 있습니다.

Access Analyzer for S3에서 결과 세부 정보를 보려면

1. https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 탐색 창에서 S3에 대한 액세스 분석기를 선택합니다.
3. Access Analyzer for S3에서 버킷을 선택합니다.
4. 세부 정보 보기를 선택합니다.

   결과 세부 정보가 IAM 콘솔의 IAM Access Analyzer에서 열립니다.

Access Analyzer for S3 보고서 다운로드

버킷 결과를 감사 목적으로 사용할 수 있는 CSV 보고서로 다운로드할 수 있습니다. 보고서에는 Amazon S3 콘솔의 Access Analyzer for S3에 표시되는 것과 동일한 정보가 포함됩니다.

보고서를 다운로드하려면

1. https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 왼쪽의 탐색 창에서 S3에 대한 액세스 분석기를 선택합니다.
3. 리전 필터에서 리전을 선택합니다.

   Access Analyzer for S3가 업데이트되어 선택한 리전의 버킷을 표시합니다.
4. 보고서 다운로드를 선택합니다.

   CSV 보고서가 생성되어 컴퓨터에 저장됩니다.

문서 이력

최신 설명서 업데이트: 2019년 3월 27일

다음 표는 2018년 6월 19일 및 이후 Amazon Simple Storage Service 콘솔 사용 설명서의 각 릴리스에서 변경된 중요 사항에 대해 설명합니다. 이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

update-history-change	update-history-description	update-history-date
새 아카이브 스토리지 클래스 (p. 128)	Amazon S3은 거의 액세스하지 않는 객체를 저장하기 위한 새로운 아카이브 스토리지 클래스인 DEEP_ARCHIVE를 제공합니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드에서 아카이브된 S3 객체를 복원하려면 어떻게 해야 합니까? 및 스토리지 클래스 항목을 참조하십시오.	March 27, 2019
S3 버킷에 대한 퍼블릭 액세스 차단 (p. 128)	Amazon S3 퍼블릭 액세스 차단은 S3 버킷 내에서 데이터에 대한 퍼블릭 액세스를 허용하는 모든 설정의 적용을 차단합니다. 자세한 내용은 S3 버킷에 대한 퍼블릭 액세스 차단 단원을 참조하십시오.	November 15, 2018
교차 리전 복제(CRR) 규칙에서 필터링 개선 (p. 128)	CRR 규칙에서 객체 필터를 지정하여 규칙을 적용할 객체의 하위 집합을 선택할 수 있습니다. 이전에는 객체 키 접두사만 필터링할 수 있었습니다. 이 릴리스에서는 객체 키 접두사, 하나 이상의 객체 태그 또는 이 두 가지를 모두에 대해 필터를 지정할 수 있습니다. 자세한 내용은 S3 버킷에 복제 규칙을 추가하는 방법 단원을 참조하십시오.	September 19, 2018
RSS에서 현재 사용 가능한 업데이트 (p. 128)	이제 Amazon Simple Storage Service 콘솔 사용 설명서 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.	June 19, 2018

이전 업데이트

다음 표에서는 2018년 6월 19일 이전 Amazon Simple Storage Service 콘솔 사용 설명서의 각 릴리스에서 변경된 중요 사항에 대해 설명합니다.

변경 사항	설명	변경 날짜
새 스토리지 클래스	Amazon S3는 이제 객체 저장을 위한 새 스토리지 클래스인 ONEZONE_IA(IA, 자주 액세스하지 않는 경우)를 제공합니다. 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 스토리지 클래스를 참조하십시오.	2018년 4월 4일
ORC 형식 Amazon S3 인벤토리 파일 지원	이제 Amazon S3는 인벤토리 출력 파일에 대해 쉼표로 구분된 값(CSV) 파일 형식 이외에 Apache ORC(Optimized Row Columnar) 형식도 지원합니다. 자세한 내용은 Amazon S3 인벤토리를 구성하려면? (p. 100) 단원을 참조하십시오.	2017년 11월 17일
버킷 권한 확인	Amazon S3 콘솔의 버킷 권한 확인 기능은 버킷 정책 및 버킷 ACL(액세스 통제 목록)을 확인하여 공개적으로 액세스 가능한 버킷을 식별합니다. 버킷 권한 확인을 사용하면 퍼블릭 읽기 및 쓰기 권한을 제공하는 S3 버킷을 쉽게 식별할 수 있습니다. .	2017년 11월 06일
S3 버킷에 대한 기본 암호화	Amazon S3 기본 암호화를 사용하면 S3 버킷의 기본 암호화 동작을 설정할 수 있습니다. 버킷에 저장되는 모든 객체를 암호화하도록 버킷에 대한 기본 암호화를 설정할 수 있습니다. Amazon S3 관리형 키(SSE-S3) 또는 AWS KMS 관리형 키(SSE-KMS)로 서버 측 암호화를 사용하여 객체를 암호화합니다. 자세한 내용은 Amazon S3 버킷의 기본 암호화를 활성화하려면 어떻게 해야 합니까? (p. 8) 단원을 참조하십시오.	2017년 11월 06일
Amazon S3 인벤토리의 암호화 상태	Amazon S3는 이제 Amazon S3 인벤토리의 암호화 상태를 지원하므로 규정 준수 감사 또는 기타 목적을 위해 저장된 객체가 어떻게 암호화되었는지 확인할 수 있습니다. 또한 모든 인벤토리 파일이 적절히 암호화되도록 서버 측 암호화(SSE) 또는 SSE-KMS를 사용하여 Amazon S3 인벤토리를 암호화하도록 구성할 수 있습니다. 자세한 내용은 Amazon S3 인벤토리를 구성하려면? (p. 100) 단원을 참조하십시오.	2017년 11월 06일
교차 리전 복제 기능 향상	이제 교차 리전 복제에서는 다음을 지원합니다. • 기본적으로 Amazon S3는 AWS KMS 관리형 키를 사용하는 서버 측 암호화를 사용하여 생성되는 객체를 원본 버킷에 복제하지 않습니다. 이제 이러한 객체를 복제하도록 복제 규칙을 구성할 수 있습니다. 자세한 내용은 S3 버킷에서 복제 규칙을 추가하는 방법 (p. 80) 단원을 참조하십시오. • 교차 계정 시나리오에서 복제본 소유권을 대상 버킷을 소유한 AWS 계정으로 변경하도록 복제 규칙을 구성할 수 있습니다. 자세한 내용은 대상 버킷이 다른 AWS 계정에 있는 경우 복제 규칙 추가 (p. 87) 단원을 참조하십시오.	2017년 11월 06일
추가된 기능 및 설명서	Amazon S3 콘솔에서 이제 AWS CloudTrail 데이터 이벤트 로깅을 사용하여 S3 버킷에 대해 객체 수준 로깅을 활성화할 수 있습니다. 자세한 내용은 AWS CloudTrail 데이터 이벤트로 S3 버킷에 대해 객체 수준 로깅을 활성화하려면 어떻게 합니까? (p. 13) 단원을 참조하십시오.	2017년 10월 19일
더 이상 사용 가능한 이전 Amazon S3 콘솔 없음	Amazon S3 콘솔의 이전 버전은 더 이상 사용할 수 없으며 이전 사용 설명서는 Amazon S3 설명서 사이트에서 삭제되었습니다.	2017년 8월 31일
새 Amazon S3 콘솔 정식 출시	새 Amazon S3 콘솔의 정식 출시를 발표했습니다.	2017년 5월 15일

AWS Glossary

For the latest AWS terminology, see the AWS Glossary in the AWS General Reference.