Procedimientos y ejemplos de API

How to enable StorageGRID in your environment

NetApp
April 26, 2024

Tabla de contenidos

Procedimientos y ejemplos de API

Pruebe y muestre opciones de cifrado de S3 en StorageGRID

StorageGRID y la API de S3 ofrecen varias formas diferentes de cifrar sus datos en reposo. Para obtener más información, consulte "Consulte los métodos de cifrado de StorageGRID".

En esta guía se mostrarán los métodos de cifrado de la API de S3.

Cifrado del servidor (SSE)

SSE permite al cliente almacenar un objeto y cifrarlo con una clave única gestionada por StorageGRID. Cuando se solicita el objeto, la clave almacenada en StorageGRID descifra el objeto.

Ejemplo de SSE

- PONGA un objeto con SSE

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

- DIRÍJASE al objeto para verificar el cifrado

```
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": {}
}
```

- OBTENGA el objeto

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

Cifrado del servidor con claves proporcionadas por el cliente (SSE-C)

SSE permite al cliente almacenar un objeto y cifrarlo con una clave única proporcionada por el cliente con el objeto. Cuando se solicita el objeto, se debe proporcionar la misma clave para descifrar y devolver el objeto.

Ejemplo de SSE-C.

- Con fines de prueba o demostración, puede crear una clave de cifrado
  - Cree una clave de cifrado

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

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

- Coloque un objeto con la clave generada

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

- Dirigir el 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=="
}
```

Si no proporciona la clave de cifrado, recibirá un error "se ha producido un error (404) al llamar a la operación HeadObject: Not found"

- Obtenga el objeto

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

Si no proporciona la clave de cifrado, recibirá un error que indica que se ha producido un error (InvalidRequest) al llamar a la operación GetObject: El objeto se ha almacenado utilizando un formulario de cifrado del lado del servidor. Se deben proporcionar los parámetros correctos para recuperar el objeto."

Cifrado del servidor de bloques (SSE-S3)

SSE-S3 permite al cliente definir un comportamiento de cifrado predeterminado para todos los objetos almacenados en un bloque. Los objetos se cifran con una clave única gestionada por StorageGRID. Cuando se solicita el objeto, éste se descifra mediante una clave almacenada en StorageGRID.

Ejemplo de bloque SSE-S3

- Crear un bloque nuevo y establecer una política de cifrado predeterminada
  - Crear nuevo bloque

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

  - Put bucket Encryption

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

- Coloque un objeto en el bloque

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

- Dirigir el 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": {}
}
```

- OBTENGA el objeto

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

Por Aron Klein

Pruebe y muestre el bloqueo de objetos de S3 en StorageGRID

El bloqueo de objetos proporciona un modelo WORM para evitar que los objetos se eliminen o se sobrescriban. La implementación de StorageGRID de un bloqueo de objetos es un activo de valor empresarial que se evalúa para ayudar a cumplir los requisitos normativos, respalda la conservación legal y el modo de cumplimiento de normativas para la retención de objetos y las políticas de retención de bloques predeterminadas.

En esta guía se demostrará la API de bloqueo de objetos S3.

Conservación legal

- La retención legal de bloqueo de objetos es un estado de activación/desactivación simple aplicado a un objeto.

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

- Verifíquelo mediante una OPERACIÓN DE OBTENER.

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

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

- Desactivar la conservación legal

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

- Verifíquelo mediante una OPERACIÓN DE OBTENER.

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

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

Modo de cumplimiento de normativas

- La retención de objetos se realiza con una Marca de tiempo de retención hasta.

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

- Compruebe el estado de retención

```
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"
    }
}
```

Retención predeterminada

- Establezca el período de retención en días y años en lugar de una fecha de retención hasta definida con la api por objeto.

```
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
```

- Compruebe el estado de retención

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

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

- Coloque un objeto en el bloque

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

- La duración de retención establecida en el bloque se convierte en una Marca de tiempo de retención en el 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"
    }
}
```

Pruebe a eliminar un objeto con una retención definida

El bloqueo de objetos se crea sobre el control de versiones. La retención se define en una versión del objeto. Si se intenta eliminar un objeto con una retención definida y no se especifica ninguna versión, se crea un marcador de borrado como la versión actual del objeto.

- Elimine el objeto con la retención definida

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

- Enumere los objetos del bloque

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

  - Observe que el objeto no aparece en la lista.
- Enumere las versiones para ver el marcador de borrado y la versión 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": "566223993089512949 26"
            }
        }
    ],
    "DeleteMarkers": [
        {
            "Owner": {
                "DisplayName": "Tenant01",
                "ID": "566223993089512949 26"
            },
            "Key": "file01.txt",
            "VersionId":
"QjVDQzgzOTAtQ0FGNi0xMUVDLThFMzgtQ0RGMjAwQjk0MjM1",
            "IsLatest": true,
            "LastModified": "2022-05-03T15:35:50.248000+00:00"
        }
    ]
}
```

- Elimine la versión bloqueada del 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
```

Por Aron Klein

Ejemplo de políticas de bloque y grupo(IAM)

A continuación se muestran ejemplos de políticas de bloques y políticas de grupo (políticas IAM).

Políticas de grupo (IAM)

Acceso a bloque de estilo de directorio de casa

Esta política de grupo sólo permitirá a los usuarios acceder a los objetos del depósito denominado nombre de usuario de los usuarios.

```
"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}/*"
    }

  ]
}
```

Denegar creación de bloque de bloqueo de objetos

Esta política de grupo restringirá a los usuarios a crear un bloque con el bloqueo de objeto habilitado en el bloque.

> Esta política no se aplica en la interfaz de usuario de StorageGRID, sino que solo se aplica mediante la API de S3.

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

Límite de retención de bloqueo de objetos

Esta política de depósito restringirá la duración de la retención de bloqueo de objetos a 10 días o 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"
      }
    }
   }
  ]
}
```

Restringir a los usuarios la supresión de objetos por versionID

Esta política de grupo restringirá a los usuarios la supresión de 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 depósito restringirá a un usuario (identificado por el ID de usuario «56622399308951294926») de eliminar 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"
        ]
      }
    }
  ]
}
```

Restringir bloque a un solo usuario con acceso de sólo lectura

Esta directiva permite a un solo usuario tener acceso de sólo lectura a un bloque y denys explícitamente acceso a todos los demás usuarios. La agrupación de las declaraciones denegadas en la parte superior de la directiva es una buena práctica para una evaluación más 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 un grupo a un único subdirectorio (prefijo) con acceso de solo lectura

Esta política permite a los miembros del grupo tener acceso de solo lectura a un subdirectorio (prefijo) dentro de un bloque. El nombre del depósito es «study» y el subdirectorio es «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/*"
            ]
        }
    ]
}
```