



절차 및 **API** 예

How to enable StorageGRID in your environment

NetApp
April 26, 2024

목차

절차 및 API 예	1
StorageGRID에서 S3 암호화 옵션 테스트 및 시연	1
StorageGRID에서 S3 오브젝트 잠금을 테스트하고 시연합니다	4
버킷 및 그룹(IAM) 정책의 예	9

절차 및 API 예

StorageGRID에서 S3 암호화 옵션 테스트 및 시연

StorageGRID와 S3 API를 사용하면 유향 데이터를 다양한 방법으로 암호화할 수 있습니다. 자세한 내용은 [을 참조하십시오 "StorageGRID 암호화 방법을 검토합니다"](#).

이 가이드에서는 S3 API 암호화 방법을 보여 줍니다.

서버 측 암호화(SSE)

SSE를 사용하면 클라이언트가 개체를 저장하고 StorageGRID에서 관리하는 고유 키로 암호화할 수 있습니다. 개체가 요청되면 StorageGRID에 저장된 키에 의해 개체가 해독됩니다.

SSE 예

- SSE가 있는 개체를 넣습니다

```
aws s3api put-object --bucket <bucket> --key <file> --body "<file>"  
--server-side-encryption AES256 --endpoint-url https://s3.example.com
```

- 객체를 확인하여 암호화를 확인합니다

```
aws s3api head-object --bucket <bucket> --key <file> --endpoint-url  
https://s3.example.com
```

```
{  
  "AcceptRanges": "bytes",  
  "LastModified": "2022-05-02T19:03:03+00:00",  
  "ContentLength": 47,  
  "ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",  
  "ContentType": "text/plain",  
  "ServerSideEncryption": "AES256",  
  "Metadata": {}  
}
```

- 객체를 가져옵니다

```
aws s3api get-object --bucket <bucket> --key <file> <file> --endpoint  
-url https://s3.example.com
```

고객 제공 키(SSE-C)를 사용한 서버측 암호화

SSE를 사용하면 클라이언트가 객체를 저장하고 해당 객체와 함께 제공된 고유 키를 사용하여 해당 객체를 암호화할 수 있습니다. 개체가 요청될 때 개체를 해독하고 반환하려면 동일한 키를 제공해야 합니다.

SSE-C의 예

- 테스트 또는 데모용으로 암호화 키를 만들 수 있습니다
 - 암호화 키를 만듭니다

```
openssl enc -aes-128-cbc -pass pass:secret -P`
```

```
salt=E9DBB6603C7B3D2A  
key=23832BAC16516152E560F933F261BF03  
iv =71E87C0F6EC3C45921C2754BA131A315
```

- 생성된 키가 있는 개체를 넣습니다

```
aws s3api put-object --bucket <bucket> --key <file> --body "file" --sse  
-customer-algorithm AES256 --sse-customer-key  
23832BAC16516152E560F933F261BF03 --endpoint-url https://s3.example.com
```

- 물체를 향하십시오

```
aws s3api head-object --bucket <bucket> --key <file> --sse-customer  
-algorithm AES256 --sse-customer-key 23832BAC16516152E560F933F261BF03  
--endpoint-url https://s3.example.com
```

```
{  
  "AcceptRanges": "bytes",  
  "LastModified": "2022-05-02T19:20:02+00:00",  
  "ContentLength": 47,  
  "ETag": "\"f92ef20ab87e0e13951d9bee862e9f9a\"",  
  "ContentType": "binary/octet-stream",  
  "Metadata": {},  
  "SSECustomerAlgorithm": "AES256",  
  "SSECustomerKeyMD5": "rjGuMdjLpPV1eRuotNaPMQ=="  
}
```



암호화 키를 제공하지 않으면 "HeadObject 작업을 호출할 때 오류 발생(404): 찾을 수 없음" 오류가 발생합니다.

- 객체를 가져옵니다

```
aws s3api get-object --bucket <bucket> --key <file> <file> --sse
--customer-algorithm AES256 --sse-customer-key
23832BAC16516152E560F933F261BF03 --endpoint-url https://s3.example.com
```



암호화 키를 제공하지 않으면 "GetObject 작업을 호출할 때 오류가 발생했습니다(InvalidRequest). 즉, 개체가 서버측 암호화 형식을 사용하여 저장되었습니다."라는 오류가 발생합니다. 객체를 검색하려면 올바른 매개 변수를 제공해야 합니다."

버킷 서버 측 암호화(SSE-S3)

SSE-S3를 사용하면 클라이언트가 버킷에 저장된 모든 오브젝트에 대해 기본 암호화 동작을 정의할 수 있습니다. 개체는 StorageGRID 에서 관리하는 고유 키로 암호화됩니다. 개체가 요청되면 StorageGRID 에 저장된 키에 의해 개체가 해독됩니다.

버킷 SSE-S3의 예

- 새 버킷을 생성하고 기본 암호화 정책을 설정합니다
 - 새 버킷을 생성합니다

```
aws s3api create-bucket --bucket <bucket> --region us-east-1
--endpoint-url https://s3.example.com
```

- 버킷 암호화

```
aws s3api put-bucket-encryption --bucket <bucket> --server-side
--encryption-configuration '{"Rules":
[{"ApplyServerSideEncryptionByDefault": {"SSEAlgorithm":
"AES256"}}]}' --endpoint-url https://s3.example.com
```

- 물체를 버킷에 넣으십시오

```
aws s3api put-object --bucket <bucket> --key <file> --body "file"
--endpoint-url https://s3.example.com
```

- 물체를 향하십시오

```
aws s3api head-object --bucket <bucket> --key <file> --endpoint-url https://s3.example.com
```

```
{
  "AcceptRanges": "bytes",
  "LastModified": "2022-05-02T20:16:23+00:00",
  "ContentLength": 47,
  "ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
  "ContentType": "binary/octet-stream",
  "ServerSideEncryption": "AES256",
  "Metadata": {}
}
```

- 객체를 가져옵니다

```
aws s3api get-object --bucket <bucket> --key <file> <file> --endpoint-url https://s3.example.com
```

_ 아론 클라인 _

StorageGRID에서 S3 오브젝트 잠금을 테스트하고 시연합니다

Object Lock은 개체가 삭제되거나 덮어쓰지는 것을 방지하는 WORM 모델을 제공합니다. StorageGRID의 객체 잠금 구현은 규제 요구사항을 충족하고, 객체 보존에 대한 법적 보류 및 규정 준수 모드를 지원하고, 기본 버킷 보존 정책을 지원하는 데 도움이 되는 코호트 평가입니다.

이 가이드에서는 S3 오브젝트 잠금 API를 보여 줍니다.

법적 증거 자료 보관

- 개체 잠금 법적 보류는 개체에 적용되는 간단한 켜기/끄기 상태입니다.

```
aws s3api put-object-legal-hold --bucket <bucket> --key <file> --legal-hold Status=ON --endpoint-url https://s3.company.com
```

- 가져오기 작업으로 확인합니다.

```
aws s3api get-object-legal-hold --bucket <bucket> --key <file> --endpoint-url https://s3.company.com
```

```
{
  "LegalHold": {
    "Status": "ON"
  }
}
```

- 법적 증거 자료 보관 기능을 끕니다

```
aws s3api put-object-legal-hold --bucket <bucket> --key <file> --legal
--hold Status=OFF --endpoint-url https://s3.company.com
```

- 가져오기 작업으로 확인합니다.

```
aws s3api get-object-legal-hold --bucket <bucket> --key <file>
--endpoint-url https://s3.company.com
```

```
{
  "LegalHold": {
    "Status": "OFF"
  }
}
```

준수 모드

- 개체 보존은 타임스탬프까지 보존하여 수행됩니다.

```
aws s3api put-object-retention --bucket <bucket> --key <file>
--retention '{"Mode":"COMPLIANCE", "RetainUntilDate": "2025-06-
10T16:00:00"}' --endpoint-url https://s3.company.com
```

- 보존 상태를 확인합니다

```
aws s3api get-object-retention --bucket <bucket> --key <file> --endpoint
-url https://s3.company.com
+
```

```
{
  "Retention": {
    "Mode": "COMPLIANCE",
    "RetainUntilDate": "2025-06-10T16:00:00+00:00"
  }
}
```

기본 보존

- 객체 API에 정의된 보존 종료 날짜를 기준으로 보존 기간을 일 및 년 단위로 설정합니다.

```
aws s3api put-object-lock-configuration --bucket <bucket> --object-lock
-configuration '{"ObjectLockEnabled": "Enabled", "Rule": {
"DefaultRetention": { "Mode": "COMPLIANCE", "Days": 10 }}}' --endpoint
-url https://s3.company.com
```

- 보존 상태를 확인합니다

```
aws s3api get-object-lock-configuration --bucket <bucket> --endpoint-url
https://s3.company.com
```

```
{
  "ObjectLockConfiguration": {
    "ObjectLockEnabled": "Enabled",
    "Rule": {
      "DefaultRetention": {
        "Mode": "COMPLIANCE",
        "Days": 10
      }
    }
  }
}
```

- 물체를 버킷에 넣으십시오

```
aws s3api put-object --bucket <bucket> --key <file> --body "file"
--endpoint-url https://s3.example.com
```

- 버킷에 설정된 보존 기간은 객체의 보존 타임 스탬프로 변환됩니다.


```
aws s3api get-object-retention --bucket <bucket> --key <file> --endpoint-url https://s3.company.com
```

```
{
  "Retention": {
    "Mode": "COMPLIANCE",
    "RetainUntilDate": "2022-03-02T15:22:47.202000+00:00"
  }
}
```

정의된 보존 개체가 있는 개체 삭제 테스트

오브젝트 잠금은 버전 관리를 기반으로 합니다. 보존은 개체 버전에 정의됩니다. 보존이 정의되어 있고 버전이 지정되지 않은 개체를 삭제하려고 하면 삭제 표식이 개체의 현재 버전으로 만들어집니다.

- 보존이 정의된 개체를 삭제합니다

```
aws s3api delete-object --bucket <bucket> --key <file> --endpoint-url https://s3.example.com
```

- 버킷의 물체를 나열합니다

```
aws s3api list-objects --bucket <bucket> --endpoint-url https://s3.example.com
```

- 개체가 나열되지 않은 것을 확인합니다.

- 버전 목록을 사용하여 삭제 마커와 원래 잠긴 버전을 확인합니다

```
aws s3api list-object-versions --bucket <bucket> --prefix <file> --endpoint-url https://s3.example.com
```

```
{
  "Versions": [
    {
      "ETag": "\"82e8bfb872e778a4687a26e6c0b36bc1\"",
      "Size": 47,
      "StorageClass": "STANDARD",
      "Key": "file.txt",
      "VersionId":
"RDVDMjYwMTQtQkNDQS0xMUVDLThGOEUtNjQ3NTAwQzAxQTk1",
      "IsLatest": false,
      "LastModified": "2022-04-15T14:46:29.734000+00:00",
      "Owner": {
        "DisplayName": "Tenant01",
        "ID": "56622399308951294926"
      }
    }
  ],
  "DeleteMarkers": [
    {
      "Owner": {
        "DisplayName": "Tenant01",
        "ID": "56622399308951294926"
      },
      "Key": "file01.txt",
      "VersionId":
"QjVDQzgZOTAtQ0FGNi0xMUVDLThFMzgtQ0RGMjAwQjk0MjM1",
      "IsLatest": true,
      "LastModified": "2022-05-03T15:35:50.248000+00:00"
    }
  ]
}
```

- 객체의 잠긴 버전을 삭제합니다

```
aws s3api delete-object --bucket <bucket> --key <file> --version-id
"<VersionId>" --endpoint-url https://s3.example.com
```

An error occurred (AccessDenied) when calling the DeleteObject operation: Access Denied

_ 아론 클라인 _

버킷 및 그룹(IAM) 정책의 예

다음은 버킷 정책 및 그룹 정책(IAM 정책)의 예입니다.

그룹 정책(IAM)

홈 디렉토리 스타일 버킷 액세스

이 그룹 정책은 사용자가 사용자 이름이 인 버킷의 객체에 액세스하는 것만 허용합니다.

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

오브젝트 잠금 버킷 생성을 거부합니다

이 그룹 정책은 사용자가 버킷에 개체 잠금이 설정된 버킷을 생성할 수 없도록 제한합니다.



이 정책은 StorageGRID UI에서 적용되지 않으며 S3 API에서만 적용됩니다.

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

개체 잠금 보존 제한

이 버킷 정책은 객체 잠금 보존 기간을 10일 이하로 제한합니다

```
{
  "Version": "2012-10-17",
  "Id": "CustSetRetentionLimits",
  "Statement": [
    {
      "Sid": "CustSetRetentionPeriod",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws:s3:::testlock-01/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:object-lock-remaining-retention-days": "10"
        }
      }
    }
  ]
}
```

버전 ID를 기준으로 개체를 삭제하지 못하도록 제한합니다

이 그룹 정책은 버전 ID를 기준으로 버전이 지정된 개체를 삭제하지 못하도록 제한합니다

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

이 버킷 정책은 사용자 ID "56622399308951294926"으로 식별된 사용자(versionID로 식별됨)가 버전 ID로 버전이 지정된 객체를 삭제하지 못하도록 제한합니다

```

{
  "Statement": [
    {
      "Action": [
        "s3:DeleteObjectVersion"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::verdeny/*",
      "Principal": {
        "AWS": [
          "56622399308951294926"
        ]
      }
    },
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::verdeny/*",
      "Principal": {
        "AWS": [
          "56622399308951294926"
        ]
      }
    }
  ]
}

```

읽기 전용 액세스 권한이 있는 단일 사용자로 버킷을 제한합니다

이 정책을 사용하면 단일 사용자가 버킷에 대한 읽기 전용 액세스를 가질 수 있고 다른 모든 사용자에게 대한 액세스를 명시적으로 부인할 수 있습니다. 정책 맨 위에 있는 Deny 문을 그룹화하는 것은 보다 빠른 평가를 위한 좋은 방법입니다.

```

{
  "Statement": [
    {
      "Sid": "Deny non user1",
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS":
"urn:sgws:identity::34921514133002833665:user/user1"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "urn:sgws:s3::bucket1",
        "urn:sgws:s3::bucket1/*"
      ]
    },
    {
      "Sid": "Allow user1 read access to bucket bucket1",
      "Effect": "Allow",
      "Principal": {
        "AWS":
"urn:sgws:identity::34921514133002833665:user/user1"
      },
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "urn:sgws:s3::bucket1",
        "urn:sgws:s3::bucket1/*"
      ]
    }
  ]
}

```

그룹을 읽기 전용 권한으로 단일 하위 디렉토리(접두사)로 제한합니다

이 정책을 사용하면 그룹의 구성원이 버킷 내의 하위 디렉터리(접두사)에 읽기 전용 액세스 권한을 가질 수 있습니다. 버킷 이름은 "study"이고 하위 디렉토리는 "study01"입니다.

```

{
  "Statement": [
    {
      "Sid": "AllowUserToSeeBucketListInTheConsole",

```

```

        "Action": [
            "s3:ListAllMyBuckets"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::*"
        ]
    },
    {
        "Sid": "AllowRootAndstudyListingOfBucket",
        "Action": [
            "s3:ListBucket"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3::: study"
        ],
        "Condition": {
            "StringEquals": {
                "s3:prefix": [
                    "",
                    "study01/"
                ],
                "s3:delimiter": [
                    "/"
                ]
            }
        }
    },
    {
        "Sid": "AllowListingOfstudy01",
        "Action": [
            "s3:ListBucket"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::study"
        ],
        "Condition": {
            "StringLike": {
                "s3:prefix": [
                    "study01/*"
                ]
            }
        }
    }
},

```



```
{
  {
    "Sid": "AllowAllS3ActionsInstudy01Folder",
    "Effect": "Allow",
    "Action": [
      "s3:Getobject"
    ],
    "Resource": [
      "arn:aws:s3:::study/study01/*"
    ]
  }
}
```

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.