버킷 및 그룹 액세스 정책

StorageGRID 11.7

NetApp
April 12, 2024

목차

버킷 및 그룹 액세스 정책

버킷 및 그룹 액세스 정책을 사용합니다

StorageGRID은 AWS(Amazon Web Services) 정책 언어를 사용하여 S3 테넌트가 해당 버킷 및 오브젝트 내의 버킷에 대한 액세스를 제어할 수 있도록 합니다. StorageGRID 시스템은 S3 REST API 정책 언어의 하위 집합을 구현합니다. S3 API에 대한 액세스 정책은 JSON으로 기록됩니다.

액세스 정책 개요

StorageGRID에서 지원하는 액세스 정책에는 두 가지 유형이 있습니다.

- * 버킷 정책 * - 버킷 정책 가져오기, 버킷 정책 적용 및 버킷 정책 삭제 S3 API 작업을 사용하여 구성됩니다. 버킷 정책은 버킷에 첨부되므로 버킷 소유자 계정 또는 버킷에 대한 다른 계정 및 버킷에 있는 오브젝트에 대한 사용자의 액세스를 제어하도록 구성됩니다. 버킷 정책은 하나의 버킷과 여러 그룹에만 적용됩니다.
- 테넌트 관리자 또는 테넌트 관리 API를 사용하여 구성된 * 그룹 정책 * 입니다. 그룹 정책은 계정의 그룹에 연결되므로 해당 그룹이 해당 계정이 소유한 특정 리소스에 액세스할 수 있도록 구성됩니다. 그룹 정책은 하나의 그룹에만 적용되고 여러 버킷에 적용될 수 있습니다.

그룹 정책과 버킷 정책 간에는 우선 순위에 차이가 없습니다.

StorageGRID 버킷 및 그룹 정책은 아마존에서 정의한 특정 문법을 따릅니다. 각 정책 안에는 정책 문의 배열이 들어 있으며 각 문에는 다음 요소가 포함되어 있습니다.

- 정책 ID(SID)(선택 사항)
- 효과
- Principal/NotPrincipal입니다
- 리소스/NotResource입니다
- 작업/NotAction
- 조건(선택 사항)

정책 문은 이 구조를 사용하여 권한을 지정합니다. pert <effect> <principal>이(가) <condition>이(가) 적용될 때 <Resource>에서 <Action>을(를) 수행하도록 허용/거부합니다.

각 정책 요소는 특정 함수에 사용됩니다.

요소	설명
SID	SID 요소는 선택 사항입니다. SID는 사용자에 대한 설명으로만 제공됩니다. StorageGRID 시스템에서 저장하지만 해석되지 않습니다.
효과	Effect 요소를 사용하여 지정된 작업의 허용 여부를 설정합니다. 지원되는 작업 요소 키워드를 사용하여 버킷 또는 오브젝트에 대해 허용(또는 거부)하는 작업을 식별해야 합니다.

요소	설명
Principal/NotPrincipal입니다	사용자, 그룹 및 계정이 특정 리소스에 액세스하고 특정 작업을 수행하도록 허용할 수 있습니다. 요청에 S3 서명이 포함되지 않은 경우 와일드카드 문자(*)를 보안 주체에 지정하여 익명 액세스가 허용됩니다. 기본적으로 계정 루트만 해당 계정이 소유한 리소스에 액세스할 수 있습니다. 버킷 정책에서 Principal 요소만 지정하면 됩니다. 그룹 정책의 경우 정책이 연결된 그룹이 암시적 Principal 요소입니다.
리소스/NotResource입니다	Resource 요소는 버킷 및 오브젝트를 식별합니다. ARN(Amazon Resource Name)을 사용하여 리소스를 식별하는 버킷 및 객체에 대한 권한을 허용하거나 거부할 수 있습니다.
작업/NotAction	Action 및 Effect 요소는 권한의 두 구성 요소입니다. 그룹이 리소스를 요청하면 리소스에 대한 액세스가 부여되거나 거부됩니다. 명시적으로 권한을 할당하지 않는 한 액세스가 거부되지만 명시적 DENY를 사용하여 다른 정책이 부여한 권한을 재정의할 수 있습니다.
조건	Condition 요소는 선택 요소입니다. 조건을 사용하면 식을 만들어 정책을 적용해야 하는 시기를 결정할 수 있습니다.

Action 요소에서 와일드카드 문자(*)를 사용하여 모든 작업이나 작업의 하위 집합을 지정할 수 있습니다. 예를 들어 이 작업은 S3:GetObject , S3:PutObject 및 S3:DeleteObject 와 같은 사용 권한을 일치시킵니다.

```
s3:*Object
```

Resource 요소에서 와일드카드 문자(\ **)** 및 **(?)**를 사용할 수 있습니다**.** 별표**(**)가 0개 이상의 문자와 일치하면 물음표(?)가 모든 단일 문자와 일치합니다.

Principal 요소에서 모든 사용자에게 권한을 부여하는 익명 액세스를 설정하는 것 외에는 와일드카드 문자는 지원되지 않습니다. 예를 들어 와일드카드(*)를 Principal 값으로 설정합니다.

```
"Principal":"*"
```

다음 예제에서는 Effect , Principal , Action 및 Resource 요소를 사용합니다. 이 예제에서는 "Allow" 효과를 사용하여 Principals, 즉 admin 그룹에 제공하는 전체 버킷 정책 문을 보여 줍니다 `federated-group/admin` 재무그룹을 의미합니다 `federated-group/finance`, 작업 수행 권한 `s3:ListBucket` 을(를) 버킷에 표시합니다 `mybucket` 및 조치 `s3:GetObject` 버킷에 있는 모든 물체

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:iam:s3:::mybucket",
        "arn:aws:iam:s3:::mybucket/*"
      ]
    }
  ]
}
```

버킷 정책은 크기 제한이 20,480바이트이고 그룹 정책은 크기 제한이 5,120바이트입니다.

정책에 대한 정합성 보장 제어 설정입니다

기본적으로 그룹 정책에 대한 모든 업데이트는 최종적으로 일치합니다. 그룹 정책이 일관되면 정책 캐싱 때문에 변경 내용이 적용되는 데 15분 정도 더 걸릴 수 있습니다. 기본적으로 버킷 정책에 대한 모든 업데이트도 최종적으로 일치합니다.

필요에 따라 버킷 정책 업데이트의 일관성 보장을 변경할 수 있습니다. 예를 들어, 보안상의 이유로 버킷 정책을 최대한 빨리 변경할 수 있습니다.

이 경우 를 설정할 수 있습니다 `Consistency-Control` PUT 버킷 정책 요청의 헤더나 PUT 버킷 정합성 보장 요청을 사용할 수 있습니다. 이 요청에 대한 정합성 제어를 변경할 때는 읽기 후 쓰기 정합성을 보장하는 * All * 값을 사용해야 합니다. Put Bucket 정합성 보장 요청의 헤더에 다른 정합성 보장 제어 값을 지정하면 요청이 거부됩니다. Put Bucket 정책 요청에 대해 다른 값을 지정하면 값이 무시됩니다. 버킷 정책이 일관되면 정책 캐싱으로 인해 변경 사항이 적용되는 데 8초가 더 걸릴 수 있습니다.

> ⓘ 정합성 수준을 * All * 로 설정하면 새 버킷 정책이 더 빨리 발효되도록 하려면 작업이 완료되면 버킷 수준 제어를 원래 값으로 다시 설정해야 합니다. 그렇지 않으면 이후의 모든 버킷 요청은 * All * 설정을 사용합니다.

정책 설명에 **ARN**을 사용합니다

정책 문에서 ARN은 Principal 및 Resource 요소에서 사용됩니다.

- 이 구문을 사용하여 S3 리소스 ARN을 지정합니다.

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- 이 구문을 사용하여 ID 리소스 ARN(사용자 및 그룹)을 지정합니다.

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

기타 고려 사항:

- 별표(*)를 와일드카드로 사용하여 개체 키 안에 0개 이상의 문자를 일치시킬 수 있습니다.
- 개체 키에 지정할 수 있는 국제 문자는 JSON UTF-8 또는 JSON\u 이스케이프 시퀀스를 사용하여 인코딩해야 합니다. 퍼센트 인코딩은 지원되지 않습니다.

  "RFC 2141 URN 구문"

  Put Bucket 정책 작업의 HTTP 요청 본문은 charset=UTF-8로 인코딩되어야 합니다.

정책에서 리소스를 지정합니다

정책 문에서 Resource 요소를 사용하여 사용 권한이 허용되거나 거부되는 버킷 또는 개체를 지정할 수 있습니다.

- 각 정책 문에는 Resource 요소가 필요합니다. 정책에서 리소스는 요소로 표시됩니다 `Resource`또는 `NotResource` 제외.
- S3 리소스 ARN을 사용하여 리소스를 지정합니다. 예를 들면 다음과 같습니다.

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- 개체 키 내에서 정책 변수를 사용할 수도 있습니다. 예를 들면 다음과 같습니다.

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- 리소스 값은 그룹 정책이 생성될 때 아직 존재하지 않는 버킷을 지정할 수 있습니다.

정책에 보안 주체를 지정합니다

Principal 요소를 사용하여 policy 문에 의해 리소스에 대한 액세스가 허용/거부된 사용자, 그룹 또는 테넌트 계정을

식별합니다.

- 버킷 정책의 각 정책 선언에는 Principal 요소가 포함되어야 합니다. 그룹 정책의 정책 설명은 그룹이 보안 주체로 인식되기 때문에 Principal 요소가 필요하지 않습니다.
- 정책에서 교장은 제외에 대해 "Principal" 또는 "NotPrincipal" 요소로 표시됩니다.
- 계정 기반 ID는 ID 또는 ARN을 사용하여 지정해야 합니다.

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- 이 예에서는 계정 루트 및 계정의 모든 사용자를 포함하는 테넌트 계정 ID 27233906934684427525를 사용합니다.

```
 "Principal": { "AWS": "27233906934684427525" }
```

- 계정 루트만 지정할 수 있습니다.

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- 특정 페더레이션 사용자("Alex")를 지정할 수 있습니다.

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- 특정 통합 그룹("관리자")을 지정할 수 있습니다.

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

- 익명 보안 주체를 지정할 수 있습니다.

```
"Principal": "*"
```

- 모호함을 방지하려면 사용자 이름 대신 사용자 UUID를 사용할 수 있습니다.

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

  예를 들어 Alex가 조직과 사용자 이름을 그대로 두고 있다고 가정해 보겠습니다 `Alex` 이(가) 삭제됩니다. 새로운 Alex가 조직에 합류하여 동일한 권한이 할당된 경우 `Alex` 사용자 이름, 새 사용자는 의도하지 않게 원래

사용자에게 부여된 권한을 상속할 수 있습니다.

- Principal 값은 버킷 정책이 생성될 때 아직 존재하지 않는 그룹/사용자 이름을 지정할 수 있습니다.

정책에서 사용 권한을 지정합니다

정책에서 Action 요소는 리소스에 대한 권한을 허용/거부하는 데 사용됩니다. 정책에서 지정할 수 있는 사용 권한 집합이 있으며, 이러한 권한은 "작업" 또는 "NotAction" 요소로 표시됩니다. 각 요소는 특정 S3 REST API 작업에 매핑됩니다.

이 표에는 버킷에 적용되는 사용 권한과 객체에 적용되는 사용 권한이 나열되어 있습니다.

Amazon S3는 이제 PUT 및 DELETE Bucket 복제 작업 모두에 S3:PutReplicationConfiguration 권한을 사용합니다. StorageGRID는 원래 Amazon S3 사양과 일치하는 각 작업에 대해 별도의 권한을 사용합니다.

기존 값을 덮어쓰는 데 PUT를 사용할 때 삭제가 수행됩니다.

버킷에 적용되는 권한

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3:생성 버킷	버킷 을 놓습니다	
S3:삭제 버킷	버킷 삭제	
S3:DeleteBucketMetadataNotification	버킷 메타데이터 알림 구성을 삭제합니다	예
S3:삭제 BucketPolicy	버킷 정책을 삭제합니다	
S3:DeleteReplicationConfiguration	버킷 복제를 삭제합니다	예, PUT 및 DELETE에 대한 별도의 권한 *
S3:GetBuckketAcl	버킷 ACL 가져오기	
S3:GetBucketCompliance	버킷 규정 준수 가져오기(더 이상 사용되지 않음)	예
S3:GetBuckketConsistency	버킷 일관성 확보	예
S3:GetBuckketCORS	버킷 CORS를 가져옵니다	
S3:GetEncryptionConfiguration	버킷 암호화 가져오기	
S3:GetBucketLastAccessTime	버킷 최종 액세스 시간 가져오기	예

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3:GetBucketLocation	버킷 위치를 가져옵니다	
S3:GetBuckMetadataNotification 을 참조하십시오	Bucket 메타데이터 알림 구성 가져오기	예
S3:GetBucketNotification 을 참조하십시오	버킷 알림을 받습니다	
S3:GetBuckketObjectLockConfiguration	개체 잠금 구성을 가져옵니다	
S3:GetBuckketPolicy를 참조하십시오	버킷 정책 가져오기	
S3:GetBucketTagging	버킷 태그 지정을 가져옵니다	
S3:GetBucketVersioning	버킷 버전 관리 가져오기	
S3:GetLifecycleConfiguration	버킷 수명 주기 가져오기	
S3:GetReplicationConfiguration	버킷 복제를 가져옵니다	
S3:ListAllMyBucket	• 서비스 받기 • 스토리지 사용량을 가져옵니다	예, 스토리지 사용량 가져오에 대해 가능합니다
S3:목록 버킷	• 버킷 가져오기(객체 나열) • 헤드 버킷 • 사후 개체 복원	
S3:ListBuckketMultipartUploads	• 다중 파트 업로드 나열 • 사후 개체 복원	
S3:목록 BuckketVersions	버킷 버전 가져오기	
S3: PutBucketCompliance	버킷 규정 준수(폐기됨)	예
S3: PutBucketConsistency	버킷 일관성을 유지합니다	예
S3: PutBucketCORS	• 버킷 CORS† 삭제 • 버킷 CORS를 넣습니다	

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3:PutEncryptionConfiguration	• Bucket 암호화를 삭제합니다 • Bucket 암호화를 적용합니다	
S3:PutBucketLastAccessTime	버킷 최종 접근 시간	예
S3:PutBucketMetadataNotification	Put Bucket 메타데이터 알림 구성	예
S3: PutBucketNotification	버킷 통지를 보냅니다	
S3:PutBucketObjectLockConfiguration	• 에 Bucket 을 놓습니다 `x-amz-bucket-object-lock-enabled: true` 요청 헤더(S3:CreateBucket 권한도 필요함) • 개체 잠금 구성을 배치합니다	
S3: PutBucketPolicy	버킷 정책을 적용합니다	
S3: PutBucketTagging	• 버킷 태그 표시 삭제† • Bucket 태그 달기	
S3: PutBucketVersioning	버킷 버전 관리	
S3: PutLifecycleConfiguration	• 버킷 수명 주기 삭제† • 버킷 수명 주기를 놓습니다	
S3:PutReplicationConfiguration	버킷 복제를 배치합니다	예, PUT 및 DELETE에 대한 별도의 권한 *

객체에 적용되는 권한

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3:중단멀티업로드입니다	• 멀티파트 업로드를 중단합니다 • 사후 개체 복원	
S3:BypassGovernanceRetention	• 개체 삭제 • 여러 개체를 삭제합니다 • 개체 보존	

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3:DeleteObject 를 선택합니다	• 개체 삭제 • 여러 개체를 삭제합니다 • 사후 개체 복원	
S3:삭제 ObjectTagging	개체 태그 지정을 삭제합니다	
S3:DeleteObjectVersionTagging	개체 태그 지정 삭제(개체의 특정 버전)	
S3:DeleteObjectVersion	개체 삭제(개체의 특정 버전)	
S3:GetObject	• 객체 가져오기 • 헤드 개체 • 사후 개체 복원 • 개체 내용 을 선택합니다	
S3:GetObjectAcl	객체 ACL을 가져옵니다	
S3:GetObjectLegalHold	객체 법적 증거 자료 보관	
S3:GetObjectRetention	개체 보존 가져오기	
S3:GetObjectTagging	개체 태그 지정을 가져옵니다	
S3:GetObjectVersionTagging	개체 태그 지정 가져오기(개체의 특정 버전)	
S3:GetObjectVersion	개체 가져오기(개체의 특정 버전)	
S3:ListMultipartUploadParts(S3:ListMultimpartUploadParts) 를	부품 나열, POST 개체 복원	
S3:PutObject	• 개체 를 넣습니다 • 개체 - 복사 를 선택합니다 • 사후 개체 복원 • 멀티파트 업로드를 시작합니다 • 멀티파트 업로드를 완료합니다 • 부품 업로드 • 업로드 부품 - 복사	

권한	**S3 REST API** 작업	**StorageGRID** 사용자 지정
S3:PutObjectLegalHold	개체를 법적 증거 자료 보관	
S3:PutObjectRetention	개체 보존	
S3:PutObjectTagging	개체 태깅을 넣습니다	
S3:PutObjectVersionTagging	개체 태그 지정(개체의 특정 버전)	
S3:PutOverwriteObject	• 개체 를 넣습니다 • 개체 - 복사 를 선택합니다 • 개체 태그 지정 • 개체 태그 지정 삭제 • 멀티파트 업로드를 완료합니다	예
S3:RestoreObject	사후 개체 복원	

PutOverwriteObject 권한을 사용합니다

S3:PutOverwriteObject 권한은 개체를 만들거나 업데이트하는 작업에 적용되는 사용자 지정 StorageGRID 권한입니다. 이 사용 권한의 설정에 따라 클라이언트가 개체의 데이터, 사용자 정의 메타데이터 또는 S3 오브젝트 태그 지정을 덮어쓸 수 있는지 여부가 결정됩니다.

이 권한에 사용할 수 있는 설정은 다음과 같습니다.

- * 허용 *: 클라이언트가 개체를 덮어쓸 수 있습니다. 기본 설정입니다.
- * 거부 *: 클라이언트가 개체를 덮어쓸 수 없습니다. Deny 로 설정된 경우 PutOverwriteObject 권한은 다음과 같이 작동합니다.
  - 기존 객체가 같은 경로에 있는 경우:
    - 오브젝트의 데이터, 사용자 정의 메타데이터 또는 S3 오브젝트 태깅을 덮어쓸 수 없습니다.
    - 진행 중인 모든 수집 작업이 취소되고 오류가 반환됩니다.
    - S3 버전 관리가 활성화된 경우 거부 설정을 사용하면 개체 태그 지정 또는 개체 삭제 태그 지정 작업에서 개체 및 현재 버전이 아닌 개체의 TagSet을 수정할 수 없습니다.
  - 기존 개체를 찾을 수 없으면 이 권한은 적용되지 않습니다.
- 이 권한이 없으면 Allow가 설정된 것과 효과가 같습니다.

> 현재 S3 정책이 덮어쓰기를 허용하고 PutOverwriteObject 권한이 Deny 로 설정된 경우 클라이언트는 개체의 데이터, 사용자 정의 메타데이터 또는 개체 태그를 덮어쓸 수 없습니다. 또한 * 클라이언트 수정 방지 * 확인란이 선택된 경우(* 구성 * > * 보안 설정 * > * 네트워크 및 개체 *) 해당 설정은 PutOverwriteObject 권한 설정을 재정의합니다.

정책에서 조건을 지정합니다

조건은 정책이 적용되는 시점을 정의합니다. 조건은 연산자 및 키 값 쌍으로 구성됩니다.

조건은 평가에 키 값 쌍을 사용합니다. 조건 요소에는 여러 조건이 포함될 수 있으며 각 조건에는 여러 키 값 쌍이 포함될 수 있습니다. 조건 블럭은 다음 형식을 사용합니다:

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

다음 예제에서 IPAddress 조건은 SOURCEIP 조건 키를 사용합니다.

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

지원되는 조건 연산자

조건 연산자는 다음과 같이 분류됩니다.

- 문자열
- 숫자
- 부울
- IP 주소입니다
- Null 확인

조건 연산자	설명
StringEquals	정확한 일치(대/소문자 구분)를 기반으로 문자열 값과 키를 비교합니다.
StringNotEquals	키를 부정 일치(대/소문자 구분)를 기반으로 문자열 값과 비교합니다.
StringEqualsIgnoreCase 를 참조하십시오	정확한 일치를 기준으로 문자열 값과 키를 비교합니다(대/소문자 무시).
StringNotEqualsIgnoreCase 를 참조하십시오	Negated matching (대소문자 무시)을 기준으로 문자열 값과 키를 비교합니다.
StringLike 를 선택합니다	정확한 일치(대/소문자 구분)를 기반으로 문자열 값과 키를 비교합니다. 및 * 를 포함할 수 있습니까? 와일드카드 문자.

조건 연산자	설명
StringNotLike 를 참조하십시오	키를 부정 일치(대/소문자 구분)를 기반으로 문자열 값과 비교합니다. 및 * 를 포함할 수 있습니까? 와일드카드 문자.
NumericEquals	정확한 일치를 기준으로 키를 숫자 값과 비교합니다.
NumericNotEquals	키를 부정 일치를 기준으로 숫자 값과 비교합니다.
NumericGreaterThan	키를 ""보다 큼"" 일치를 기준으로 숫자 값과 비교합니다.
NumericGreaterThanEquals	키를 ""크거나 같음"" 일치를 기준으로 숫자 값과 비교합니다.
NumericLessThan	""보다 작음" 일치를 기준으로 키를 숫자 값과 비교합니다.
NumericLessThanEquals	키를 ""보다 작음 또는 같음" 일치를 기준으로 숫자 값과 비교합니다.
불입니다	"true 또는 false" 일치를 기준으로 키를 부울 값과 비교합니다.
IP 주소	키를 IP 주소 또는 IP 주소 범위와 비교합니다.
NotIpAddress 를 참조하십시오	부정 일치를 기준으로 IP 주소 또는 IP 주소 범위와 키를 비교합니다.
null입니다	현재 요청 컨텍스트에 조건 키가 있는지 확인합니다.

지원되는 조건 키

범주	적용 가능한 조건 키	설명
IP 연산자	AWS: SOURCEIP	요청이 전송된 IP 주소와 비교합니다. 버킷 또는 오브젝트 작업에 사용할 수 있습니다. • 참고: * S3 요청이 관리 노드 및 게이트웨이 노드의 로드 밸런서 서비스를 통해 전송된 경우 로드 밸런서 서비스의 IP 주소 업스트림과 비교됩니다. • 참고 *: 타사, 비투명 로드 밸런서가 사용되는 경우 이 로드 밸런서의 IP 주소와 비교합니다. 모두 `X-Forwarded-For` 헤더의 유효성을 확인할 수 없기 때문에 헤더가 무시됩니다.
리소스/ID입니다	AWS: 사용자 이름	요청이 전송된 보낸 사람의 사용자 이름과 비교합니다. 버킷 또는 오브젝트 작업에 사용할 수 있습니다.

범주	적용 가능한 조건 키	설명
S3:ListBucket 및 S3: ListBuckketVersions 권한	S3: 구분 기호	버킷 가져오기 또는 버킷 오브젝트 버전 가져오기 요청에 지정된 구분 기호 매개변수와 비교합니다.
S3:ListBucket 및 S3: ListBuckketVersions 권한	S3: 최대 키	버킷 가져오기 또는 버킷 객체 버전 가져오기 요청에 지정된 최대 키 매개변수와 비교합니다.
S3:ListBucket 및 S3: ListBuckketVersions 권한	S3: 접두어	Get Bucket 또는 Get Bucket Object Versions 요청에 지정된 접두사 매개 변수와 비교합니다.
S3:PutObject	S3: 오브젝트 잠금 장치 - 남은 보존 기간(일)	에 지정된 보존 종료 날짜와 비교합니다 `x-amz-object-lock-retain-until-date` 다음 요청에 대해 허용 범위 내에 있는지 확인하기 위해 버킷 기본 보존 기간에서 헤더를 요청하거나 계산합니다. • 개체 를 넣습니다 • 개체 - 복사 를 선택합니다 • 멀티파트 업로드를 시작합니다
S3:PutObjectRetention	S3: 오브젝트 잠금 장치 - 남은 보존 기간(일)	허용 범위 내에 있는지 확인하기 위해 Put Object Retention 요청에 지정된 Retain-until-date와 비교합니다.

정책에 변수를 지정합니다

정책의 변수를 사용하여 사용 가능한 정책 정보를 채울 수 있습니다. 에서 정책 변수를 사용할 수 있습니다 `Resource` 의 요소 및 문자열 비교 `Condition` 요소.

이 예제에서 변수는 입니다 `${aws:username}` 은(는) Resource 요소의 일부입니다.

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

이 예제에서 변수는 입니다 `${aws:username}` 조건 블럭의 조건 값의 일부입니다:

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

변수	설명
`${aws:SourceIp}`	SOURCEIP 키를 제공된 변수로 사용합니다.
`${aws:username}`	제공된 변수로 사용자 이름 키를 사용합니다.
`${s3:prefix}`	서비스별 prefix key를 제공된 variable 로 사용한다.
`${s3:max-keys}`	서비스별 최대 키 키를 제공된 변수로 사용합니다.
`${*}`	특수 문자. 문자를 리터럴 * 문자로 사용합니다.
`${?}`	특수 문자. 문자를 리터럴로 사용합니까? 문자.
`${$}`	특수 문자. 문자를 리터럴 $ 문자로 사용합니다.

특별한 처리가 필요한 정책을 생성합니다

때로는 정책에 따라 보안이 위험하거나 계정 루트 사용자를 잠그는 등 지속적인 작업에 위험한 사용 권한을 부여할 수 있습니다. StorageGRID S3 REST API 구현은 Amazon보다 정책 검증 중에 덜 제한적이지만 정책 평가 중에도 동일하게 엄격합니다.

정책 설명입니다	정책 유형입니다	아마존 행동	**StorageGRID** 동작
루트 계정에 대한 모든 권한을 스스로 거부합니다	버킷	유효하고 적용되지만 루트 사용자 계정은 모든 S3 버킷 정책 작업에 대한 권한을 보유합니다	동일합니다
사용자/그룹에 대한 모든 권한을 스스로 거부합니다	그룹	유효하고 시행되었습니다	동일합니다
외부 계정 그룹에 모든 권한을 허용합니다	버킷	주체가 잘못되었습니다	유효하지만 모든 S3 버킷 정책 작업에 대한 권한은 정책에서 허용하는 경우 405 메서드 허용되지 않음 오류를 반환합니다

정책 설명입니다	정책 유형입니다	아마존 행동	**StorageGRID** 동작
외부 계정 루트 또는 사용자에게 모든 권한을 허용합니다	버킷	유효하지만 모든 S3 버킷 정책 작업에 대한 권한은 정책에서 허용하는 경우 405 메서드 허용되지 않음 오류를 반환합니다	동일합니다
모든 사용자에게 모든 작업에 대한 사용 권한을 허용합니다	버킷	유효하지만 모든 S3 버킷 정책 작업에 대한 사용 권한이 외국 계정 루트 및 사용자에 대해 405 메서드 허용 안 됨 오류를 반환합니다	동일합니다
모든 작업에 대한 모든 사용자의 권한을 거부합니다	버킷	유효하고 적용되지만 루트 사용자 계정은 모든 S3 버킷 정책 작업에 대한 권한을 보유합니다	동일합니다
보안 주체는 존재하지 않는 사용자 또는 그룹입니다	버킷	주체가 잘못되었습니다	유효합니다
리소스가 존재하지 않는 S3 버킷입니다	그룹	유효합니다	동일합니다
보안 주체는 로컬 그룹입니다	버킷	주체가 잘못되었습니다	유효합니다
정책은 개체를 넣을 수 있는 비소유자 계정(익명 계정 포함) 권한을 부여합니다	버킷	유효합니다. 객체는 생성자 계정이 소유하며 버킷 정책은 적용되지 않습니다. 생성자 계정은 개체 ACL을 사용하여 개체에 대한 액세스 권한을 부여해야 합니다.	유효합니다. 오브젝트는 버킷 소유자 계정이 소유합니다. 버킷 정책이 적용됩니다.

WORM(Write-Once-Read-Many) 보호

WORM(Write-Once-Read-Many) 버킷을 생성하여 데이터, 사용자 정의 오브젝트 메타데이터 및 S3 오브젝트 태깅을 보호할 수 있습니다. 새 객체를 생성하고 기존 컨텐츠를 덮어쓰거나 삭제하지 못하도록 WORM 버킷을 구성합니다. 여기에 설명된 방법 중 하나를 사용합니다.

덮어쓰기가 항상 거부되도록 하려면 다음을 수행할 수 있습니다.

- Grid Manager에서 * 구성 * > * 보안 * > * 보안 설정 * > * 네트워크 및 개체 * 로 이동하여 * 클라이언트 수정 방지 * 확인란을 선택합니다.
- 다음 규칙 및 S3 정책을 적용합니다.
  - S3 정책에 PutOverwriteObject 거부 작업을 추가합니다.
  - DeleteObject 거부 작업을 S3 정책에 추가합니다.

◦ S3 정책에 오브젝트 허용(Put Object Allow) 작업을 추가합니다.

S3 정책에서 DeleteObject 를 deny 로 설정해도 ""30일 후 0개 복사본""과 같은 규칙이 있을 때 ILM이 개체를 삭제하는 것을 차단하지 않습니다.

이러한 규칙과 정책이 모두 적용되더라도 동시 쓰기를 방지하지 않습니다(상황 A 참조). 순차적 완료된 덮어쓰기를 방지합니다(상황 B 참조).

- 상황 A *: 동시 쓰기(보호 안 됨)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

- 상황 B *: 순차적 완료된 덮어쓰기(방지됨)

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

관련 정보

- "StorageGRID ILM 규칙이 개체를 관리하는 방법"
- "버킷 정책의 예"
- "그룹 정책의 예"
- "ILM을 사용하여 개체를 관리합니다"
- "테넌트 계정을 사용합니다"

버킷 정책의 예

이 섹션의 예를 사용하여 버킷에 대한 StorageGRID 액세스 정책을 구축합니다.

버킷 정책은 정책이 연결된 버킷에 대한 액세스 권한을 지정합니다. 버킷 정책은 S3 PutBucketPolicy API를 사용하여 구성됩니다. 을 참조하십시오 "버킷 작업".

다음 명령에 따라 AWS CLI를 사용하여 버킷 정책을 구성할 수 있습니다.

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

예: 모든 사용자가 버킷에 읽기 전용 액세스를 허용합니다

이 예제에서는 anonymous 를 비롯한 모든 사람이 버킷에 있는 오브젝트를 나열하고 버킷에 있는 모든 오브젝트에 대해 오브젝트 가져오기 작업을 수행할 수 있습니다. 다른 모든 작업은 거부됩니다. 이 정책은 계정 루트 외에는 버킷에 쓸 수

있는 권한이 없으므로 특히 유용하지 않을 수 있습니다.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

예: 한 계정의 모든 사용자가 완전히 액세스할 수 있도록 허용하고 다른 계정의 모든 사용자는 버킷에 읽기 전용으로 액세스할 수 있습니다

이 예제에서는 지정된 계정의 모든 사용자가 버킷에 완전히 액세스할 수 있지만, 지정된 다른 계정의 모든 사용자는 버킷을 나열하고 으로 시작하는 버킷의 개체에 대해 GetObject 작업만 수행할 수 있습니다 `shared/` 개체 키 접두사입니다.

> StorageGRID에서 비소유자 계정(익명 계정 포함)으로 생성된 객체는 버킷 소유자 계정이 소유합니다. 버킷 정책은 이러한 오브젝트에 적용됩니다.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

예: 모든 사용자가 버킷에 대한 읽기 전용 액세스 및 지정된 그룹에 의한 전체 액세스 허용

이 예제에서는 anonymous 를 포함한 모든 사용자가 버킷을 나열하고 버킷의 모든 오브젝트에 대해 오브젝트 가져오기 작업을 수행할 수 있지만 그룹에 속한 사용자만 수행할 수 있습니다 `Marketing` 지정된 계정에서 전체 액세스가 허용됩니다.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket","s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

예: 클라이언트가 **IP** 범위에 있는 경우 모든 사용자가 버킷에 대한 읽기 및 쓰기 액세스를 허용합니다

이 예제에서는 요청이 지정된 IP 범위(54.240.143.0 ~ 54.240.143.255, 54.240.143.188 제외)에서 발생한 경우 anonymous를 포함한 모든 사람이 버킷을 나열하고 버킷의 모든 오브젝트에 대해 오브젝트 작업을 수행할 수 있습니다. 다른 모든 작업이 거부되고 IP 범위를 벗어난 모든 요청이 거부됩니다.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

예: 지정된 통합 사용자가 단독으로 버킷을 완전히 액세스할 수 있도록 허용합니다

이 예에서는 페더레이션 사용자 Alex가 에 대한 전체 액세스를 허용합니다 `examplebucket` 버킷과 그 물체. "root"를 포함한 다른 모든 사용자는 모든 작업을 명시적으로 거부합니다. 그러나 "root"는 PUT/GET/DeleteBucketPolicy에 대한 권한이 거부되지 않습니다.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

예: **PutOverwriteObject** 권한

이 예에서 는 입니다 `Deny` PutOverwriteObject 및 DeleteObject 에 대한 효과 개체의 데이터, 사용자 정의 메타데이터 및 S3 개체 태그 지정을 덮어쓰거나 삭제할 수 없습니다.

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

그룹 정책의 예

이 섹션의 예제를 사용하여 그룹에 대한 StorageGRID 액세스 정책을 작성합니다.

그룹 정책은 정책이 연결된 그룹에 대한 액세스 권한을 지정합니다. 아니요 `Principal` 암시적 정책이므로 정책의 요소입니다. 그룹 정책은 테넌트 관리자 또는 API를 사용하여 구성됩니다.

예: 테넌트 관리자를 사용하여 그룹 정책을 설정합니다

테넌트 관리자에서 그룹을 추가하거나 편집할 때 그룹 정책을 선택하여 이 그룹의 구성원이 가질 S3 액세스 권한을

결정할 수 있습니다. 을 참조하십시오 "S3 테넌트에 대한 그룹을 생성합니다".

- * S3 액세스 없음 *: 기본 옵션. 버킷 정책을 통해 액세스 권한이 부여되지 않은 한 이 그룹의 사용자는 S3 리소스에 액세스할 수 없습니다. 이 옵션을 선택하면 루트 사용자만 기본적으로 S3 리소스에 액세스할 수 있습니다.
- * 읽기 전용 액세스 *: 이 그룹의 사용자는 S3 리소스에 대한 읽기 전용 액세스 권한을 가집니다. 예를 들어 이 그룹의 사용자는 개체를 나열하고 개체 데이터, 메타데이터 및 태그를 읽을 수 있습니다. 이 옵션을 선택하면 읽기 전용 그룹 정책의 JSON 문자열이 텍스트 상자에 나타납니다. 이 문자열을 편집할 수 없습니다.
- * 전체 액세스 *: 이 그룹의 사용자는 버킷을 포함하여 S3 리소스에 대한 모든 액세스 권한을 가집니다. 이 옵션을 선택하면 전체 액세스 그룹 정책의 JSON 문자열이 텍스트 상자에 나타납니다. 이 문자열을 편집할 수 없습니다.
- * 랜섬웨어 완화 *: 이 샘플 정책은 이 테넌트의 모든 버킷에 적용됩니다. 이 그룹의 사용자는 일반적인 작업을 수행할 수 있지만 개체 버전 관리가 활성화된 버킷에서 개체를 영구적으로 삭제할 수는 없습니다.

  모든 버킷 관리 권한이 있는 테넌트 관리자 사용자는 이 그룹 정책을 재정의할 수 있습니다. 모든 버킷 관리 권한을 신뢰할 수 있는 사용자로 제한하고 가능한 경우 MFA(Multi-Factor Authentication)를 사용합니다.

- * 사용자 정의 *: 그룹의 사용자에게는 텍스트 상자에 지정한 사용 권한이 부여됩니다.

예: 모든 버킷에 대한 그룹 전체 액세스 허용

이 예에서 그룹의 모든 구성원은 버킷 정책에 의해 명시적으로 거부되지 않는 한 테넌트 계정이 소유한 모든 버킷에 대해 전체 액세스가 허용됩니다.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

예: 모든 버킷에 대한 그룹 읽기 전용 액세스를 허용합니다

이 예제에서 그룹의 모든 구성원은 버킷 정책에 의해 명시적으로 거부되지 않는 한 S3 리소스에 대해 읽기 전용 액세스 권한을 갖습니다. 예를 들어 이 그룹의 사용자는 개체를 나열하고 개체 데이터, 메타데이터 및 태그를 읽을 수 있습니다.

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

예: 그룹 구성원이 버킷의 "" 폴더에만 완전히 액세스할 수 있도록 허용합니다

이 예제에서 그룹의 구성원은 지정된 버킷의 특정 폴더(키 접두사)를 나열하고 액세스할 수만 있습니다. 이러한 폴더의 개인 정보를 확인할 때는 다른 그룹 정책 및 버킷 정책의 액세스 권한을 고려해야 합니다.

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```