TR-4921: 랜섬웨어 방어

How to enable StorageGRID in your environment

NetApp
July 05, 2024

목차

TR-4921: 랜섬웨어 방어

랜섬웨어로부터 StorageGRID S3 오브젝트 보호

StorageGRID 보안 모범 사례로 랜섬웨어 공격과 데이터를 보호하는 방법에 대해 알아보십시오.

랜섬웨어 공격이 증가하고 있습니다. 이 문서에서는 StorageGRID에서 개체 데이터를 보호하는 방법에 대한 몇 가지 권장 사항을 제공합니다.

오늘날의 랜섬웨어는 데이터 센터에 있어서 항상 존재하는 위험입니다. 랜섬웨어는 데이터를 암호화하여 사용하는 사용자 및 애플리케이션이 사용할 수 없도록 설계되었습니다. 보안은 강화된 네트워킹과 견고한 사용자 보안 관행의 일반적인 방어부터 시작하며, 데이터 액세스 보안 관행에 따라야 합니다.

랜섬웨어는 오늘날 가장 큰 보안 위협 중 하나입니다. NetApp StorageGRID 팀은 이러한 위협에 대비하기 위해 고객과 협력하고 있습니다. 개체 잠금 및 버전 관리를 사용하면 원치 않는 변경을 방지하고 악의적인 공격으로부터 복구할 수 있습니다. 데이터 보안은 오브젝트 스토리지가 데이터 센터의 한 부분에 불과합니다.

StorageGRID 모범 사례

StorageGRID의 경우 보안 모범 사례에는 관리 및 개체 액세스를 위해 서명된 인증서와 함께 HTTPS를 사용하는 것이 포함되어야 합니다. 애플리케이션 및 개인에 대한 전용 사용자 계정을 생성하고 애플리케이션 액세스 또는 사용자 데이터 액세스에 테넌트 루트 계정을 사용하지 마십시오. 즉, 최소 권한 원칙을 따릅니다. IAM(Identity and Access Management) 정책이 정의된 보안 그룹을 사용하여 사용자 권한을 관리하고 응용 프로그램 및 사용자에 고유한 계정에 액세스합니다. 적절한 조치를 취하는 동안에도 데이터를 보호해야 합니다. S3(Simple Storage Service)의 경우 오브젝트를 암호화하도록 수정하면 원래 오브젝트를 덮어쓰면 수행됩니다.

방어방법

S3 API의 기본 랜섬웨어 보호 메커니즘은 오브젝트 잠금을 구현하는 것입니다. 모든 애플리케이션이 오브젝트 잠금과 호환되지 않으므로 이 보고서에서 설명하는 오브젝트를 보호하기 위한 다른 두 가지 옵션, 즉 버전 관리가 활성화된 다른 버킷으로의 복제 및 IAM 정책을 통한 버전 관리가 있습니다.

추가 정보를 찾을 수 있는 위치

이 문서에 설명된 정보에 대해 자세히 알아보려면 다음 문서 및/또는 웹 사이트를 검토하십시오.

- NetApp StorageGRID 문서 센터 https://docs.netapp.com/us-en/storagegrid-118/
- NetApp StorageGRID 지원 https://docs.netapp.com/us-en/storagegrid-enable/
- StorageGRID 문서 리소스 페이지 https://www.netapp.com/data-storage/storagegrid/documentation/
- NetApp 제품 설명서 https://www.netapp.com/support-and-training/documentation/

오브젝트 잠금을 사용한 랜섬웨어 방어

StorageGRID의 오브젝트 잠금이 WORM 모델을 제공하여 데이터 삭제 또는 덮어쓰기를 방지하는 방법과 규정 요구사항을 충족하는 방법에 대해 알아보십시오.

오브젝트 잠금은 WORM 모델을 제공하여 오브젝트를 삭제하거나 덮어쓰지 못하도록 합니다. StorageGRID은

오브젝트 잠금 구축을 "Cohasset 평가됨" 통해 규정 요구사항을 충족하고, 오브젝트 보존에 대한 법적 증거 자료 보관, 규정 준수 모드, 거버넌스 모드와 기본 버킷 보존 정책을 지원합니다. 버킷 생성 및 버전 관리에서 오브젝트 잠금을 활성화해야 합니다. 개체의 특정 버전이 잠겨 있으며 버전 ID가 정의되지 않은 경우 현재 버전의 개체에 보존이 배치됩니다. 현재 버전에 보존이 구성되어 있고 개체를 삭제, 수정 또는 덮어쓰려고 하면 삭제 표식 또는 개체의 새 수정본을 현재 버전으로 사용하여 새 버전이 만들어집니다. 잠긴 버전은 현재 버전이 아닌 버전으로 유지됩니다. 아직 호환되지 않는 애플리케이션의 경우 오브젝트 잠금과 버킷에 배치된 기본 보존 구성을 계속 사용할 수 있습니다. 구성이 정의된 후 버킷에 삽입되는 각 새 오브젝트에 오브젝트 보존을 적용합니다. 보존 시간이 경과하기 전에 응용 프로그램이 개체를 삭제하거나 덮어쓰지 않도록 구성된 한 이 기능은 작동합니다.

다음은 Object Lock API를 사용하는 몇 가지 예입니다.

오브젝트 잠금 법적 보관은 오브젝트에 적용되는 간단한 켜기/끄기 상태입니다.

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal
-hold Status=ON --endpoint-url https://s3.company.com
```

법적 증거 자료 보관 상태를 설정해도 성공하면 어떤 값도 반환되지 않으므로 가져오기 작업으로 확인할 수 있습니다.

```
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "LegalHold": {
        "Status": "ON"
    }
}
```

법적 보류를 해제하려면 끄기 상태를 적용합니다.

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal
-hold Status=OFF --endpoint-url https://s3.company.com
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "LegalHold": {
        "Status": "OFF"
    }
}
```

객체 보존 설정은 Retain until timestamp로 설정됩니다.

```
aws s3api put-object-retention --bucket mybucket --key myfile.txt
--retention '{"Mode":"COMPLIANCE", "RetainUntilDate": "2022-06-
10T16:00:00"}'  --endpoint-url https://s3.company.com
```

다시 한 번 말씀드리지만 성공 시 반환된 값이 없으므로 GET 호출과 마찬가지로 보존 상태를 확인할 수 있습니다.

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-06-10T16:00:00+00:00"
    }
```

객체 잠금이 활성화된 버킷에 기본 보존을 설정하면 보존 기간이 일 및 년 단위로 사용됩니다.

```
aws s3api put-object-lock-configuration --bucket mybucket --object-lock
-configuration '{ "ObjectLockEnabled": "Enabled", "Rule": {
"DefaultRetention": { "Mode": "COMPLIANCE", "Days": 1 }}}' --endpoint-url
https://s3.company.com
```

대부분의 작업과 마찬가지로 성공 시 응답이 반환되지 않으므로 확인할 구성에 대해 GET를 수행할 수 있습니다.

```
aws s3api get-object-lock-configuration --bucket mybucket --endpoint-url
https://s3.company.com
{
    "ObjectLockConfiguration": {
        "ObjectLockEnabled": "Enabled",
        "Rule": {
            "DefaultRetention": {
                "Mode": "COMPLIANCE",
                "Days": 1
            }
        }
    }
}
```

다음으로, 보존 구성이 적용된 상태로 버켓에 객체를 넣을 수 있습니다.

```
aws s3 cp myfile.txt s3://mybucket --endpoint-url https://s3.company.com
```

Put 작업이 응답을 반환합니다.

```
upload: ./myfile.txt to s3://mybucket/myfile.txt
```

보존 개체에서 이전 예제에서 버킷에 설정된 보존 기간은 개체의 보존 타임스탬프로 변환됩니다.

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt
--endpoint-url https://s3.company.com
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-03-02T15:22:47.202000+00:00"
    }
}
```

버전 관리와 함께 복제된 버킷을 사용하는 랜섬웨어 방어

StorageGRID CloudMirror를 사용하여 오브젝트를 보조 버킷으로 복제하는 방법에 대해 알아보십시오.

모든 애플리케이션과 워크로드가 오브젝트 잠금과 호환되지 않습니다. 또 다른 옵션은 오브젝트를 동일한 그리드(액세스가 제한된 다른 테넌트 권장) 또는 StorageGRID 플랫폼 서비스를 사용하는 기타 S3 엔드포인트인 CloudMirror에 복제하는 것입니다.

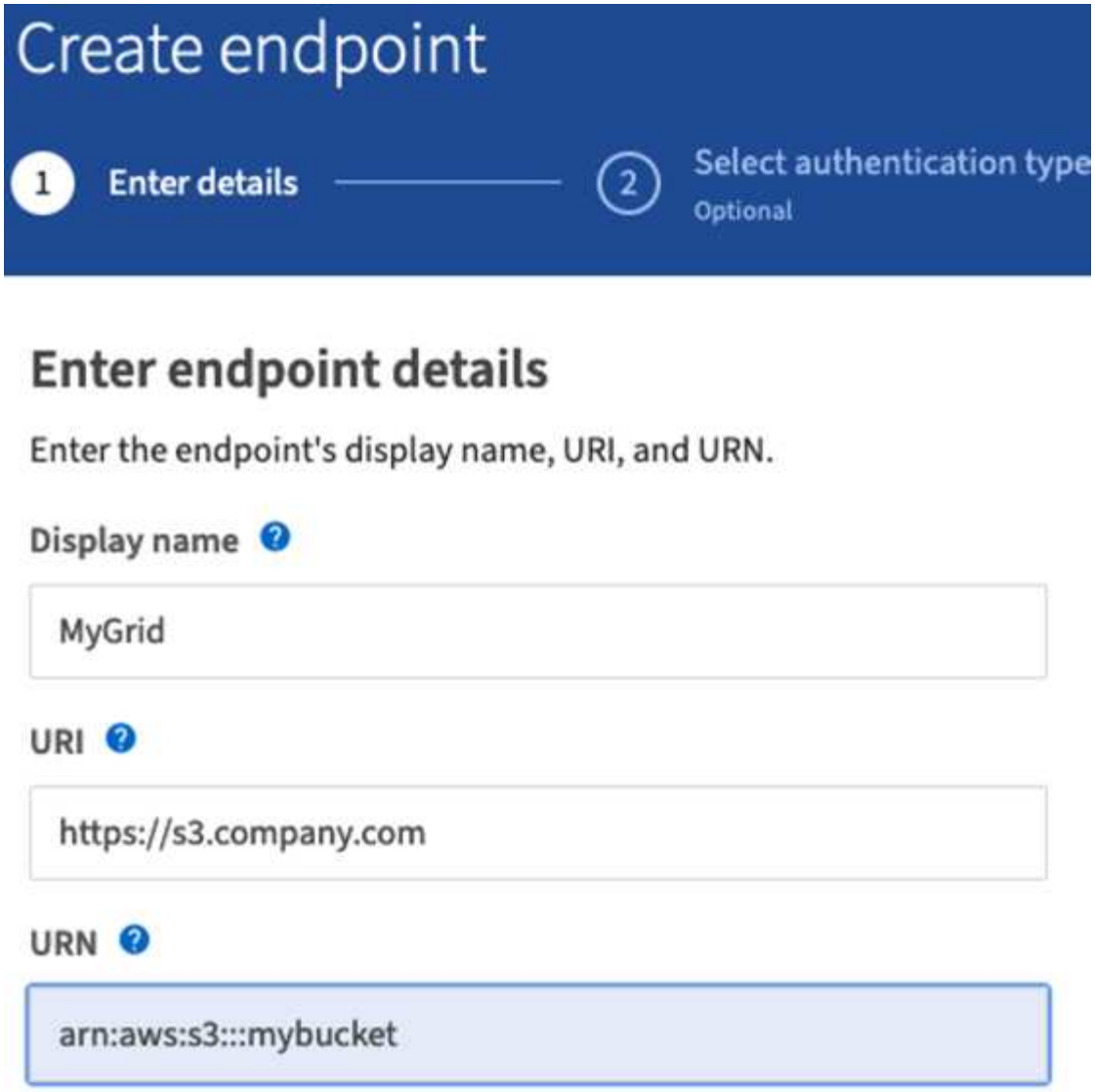
StorageGRID CloudMirror는 StorageGRID의 구성 요소로, 버킷의 오브젝트를 소스 버킷에 수집될 때 정의된 대상에 복제하도록 구성할 수 있으며 삭제를 복제하지 않는다. CloudMirror는 StorageGRID의 통합 구성 요소이므로 S3 API 기반 공격에 의해 해제하거나 조작할 수 없습니다. 버전 관리를 사용하도록 설정한 상태에서 이 복제된 버킷을 구성할 수 있습니다. 이 시나리오에서는 폐기해도 안전한 복제된 버킷의 이전 버전을 자동으로 정리해야 합니다. 이를 위해 StorageGRID ILM 정책 엔진을 사용할 수 있습니다. 공격을 식별하고 복구하기에 충분한 며칠간 현재 시간을 기준으로 개체 배치를 관리하는 규칙을 만듭니다.

이 접근 방식의 한 가지 단점은 버킷의 완전한 두 번째 복사본과 일정 시간 동안 유지되는 오브젝트의 여러 버전을 확보함으로써 더 많은 스토리지를 소비한다는 것입니다. 또한 기본 버킷에서 의도적으로 삭제된 객체를 복제된 버킷에서 수동으로 제거해야 합니다. NetApp CloudSync와 같은 제품 이외의 다른 복제 옵션으로는 비슷한 솔루션에 대해 삭제 작업을 복제할 수 있습니다. 버전 관리가 활성화되고 객체 잠금이 설정되지 않은 보조 버킷의 또 다른 단점은 보조 위치에 손상을 일으키는 데 사용할 수 있는 권한이 있는 계정이 많다는 것입니다. 장점은 해당 엔드포인트 또는 테넌트 버킷에 대한 고유한 계정이어야 하며, 주 위치의 계정에 대한 액세스 권한이 포함되지 않거나 그 반대의 경우도 마찬가지입니다.

소스 및 대상 버킷을 생성하고 대상이 버전 관리로 구성된 후에는 다음과 같이 복제를 구성하고 설정할 수 있습니다.

단계

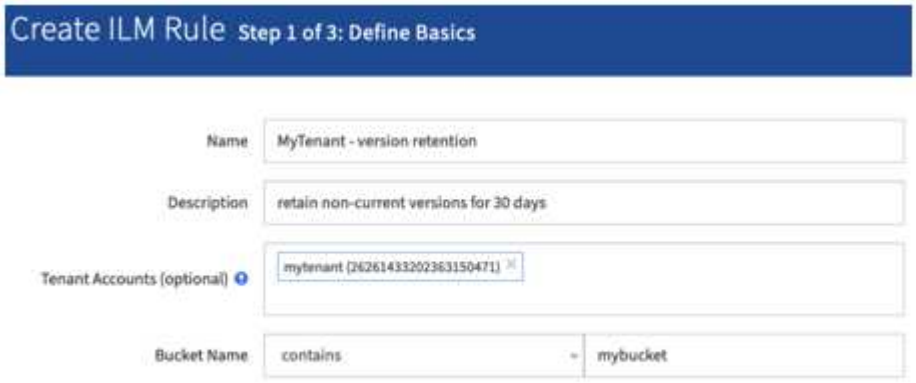
1. CloudMirror를 구성하려면 S3 대상에 대한 플랫폼 서비스 엔드포인트를 생성합니다.

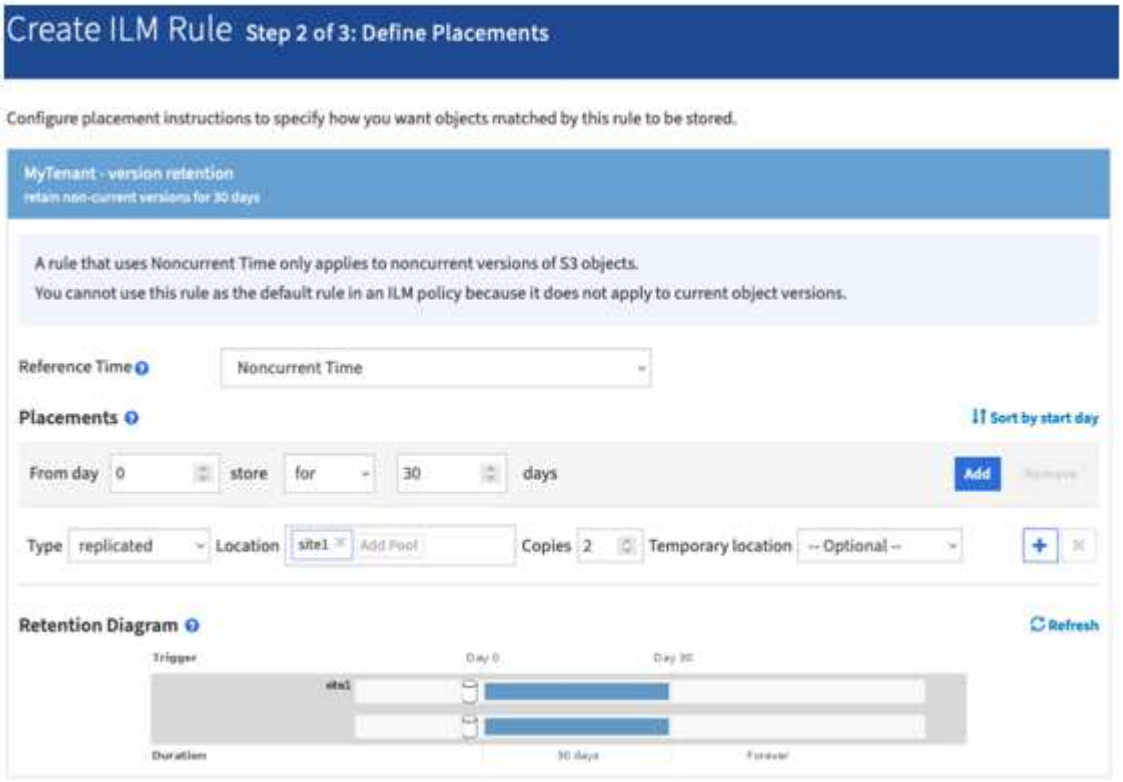


2. 소스 버킷에서 구성된 엔드포인트를 사용하도록 복제를 구성합니다.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
            <Bucket>arn:aws:s3:::mybucket</Bucket>
            <StorageClass>STANDARD</StorageClass>
        </Destination>
    </Rule>
</ReplicationConfiguration>
```

3. 스토리지 배치 및 버전 스토리지 기간 관리를 관리하는 ILM 규칙을 생성합니다. 이 예에서는 저장할 객체의 최신 버전이 아닌 버전이 구성되어 있습니다.





30일 동안 사이트 1에 2개의 복사본이 있습니다. 또한 소스 버킷 스토리지 기간과 일치하도록 ILM 규칙에서 수집 시간을 참조 시간으로 사용하는 것을 기반으로 오브젝트의 현재 버전에 대한 규칙을 구성합니다. 오브젝트 버전에 대한 스토리지 배치는 삭제 코딩 또는 복제할 수 있습니다.

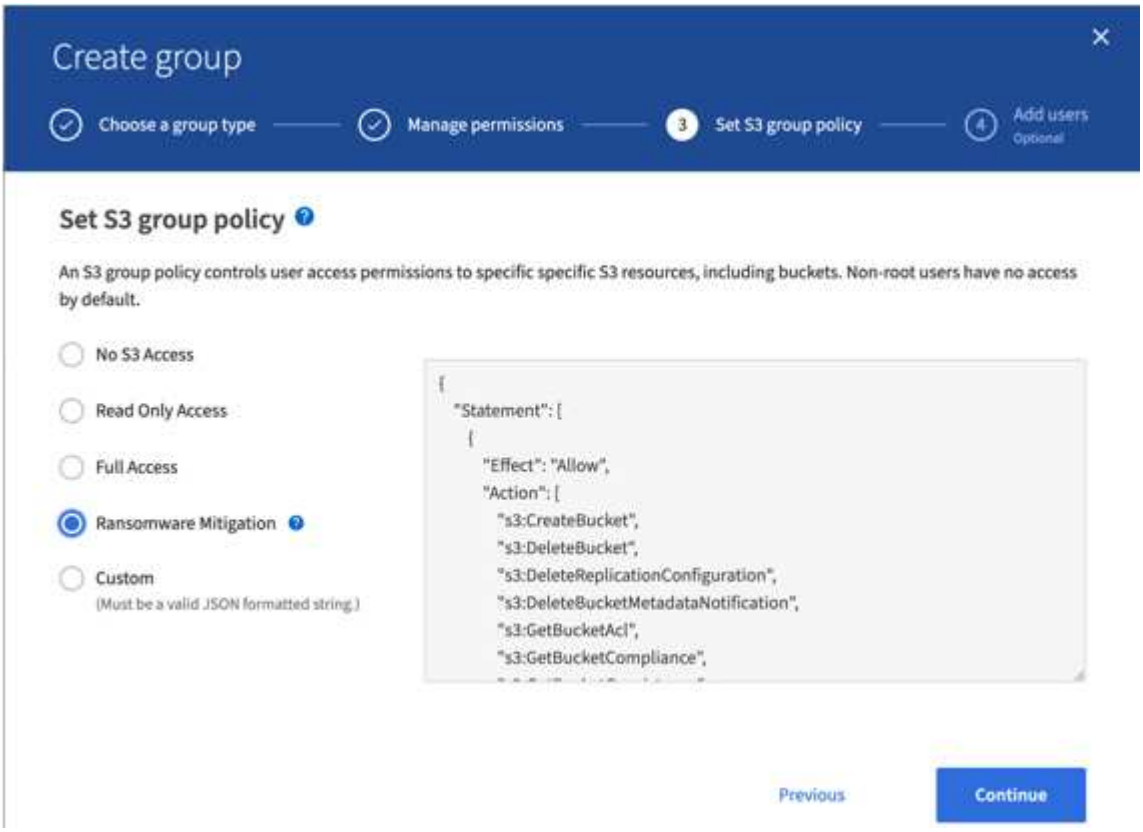
보호 **IAM** 정책을 통한 버전 관리를 사용한 랜섬웨어 방어

버킷에서 버전 관리를 활성화하고 StorageGRID의 사용자 보안 그룹에 IAM 정책을 구현하여 데이터를 보호하는 방법에 대해 알아보십시오.

오브젝트 잠금 또는 복제를 사용하지 않고 데이터를 보호하는 방법은 버킷에서 버전 관리를 활성화하고 사용자 보안 그룹에 IAM 정책을 구현하여 사용자의 오브젝트 버전 관리 기능을 제한하는 것입니다. 공격이 발생할 경우 데이터의 잘못된 새 버전이 현재 버전으로 만들어지고 최신 버전이 아닌 최신 버전이 안전한 클린 데이터입니다. 데이터에 대한 액세스를 얻기 위해 손상된 계정에는 나중에 복원 작업을 위해 데이터를 보호하는 최신 버전이 아닌 버전을 삭제하거나 변경할 수 있는 액세스 권한이 없습니다. 이전 시나리오와 마찬가지로 ILM 규칙은 사용자가 선택한 기간 동안 비최신

버전의 보존을 관리합니다. 단점은 공격자 공격에 대한 권한이 있는 계정이 존재할 가능성이 여전히 존재하지만 모든 응용 프로그램 서비스 계정과 사용자는 보다 제한적인 액세스를 사용하여 구성해야 한다는 것입니다. 제한 그룹 정책은 사용자 또는 응용 프로그램에서 수행할 수 있는 각 작업을 명시적으로 허용해야 하며, 사용자가 수행할 수 없도록 하려는 모든 작업은 명시적으로 거부해야 합니다. 앞으로 새 작업이 도입될 수 있으므로 와일드카드 ALLOW를 사용하지 않는 것이 좋습니다. 이 경우 허용할지 거부할지 여부를 제어할 수 있습니다 NetApp. 이 솔루션의 경우 거부 목록에는 사용자 또는 프로그래밍 방식의 변경으로부터 버킷 및 개체 버전의 버전 관리를 보호하기 위해 DeleteObjectVersion, PutBucketPolicy, DeleteBucketPolicy, PutLifecycleConfiguration 및 PutBucketVersioning이 포함되어야 합니다.

StorageGRID 11.7에는 이 솔루션을 더 쉽게 구현할 수 있도록 새로운 S3 그룹 정책 옵션 "랜섬웨어 완화"가 도입되었습니다. 테넌트에서 사용자 그룹을 생성할 때 그룹 권한을 선택하면 이 새로운 옵션 정책을 볼 수 있습니다.



다음은 명시적으로 허용되는 대부분의 사용 가능한 작업과 필요한 최소 거부 작업이 포함된 그룹 정책의 내용입니다.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteReplicationConfiguration",
"s3:DeleteBucketMetadataNotification",
                "s3:GetBucketAcl",
                "s3:GetBucketCompliance",
                "s3:GetBucketConsistency",
                "s3:GetBucketLastAccessTime",
```

```
                "s3:GetBucketLocation",
                "s3:GetBucketNotification"
"s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicy",
                "s3:GetBucketMetadataNotification",
                "s3:GetReplicationConfiguration",
                "s3:GetBucketCORS",
                "s3:GetBucketVersioning",
                "s3:GetBucketTagging",
                "s3:GetEncryptionConfiguration",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:ListAllMyBuckets",
                "s3:ListBucketMultipartUploads",
                "s3:PutBucketConsistency",
                "s3:PutBucketLastAccessTime",
                "s3:PutBucketNotification",
"s3:PutBucketObjectLockConfiguration",
                "s3:PutReplicationConfiguration",
                "s3:PutBucketCORS",
                "s3:PutBucketMetadataNotification",
                "s3:PutBucketTagging",
                "s3:PutEncryptionConfiguration",
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectVersionTagging",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectLegalHold",
                "s3:PutObjectRetention",
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging",
                "s3:RestoreObject",
                "s3:ValidateObject",
                "s3:PutBucketCompliance",
```

```
                "s3:PutObjectVersionAcl"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "s3:DeleteObjectVersion",
                "s3:DeleteBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketVersioning"
            ],
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```