Procedimentos e exemplos de API

How to enable StorageGRID in your environment

NetApp
December 11, 2024

Índice

Procedimentos e exemplos de API

Teste e demonstre as opções de criptografia S3 no StorageGRID

Por Aron Klein

O StorageGRID e a API S3 oferecem várias maneiras diferentes de criptografar seus dados em repouso. Para saber mais, "Reveja os métodos de encriptação StorageGRID" consulte .

Este guia demonstrará os métodos de criptografia da API S3.

Criptografia do lado do servidor (SSE)

O SSE permite que o cliente armazene um objeto e criptografe-o com uma chave única que é gerenciada pelo StorageGRID. Quando o objeto é solicitado, o objeto é descriptografado pela chave armazenada no StorageGRID.

Exemplo SSE

- COLOQUE um objeto com SSE

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

- DIRIJA o objeto para verificar a criptografia

```
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": {}
}
```

- OBTENHA o objeto

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

Criptografia do lado do servidor com chaves fornecidas pelo cliente (SSE-C)

SSE permite que o cliente armazene um objeto e criptografe-o com uma chave única que é fornecida pelo cliente com o objeto. Quando o objeto é solicitado, a mesma chave deve ser fornecida para descriptografar e retornar o objeto.

Exemplo SSE-C.

- Para fins de teste ou demonstração, você pode criar uma chave de criptografia
  - Crie uma chave de criptografia

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

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

- Coloque um objeto com a chave gerada

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

- Cabeça o objeto

```
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=="
}
```

Se você não fornecer a chave de criptografia, você receberá um erro "ocorreu um erro (404) ao chamar a operação HeadObject: Not found"

- Obtenha o objeto

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

Se você não fornecer a chave de criptografia, você receberá um erro "ocorreu um erro (InvalidRequest) ao chamar a operação GetObject: O objeto foi armazenado usando uma forma de criptografia do lado do servidor. Os parâmetros corretos devem ser fornecidos para recuperar o objeto."

Criptografia do lado do servidor do bucket (SSE-S3)

O SSE-S3 permite que o cliente defina um comportamento de criptografia padrão para todos os objetos armazenados em um bucket. Os objetos são criptografados com uma chave exclusiva que é gerenciada pelo StorageGRID. Quando o objeto é solicitado, o objeto é descriptografado pela chave armazenada no StorageGRID.

Exemplo SSE-S3 do bucket

- Crie um novo intervalo e defina uma política de criptografia padrão
  - Crie um novo balde

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

  - Coloque criptografia de bucket

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

- Coloque um objeto no balde

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

- Cabeça o objeto

```
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": {}
}
```

- OBTENHA o objeto

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

Teste e demonstre o bloqueio de objetos S3D no StorageGRID

Por Aron Klein

O Object Lock fornece um modelo WORM para impedir que objetos sejam excluídos ou substituídos. A implementação do StorageGRID do bloqueio de objetos é avaliada pela Cohasset para ajudar a atender aos requisitos regulatórios, oferecendo suporte à retenção legal e ao modo de conformidade para retenção de objetos e políticas de retenção de buckets padrão.

Este guia demonstrará a API S3D Object Lock.

Guarda legal

- Bloqueio de objeto retenção legal é um simples status de ligar/desligar aplicado a um objeto.

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

- Verifique-o com uma operação GET.

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

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

- Desligue a retenção legal

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

- Verifique-o com uma operação GET.

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

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

Modo de conformidade

- A retenção de objeto é feita com um carimbo de data/hora retent until.

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

- Verifique o status de retenção

```
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"
    }
}
```

Retenção padrão

- Defina o período de retenção em dias e anos versículos a data de retenção até definida com a api per object.

```
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
```

- Verifique o status de retenção

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

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

- Coloque um objeto no balde

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

- A duração de retenção definida no bucket é convertida em um carimbo de data/hora de retenção no objeto.

```
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"
    }
}
```

Teste a exclusão de um objeto com uma retenção definida

O bloqueio de objetos é construído sobre o controle de versão. A retenção é definida em uma versão do objeto. Se uma tentativa for feita para excluir um objeto com uma retenção definida e nenhuma versão for especificada, um marcador de exclusão será criado como a versão atual do objeto.

- Exclua o objeto com retenção definida

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

- Liste os objetos no intervalo

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

  - Observe que o objeto não está listado.

- Liste versões para ver o marcador de exclusão e a versão original bloqueada

```
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"
        }
    ]
}
```

- Exclua a versão bloqueada do objeto

```
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
```

Exemplo de políticas de bucket e Group(IAM)

Aqui estão exemplos de políticas de bucket e políticas de grupo (políticas do IAM).

Políticas de grupo (IAM)

Acesso ao bucket do estilo do Home Directory

Essa política de grupo só permitirá que os usuários acessem objetos no intervalo chamado nome de usuário do usuário.

```
"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}/*"
    }

  ]
}
```

Negar criação de bucket de bloqueio de objetos

Esta política de grupo restringirá os usuários a criar um bucket com o bloqueio de objetos ativado no bucket.

Esta política não é aplicada na IU do StorageGRID, ela só é aplicada pela API S3.

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

Limite de retenção de bloqueio de objetos

Esta política de bucket restringirá a duração de retenção de bloqueio de objetos a 10 dias ou menos

```
{
 "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"
      }
    }
   }
  ]
}
```

Restrinja os usuários de excluir objetos por versionID

Esta política de grupo irá restringir os usuários de excluir objetos versionados por versionID

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

Esta política de bucket irá restringir um usuário(identificado pelo UserId "56622399308951294926") de excluir objetos versionados por versionID

```
{
  "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"
        ]
      }
    }
  ]
}
```

Restrinja o bucket a um único usuário com acesso somente leitura

Essa política permite que um único usuário tenha acesso somente leitura a um bucket e explicitamente o acesso da denys a todos os outros usuários. Agrupar as declarações deny no topo da política é uma boa prática para uma avaliação mais rápida.

```
{
    "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/*"
            ]
        }
    ]
}
```

Restrinja um grupo a um subdiretório único (prefixo) com acesso somente leitura

Essa diretiva permite que os membros do grupo tenham acesso somente leitura a um subdiretório (prefixo) dentro de um intervalo. O nome do intervalo é "estudo" e o subdiretório é "study01".

```
{
    "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/*"
            ]
        }
    ]
}
```

Informações sobre direitos autorais

Informações sobre marcas comerciais